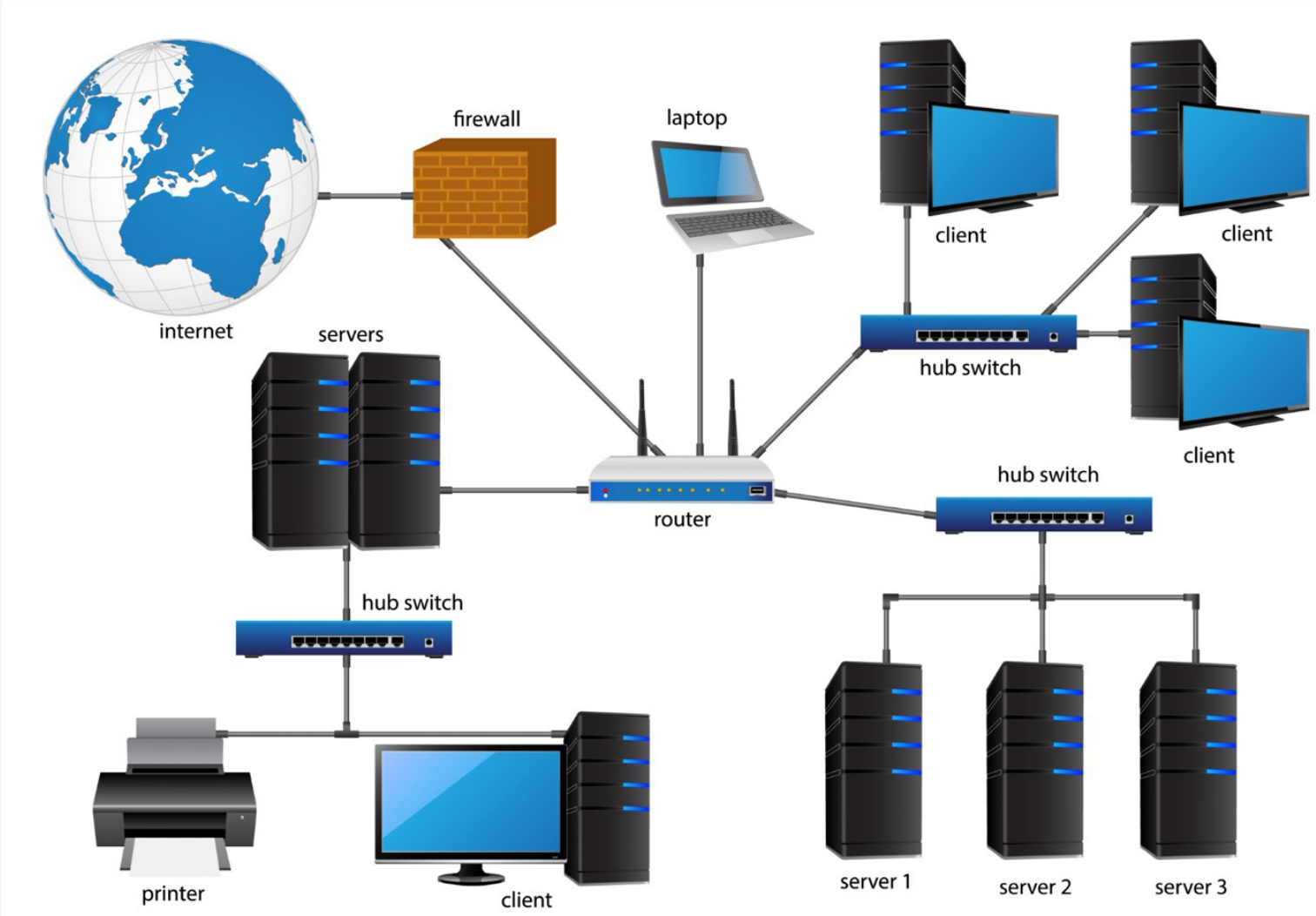
Get Ready to CRUSH Your CCNA Exam



CCNA (200-301) Practice Exam

CREATED BY

KevinWallace Training, LLC

Welcome to your CCNA (200-301) practice exam!

We at Kevin Wallace Training, LLC (https://kwtrain.com) want to help you *earn* your certification, not memorize brain dumps.

So, all questions in this practice exam were entirely created by us based on Cisco's CCNA (200-301) exam blueprint.

Even more important that the questions though are our **detailed explanations**, found in the second portion of this document.

We want you to know why each correct answer is correct. So, please spend plenty of time reading through the explanations for each question.

Before diving in, here are a couple of links to help us stay in contact:

---

https://youtube.com/kwallaceccie

You'll find hundreds of training videos on our YouTube channel to help explore a wide range of IT topics.

---

https://kwtrain.com/products

If you like our YouTube videos, you'll love our complete video training series.

I wish you all the best in your studies,

Kevin Wallace, CCIEx2 #7945 Emeritus (Enterprise Infrastructure & Collaboration)

Questions

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

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

2. 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

3. 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

4. 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

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

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

6. 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

7. 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

8. 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

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

   A. SW1#**mac address-table aging-time 60**
   B. SW1#**mac address-table aging-time 1**
   C. SW1#**mac address-table aging-time 3600**
   D. SW1#**mac address-table aging-time 600**

10. 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**

11. 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

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

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

13. Which command allows us to assign switch interface fa 1/0/1 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**

14. 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

15. 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**

16. 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

17. 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

18. 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

19. 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**

20. 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**

21. 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

22. 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

23. 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

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

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

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

A. 10100100
B. 01111100
C. 01111001
D. 01110000

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

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

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

Network 1 = 192.168.2.0 /24
Network 2 = 192.168.4.0 /24
Network 3 = 192.168.6.0 /24
Network 4 = 192.168.8.0 /24

A. /20
B. /22
C. /4
D. /16

28. 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

29. 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

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

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

31. 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

32. 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. 64

B. 112
C. 107
D. 86

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

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

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

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

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

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

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

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

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

A. IP Address

B. Shim Header
C. DLCI
D. MAC Address

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

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

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

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

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

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

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

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

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

A. Dopant

B. Jacket
C. Cladding
D. Core

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

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

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

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

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

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

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

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

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

A. PVST

B. Rapid PVST+
C. RSTP
D. MSTP

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

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

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

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

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

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

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

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

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

A. R1(config)#**ip route 10.0.0.0 255.255.255.0 192.168.1.10 91**
B. R1(config)#**ip route 10.0.0.0 255.255.255.0 192.168.1.10 backup**

C. R1(config)#**ip route 10.0.0.0 255.255.255.0 192.168.1.10 ospf preferred**
D. R1(config)#**ip route 10.0.0.0 255.255.255.0 192.168.1.10 111**

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

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

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

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

64. Which OSPF network type requires DR and BDR election?

A. Broadcast
B. Point-to-Point
C. Non-Broadcast
D. Shared

65. Which type of Link-State Advertisement (LSA) is created by each router in an OSPF network, containing information about the directly attached networks?

A. Type 1
B. Type 2
C. Type 3
D. Type 4

66. Which of the following commands will advertise interfaces in the 10.1.1.0/24 range into OSPF area 0?

A. R1(config-router)#**network 10.1.1.0 class-c area 0**
B. R1(config-router)#**network 10.1.1.0 255.255.255.0 area 0**
C. R1(config-router)#**network 10.1.1.0 0.0.0.255 area 0**
D. R1(config-router)#**network 10.1.1.0 subnet /24 area 0**

67. During Hot Standby Router Protocol (HSRP) active router election, what value can be manually altered to influence the winner?

A. Router ID
B. HSRP Priority
C. HSRP Group Number
D. Loopback Address

68. What is the default Advertisement Interval used in Virtual Router Redundancy Protocol (VRRP)?

A. 1 second
B. 3 seconds
C. 5 seconds
D. 10 seconds

69. Which first hop redundancy protocol makes use of all routers in the group, rather than electing primary and secondary devices?

A. HSRP
B. GLBP
C. VRRP
D. MPLS

70. What is the highest believable stratum value in Network Time Protocol (NTP) hierarchy?

A. 8
B. 12
C. 15
D. 16

71. Which of the following is not an advantage of Network Address Translation (NAT)?

A. Provides privacy to the inside hosts.
B. Eliminates the need for re-numbering when a network topology changes.
C. Conserves the registered IP address space.
D. Simplifies the use of tunneling protocols.

72. Which type of Network Address Translation (NAT) allows multiple users to be connected to the Internet using only a single public IP address?

A. Static NAT
B. Dynamic NAT
C. Port Address Translation
D. NAT Pool

73. Which protocol is most commonly used by a wireless LAN controller for controlling a lightweight access point (AP)?

A. LWAPP
B. CAPWAP
C. LDAP
D. AD HOC

74. How much space is found between channels 13 and 14 in the 2.4 Gigahertz (GHz) wireless range?

A. 12 MHz
B. 5 MHz
C. 10 MHz
D. 1 MHz

75. Which channel combination is ideal when using the 2.4 Gigahertz (GHz) band in order to avoid channel overlap?

A. 3,6,9,12
B. 1,7,14
C. 3,8,13
D. 1,6,11

76. When will the second attempt to renew DHCP information configured for an 8-hour lease take place?

A. After 4 hours
B. After 6 hours

C. After 7 hours
D. After 8 hours

77. What is the name of the notification message sent out by an SNMP agent?

A. OID
B. Trap
C. MIB
D. Query

78. Which command will show us locally stored Syslog information on a router?

A. R1#**syslog info**
B. R1#**show log local**
C. R1#**show logging**
D. R1#**show syslog**

79. Which file transfer protocol communicates by way of User Datagram Protocol (UDP)?

A. FTP
B. SFTP
C. FTPS
D. TFTP

80. Which Quality of Service (QoS) mechanism is performed at the input interface?

A. Classification and Marking
B. Congestion Management
C. Congestion Avoidance
D. Link Efficiency

81. Within an IPv6 Type of Service (ToS) byte, which category of traffic does the highest possible Differentiated Services Code Point (DSCP) binary value 101 110 indicate?

A. Default
B. Drop Traffic
C. Expedited Forwarding
D. Priority

82. Given a Committed Burst (Bc) of 6,000 bits and a Timing Interval (Tc) of 1/8th of a second (0.125 seconds), what is the Committed Information Rate (CIR)?

A. 12,000 bps
B. 750 bps
C. 48,000 bps
D. 6,000 bps

83. Which type of attack commonly attempts to appear as the default gateway of the network in order to intercept traffic?

A. Ransomware
B. ARP Poisoning
C. DNS Poisoning
D. Phishing

84. Which wireless encryption protocol uses 192-bit Advanced Encryption Standard (AES) for privacy protection in enterprise environments?

A. WPA
B. WPA2
C. WPA3
D. TKIP

85. Which piece of the AAA framework determines what a user is allowed to do?

A. Authentication
B. Authorization
C. Accounting
D. Access

86. When configuring DHCP Snooping, which command allows us to rate limit a range of user-facing ports in order to help prevent Denial of Service (DoS) attacks?

A. SW1(config-if-range)#**ip dhcp snooping limit rate 100**
B. SW1(config-if-range)#**ip dhcp snooping rate limit 100**
C. SW1(config-if-range)#**ip dhcp snooping 100 limit rate**
D. SW1(config-if-range)#**ip dhcp snooping 100 rate limit**

87. Which Quadrature Amplitude Modulation (QAM) value is used by 802.11ax?

A. 64-QAM
B. 1024-QAM
C. 256-QAM
D. 2048-QAM

88. Which type of Access Control List (ACL) allows you to prioritize traffic by source port?

A. Standard
B. Extended
C. Named
D. Numbered

89. Which of the following numbered Access Control Lists (ACLs) is a Standard ACL?

A. 1999
B. 101
C. 100
D. 2000

90. Where should more specific Access Control Entries (ACEs) be placed within an Access Control List (ACL)?

A. Near the bottom
B. Near the middle
C. After a deny all command
D. Near the top

91. Which Cisco features allows us to mitigate CAM table overflow attacks?

A. STP
B. PortFast
C. ACL
D. Port Security

92. What is the default Port Security violation mode on a switch?

A. Protect
B. Restrict
C. Shutdown
D. Drop

93. Which plane of operation is used to move traffic from an ingress interface to an appropriate egress interface as quickly as possible?

A. Data Plane
B. Control Plane
C. Management Plane
D. Remote Plane

94. When using REST APIs, which HTTP verb allows us to update something on the SDN controller?

A. POST
B. WRITE
C. CREATE
D. PUT

95. What is the name for a collection of manifests and data in Puppet?

A. Resource
B. Module
C. Manifest
D. Class

96. Which file transfer protocol does not have a mechanism for authentication?

A. FTP
B. SFTP
C. FTPS
D. TFTP

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

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

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

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

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

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

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

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

Questions and Answers

1. 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.

2. 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.

3. 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).

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

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

A. SW1#**mac address-table aging-time 60**
B. SW1#**mac address-table aging-time 1**
C. SW1#**mac address-table aging-time 3600**
D. SW1#**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.

10. 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.

11. 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.

12. 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.

13. Which command allows us to assign switch interface fa 1/0/1 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 group configuration mode.

14. 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.

15. 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.

16. 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).

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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. Standard unicast protocols include HTTP, FTP, and Telnet.

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

A. 10100100
B. 01111100
C. 01111001
D. 01110000

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.

26. 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.

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

    Network 1 = 192.168.2.0 /24
    Network 2 = 192.168.4.0 /24
    Network 3 = 192.168.6.0 /24
    Network 4 = 192.168.8.0 /24

A. /20
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 20 bits. This tells us that we should use a /20 subnet mask, or 255.255.240.0 in dotted decimal.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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

33. 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.

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

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

Answer: C
Explanation: The first step is when a client sends a SYN (synchronization) message to another client or server as a request to begin the 3-way handshake process. The other end will respond with a SYN-ACK (synchronization and acknowledgement) message if the SYN is accepted. The

final message is an ACK (acknowledgement) message sent from the original client, which completes the establishment of the TCP session.

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

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

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

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

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

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

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

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

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

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

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

Answer: A
Explanation: The rules for abbreviating an IPv6 address are below.

1. Leading zeros in a quartet can be omitted.
2. Consecutive quartets containing all zeros can be represented with a double colon.
3. Only one double colon can be used per address.

Given these rules, the leading zeros can be removed from the 2nd (0a1e), 4th (0d4c) and 7th (07a0) quartets. The 5th and 6th quartets consecutively contain all zeros, which can be replaced with a double colon.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. Destination IPv6 address

B. Source IPv6 Address
C. Link Local IPv6 Address
D. Global Unicast Address

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. Attenuation

B. Crosstalk
C. Jitter
D. Latency

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

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

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

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

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

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

Answer: D
Explanation: This command configures switch SW2 to takeover in the event that the primary root on VLAN 1 fails.

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

A. PVST
B. Rapid PVST+

C. RSTP
D. MSTP

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

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

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

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

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

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

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

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

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

Answer: A

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

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

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

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

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

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

Answer: D
Explanation: The default administrative distance (AD) value for a static route is 1, meaning that the route would be preferred over the OSPF route. If we want to make this a backup route, we must change the AD value to something larger than the AD value of an OSPF route, which is 110. With this command, a floating static route will be created with an AD value of 111.

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

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

Answer: B
Explanation: An OSPF-enabled router advertises Hello messages through the multicast address 224.0.0.5. This is sent to all routers connected to its interfaces in an attempt to search for

potential OSPF neighbors. The Hello messages contain all the necessary information needed to form a neighbor relationship between two OSPF-enabled routers on the same subnet.

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

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

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

64. Which OSPF network type requires DR and BDR election?

A. Broadcast
B. Point-to-Point
C. Non-Broadcast
D. Shared

Answer: A
Explanation: The broadcast network type is much more efficient for connecting a large number of devices in an OSPF network, as opposed to point-to-point networks. DR and BDR election allow for a multiaccess segment where full-mesh connectivity is not necessary.

65. Which type of Link-State Advertisement (LSA) is created by each router in an OSPF network, containing information about the directly attached networks?

A. Type 1
B. Type 2
C. Type 3
D. Type 4

Answer: A
Explanation: Type 1 LSAs are known as Router LSAs. A Type 1 Router LSA is exchanged between routers in the same area of origin and remain only within that area. An OSPF router used these packets to describe its own interfaces, as well as to carry information about its neighbors to adjacent routers in the same area.

66. Which of the following commands will allow interfaces with addresses in the 10.1.1.0/24 range to participate in OSPF area 0?

A. R1(config-router)#**network 10.1.1.0 class-c area 0**
B. R1(config-router)#**network 10.1.1.0 255.255.255.0 area 0**
C. R1(config-router)#**network 10.1.1.0 0.0.0.255 area 0**
D. R1(config-router)#**network 10.1.1.0 subnet /24 area 0**

Answer: C
Explanation: Rather than using a subnet mask to designate interfaces participating in OSPF, we instead use a wildcard mask. This can essentially be thought of as the inverse of the subnet mask, where each octet value in the subnet mask is subtracted from the value 255.

67. During Hot Standby Router Protocol (HSRP) active router election, what value can be manually altered to influence the winner?

A. Router ID
B. HSRP Priority
C. HSRP Group Number
D. Loopback Address

Answer: B
Explanation: During HSRP active router election, the router with the highest priority will win the election. By default, the HSRP priority value is set to 100. An active router can be manually identified by assigning a priority value of more than 100 to the desired active router.

68. What is the default Advertisement Interval used in Virtual Router Redundancy Protocol (VRRP)?

A. 1 second
B. 3 seconds
C. 5 seconds
D. 10 seconds

Answer: A
Explanation: Instead of using a Hello message as HSRP does, this type of message in VRRP is referred to as an Advertisement Interval. These advertisements are used to determine if the master router is up and functioning and are sent every 1 second by default.

69. Which first hop redundancy protocol makes use of all routers in the group, rather than electing primary and secondary devices?

A. HSRP
B. GLBP
C. VRRP
D. MPLS

Answer: B
Explanation: Gateway Load Balancing Protocol (GLBP) is a Cisco proprietary protocol that offers both redundancy and load balancing. This is performed by balancing traffic over multiple routers using a single virtual IP address and multiple virtual MAC addresses.

70. What is the highest believable stratum value in Network Time Protocol (NTP) hierarchy?

A. 8
B. 12
C. 15
D. 16

Answer: C
Explanation: The highest possible stratum value that is considered to be a believable time source is Stratum 15. Any stratum number above 15 would be considered unreliable, and time would not be learned from such a source.

71. Which of the following is not an advantage of Network Address Translation (NAT)?

A. Provides privacy to the inside hosts.
B. Eliminates the need for re-numbering when a network topology changes.
C. Conserves the registered IP address space.
D. Simplifies the use of tunneling protocols.

Answer: D
Explanation: Because the nature of NAT is to modify a portion of the packet during translation, and IPsec is designed to prevent the manipulation of data in transit, there are known issues with using IPsec and NAT in conjunction. In order to completely avoid problems, IPsec tunnel endpoints should always be located in the public address space.

72. Which type of Network Address Translation (NAT) allows multiple users to be connected to the Internet using only a single public IP address?

A. Static NAT
B. Dynamic NAT
C. Port Address Translation
D. NAT Pool

Answer: C
Explanation: Port Address Translation (PAT) allows multiple private IP addresses to be translated into a single registered public IP address, with port numbers used to distinguish which traffic belongs to which private IP address.

73. Which protocol is most commonly used by a wireless LAN controller for controlling a lightweight access point (AP)?

A. LWAPP
B. CAPWAP
C. LDAP
D. AD HOC

Answer: B
Explanation: The Control and Provisioning of Wireless Access Points (CAPWAP) protocol is an update to the original Lightweight Access Point Protocol (LWAPP) standard and is most commonly used today by wireless LAN controllers for management of access points (APs).

74. How much space is found between channels 13 and 14 in the 2.4 Gigahertz (GHz) wireless range?

A. 12 MHz
B. 5 MHz
C. 10 MHz
D. 1 MHz

Answer: A
Explanation: There are 14 channels designated in the 2.4 Gigahertz (GHz) wireless range. Channels 1 through 13 have a space of 5 Megahertz (MHz) between them. The exception is the space between channels 13 and 14, which is 12 MHz.

75. Which channel combination is ideal when using the 2.4 Gigahertz (GHz) band in order to avoid channel overlap?

A. 3,6,9,12
B. 1,7,14

C. 3,8,13
D. 1,6,11

Answer: D
Explanation: When selecting a 2.4 GHz wireless channel, channels 12 and 13 are allowed only under low powered conditions, and channel 14 is banned completely in the United States. This means that channels 1, 6, and 11 are the only non-overlapping channels in this range.

76. When will the second attempt to renew DHCP information configured for an 8-hour lease take place?

A. After 4 hours
B. After 6 hours
C. After 7 hours
D. After 8 hours

Answer: C
Explanation: The first attempt to renew a DHCP lease will take place when half of the configured lease time is reached. The second attempt takes place at 7/8 (87.5%) of the lease time, which would be after 7 hours in this example.

77. What is the name of the notification message sent out by an SNMP agent?

A. OID
B. Trap
C. MIB
D. Query

Answer: B
Explanation: SNMP trap messages are alert messages or notifications that are sent from a remote SNMP-enabled device (referred to as an SNMP agent) to a central SNMP manager.

78. Which command will show us locally stored Syslog information on a router?

A. R1#**syslog info**
B. R1#**show log local**
C. R1#**show logging**
D. R1#**show syslog**

Answer: C

Explanation: This command will display the state of Syslog and the contents of the local system logging buffer.

79. Which file transfer protocol communicates by way of User Datagram Protocol (UDP)?

A. FTP
B. SFTP
C. FTPS
D. TFTP

Answer: D
Explanation: Trivial File Transfer Protocol (TFTP) is a much simpler version of FTP, but it lacks a method for user authentication. This uses UDP communication, as opposed to the TCP communication used by more complex file transfer protocols.

80. Which Quality of Service (QoS) mechanism is performed at the input interface?

A. Classification and Marking
B. Congestion Management
C. Congestion Avoidance
D. Link Efficiency

Answer: A
Explanation: Classification and Marking is done at the input interface as near to the source as possible. This allows critical traffic to be marked early so the next hop can quickly and efficiently make a forwarding decision.

81. Within an IPv6 Type of Service (ToS) byte, which category of traffic does the highest possible Differentiated Services Code Point (DSCP) binary value 101 110 indicate?

A. Default
B. Drop Traffic
C. Expedited Forwarding
D. Priority

Answer: C
Explanation: This highest possible DSCP priority marking is referred to as Expedited Forwarding. Voice packets would be marked with this DSCP value, since their sensitivity to latency requires high priority treatment on the network.

82. Given a Committed Burst (Bc) of 6,000 bits and a Timing Interval (Tc) of 1/8th of a second (0.125 seconds), what is the Committed Information Rate (CIR)?

A. 12,000 bps
B. 750 bps
C. 48,000 bps
D. 6,000 bps

Answer: C
Explanation: The formula used to calculate the Committed Information Rate (CIR) is CIR = Bc/Tc. Using the given numbers, the equation becomes CIR = 6,000 bits / 0.125 seconds, which is 48,000 bps.

83. Which type of attack commonly attempts to appear as the default gateway of the network in order to intercept traffic?

A. Ransomware
B. ARP Poisoning
C. DNS Poisoning
D. Phishing

Answer: B
Explanation: Address Resolution Protocol (ARP) Poisoning is when an attacker sends falsified ARP messages over a LAN in order to link their own MAC address with the IP address of a legitimate network resource, often the default gateway. This allows all traffic to flow through their device, giving them an opportunity to intercept sensitive data.

84. Which wireless encryption protocol uses 192-bit Advanced Encryption Standard (AES) for privacy protection in enterprise environments?

A. WPA
B. WPA2
C. WPA3
D. TKIP

Answer: C
Explanation: Wi-Fi Protected Access version 3 is an update to the WPA standard that will replace version 2 within the next few years. Among other enhancements, WPA3 will include a 192-bit AES security suite for use in Enterprise Mode.

85. Which piece of the AAA framework determines what a user is allowed to do?

A. Authentication
B. Authorization
C. Accounting
D. Access

Answer: B
Explanation: After a user has been authenticated, authorization is used to determine which resources the user is allowed to affect, or which operations they can perform. This is distinct from authentication, as a user may be properly authenticated on the network but may not be authorized for a particular action based on their privileges.

86. When configuring DHCP Snooping, which command allows us to rate limit a range of user-facing ports in order to help prevent Denial of Service (DoS) attacks?

A. SW1(config-if-range)#**ip dhcp snooping limit rate 100**
B. SW1(config-if-range)#**ip dhcp snooping rate limit 100**
C. SW1(config-if-range)#**ip dhcp snooping 100 limit rate**
D. SW1(config-if-range)#**ip dhcp snooping 100 rate limit**

Answer: A
Explanation: This command configures a range of interfaces with a rate limit, ensuring that user-facing ports will not be overwhelmed with requests in a DoS situation. The unit for this limit is set in packets per second on most devices, and any traffic exceeding the limit will be dropped.

87. Which Quadrature Amplitude Modulation (QAM) value is used by 802.11ax?

A. 64-QAM
B. 1024-QAM
C. 256-QAM
D. 2048-QAM

Answer: B
Explanation: 802.11ax has a higher modulation scheme, moving from 256-QAM used by 802.11ac to 1024-QAM. This translates to better throughput and 25% higher data capacity, where 10 bits are represented per symbol.

88. Which type of Access Control List (ACL) allows you to prioritize traffic by source port?

A. Standard

B. Extended
C. Named
D. Numbered

Answer: B
Explanation: A Standard ACL allows you to prioritize traffic by the source IP address only. An Extended ACL provides greater control over which traffic is prioritized, using source and destination IP addresses, source and destination TCP/UDP ports, and protocol ID.

89. Which of the following numbered Access Control Lists (ACLs) is a Standard ACL?

A. 1999
B. 101
C. 100
D. 2000

Answer: A
Explanation: Standard ACLs fall within the range of numbers 1 – 99, with an expanded range identified as numbers 1300 – 1999.

90. Where should more specific Access Control Entries (ACEs) be placed within an Access Control List (ACL)?

A. Near the bottom
B. Near the middle
C. After a deny all command
D. Near the top

Answer: D
Explanation: More specific Access Control Entries (ACEs) should be placed near the top of an ACL. Since ACLs are processed in a top-down manner, more specific ACEs could potentially be skipped if general ACEs find a traffic match first.

91. Which Cisco features allows us to mitigate CAM table overflow attacks?

A. STP
B. PortFast
C. ACL
D. Port Security

Answer: D

Explanation: In a CAM table overflow attack, frames are flooded into the network in an attempt to fill up the CAM table with spoofed MAC addresses. The Port Security feature allows us to specify the maximum number of MAC addresses that can be learned by a particular port.

92. What is the default Port Security violation mode on a switch?

A. Protect
B. Restrict
C. Shutdown
D. Drop

Answer: C
Explanation: The shutdown option is the default Port Security action taken during a violation. This will put the interface into an error-disabled state and send an SNMP trap notification, if configured for SNMP.

93. Which plane of operation is used to move traffic from an ingress interface to an appropriate egress interface as quickly as possible?

A. Data Plane
B. Control Plane
C. Management Plane
D. Remote Plane

Answer: A
Explanation: The Data Plane is also referred to as the Forwarding Plane, responsible for forwarding traffic to the next hop along the path to the destination based on control plane logic.

94. When using REST APIs, which HTTP verb allows us to update something on the SDN controller?

A. POST
B. WRITE
C. CREATE
D. PUT

Answer: D
Explanation: The HTTP PUT verb is most often used for updating existing information on a controller. PUT replaces the information with a newer version in its entirety.

95. What is the name for a collection of manifests and data in Puppet?

A. Resource
B. Module
C. Manifest
D. Class

Answer: B
Explanation: A module is a collection of manifests and data, such as facts, files, and templates. These are useful for organizing Puppet code, allowing the code to be split into multiple manifests.

96. Within Ansible, what is the name for an ordered list of tasks or instructions?

A. Inventory
B. Playbook
C. YAML
D. Module

Answer: B
Explanation: Ordered lists of tasks are referred to as playbooks within Ansible. These playbooks allow you to run tasks repeatedly and are written in the YAML syntax.

97. Which file transfer protocol does not have a mechanism for authentication?

A. FTP
B. SFTP
C. FTPS
D. TFTP

Answer: D
Explanation: Trivial File Transfer Protocol (TFTP) is a much simpler version of FTP, but it lacks a method for user authentication. This uses UDP communication, as opposed to the TCP communication used by more complex file transfer protocols.

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

A. Global Unicast
B. Loopback
C. Multicast

D. Link Local

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

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

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

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

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

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

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

Thanks for studying with our CCNA (200-301) Practice Exam!

If you've read through this entire document, I know something about you…

Specifically, I know you and I are a lot alike and that we're hungry to always be learning and advancing our careers.

I sincerely hope this practice exam helps you advance in your career and achiever your CCNA certification.

If you'd like even more in-depth video-based training from us, please check out all our courses at the following link:

https://kwtrain.com/products

Take good care,

Kevin Wallace, CCIEx2 #7945 Emeritus (Enterprise Infrastructure & Collaboration)