ENARSI v1.1 (300-410) Video Training Series
Practice Exam

Questions

1. Which of the following sources of route information has the highest (i.e. the least believable) administrative distance?

   A. RIP
   B. External EIGRP
   C. OSPF
   D. Internal EIGRP

2. What is the seed metric for EIGRP?

   A. 20
   B. 1
   C. Infinity
   D. 0

3. Which of the following is not an option for assigning a metric to a routing protocol?

   A. Set a default metric for all routing sources being injected into a routing protocol.
   B. Set a metric using a Route Map.
   C. Specify a metric as part of the “redistribute” command.
   D. Specify a metric with a Route Tag.

4. You wish to redistribute all routes within AS 1 into AS 2 with the exception of 192.168.1.0/24. Which of the following approaches can you use to selectively filter that route?

   A. Create an ACL to match the 192.168.1.0/24 network, and reference that ACL under a “route map deny” statement.
   B. Use the “filter-list 192.168.1.0/24” option as part of the “redistribute” command.
   C. Create an ACL to match the 192.168.1.0/24 network, and reference that network in a “distribute list” command.
   D. Use the “distribute-list 192.168.1.0/24” option as part of the “redistribute” command.

5. What route-map configuration mode command is used to set a route tag to a value of 10?

   A. create tag 10
   B. match tag 10
   C. tag mode 10
   D. set tag 10

6. When redistributing IPv6 routes, which of the following is true?

   A. By default, the “redistribute” command includes connected routes on interfaces enabled for the redistributed protocol.
   B. By default, the “redistribute” command does not include connected routes on interfaces enabled for the redistributed protocol.
   C. The “redistribute” command is used exclusively for redistributing IPv4 routes, while the “redistribute-v6” command is used for redistributing IPv6 routes.
   D. If you wish to set a non-default metric on a redistributed route, the “metric” option must be used as part of the “redistribute” command.

7. Where should Policy Based Routing (PBR) be applied on a router?

   A. On a router’s egress interface
   B. In a router’s global configuration mode
   C. On a router’s ingress interface
   D. In a router’s router configuration mode

8. What configuration structure does PBR use to match traffic and specify behavior for that traffic?

   A. policy-map
   B. route-map
   C. class-map
   D. access-class

9. Which of the following is true regarding VRF, by default?

   A. With VRF, virtual routers share an IP routing table.
   B. With VRF, virtual routers have their own IP routing table, but they also see routes in the physical router’s IP routing table.
   C. With VRF, all virtual routers must be using the same IP routing protocol.
   D. With VRF, all virtual routers have their own independent IP routing tables.

10. In a VRF configuration, you wish view the IP routing table of a virtual router with a VRF instance name of “TENANT-A”. What command would you use?

A. show ip route vrf TENANT-A
B. show address family ip4 TENANT-A
C. show vrf TENANT-A ip route
D. show virtual-instance TENANT-A ip route

11. Which of the following protocols does EIGRP use to ensure delivery of routing updates?

A. STP
B. Dijkstra
C. RTP
D. DUAL

12. What is EIGRP’s default Hold Time on a LAN interface?

A. 5 seconds
B. 10 seconds
C. 15 seconds
D. 20 seconds

13. By default, EIGRP uses which of the following parameters to calculate its metric?

A. Delay and Load
B. Bandwidth and Delay
C. Bandwidth and Reliability
D. Bandwidth, Delay, Reliability, Load, and MTU

14. What is the name given to an EIGRP backup route that has met the Feasibility Condition?
A. Feasible Successor Route
B. Successor Route
C. Standby Route
D. DUAL Route

15. EIGRP’s Feasibility Condition requires a Feasible Successor’s Reported Distance to be less than what?

A. The Advertised Distance of the Successor Route
B. The Administrative Distance of the Successor Route
C. The Reported Distance of the Successor Route
D. The Feasible Distance of the Successor Route

16. If an EIGRP router loses its Successor Route to a destination network and it has no Feasible Successor Route, what message does the router send out in an attempt to find an alternate path to the network?

A. Hello
B. Query
C. Open
D. Discover

17. Which of the following is true of EIGRP for IPv4 neighbors?

A. EIGRP neighbors must have matching Variance values
B. EIGRP neighbors must have matching Process IDs (PIDs)
C. EIGRP neighbors must have matching Autonomous System (AS) numbers
D. EIGRP neighbors must have matching Hello and Hold Timers

18. What can be used in an EIGRP Stub Router configuration to allow selected routes to be advertised by the Stub Router?

A. Leak Map
B. Policy Map
C. Class Map
D. Service Policy

19. Under which condition will EIGRP not load balance across a backup path with the Variance feature?

A. The backup path's metric equals, but is not less than, the product of the Variance and the metric of the Successor Route.
B. The backup path does not meet the Feasibility Condition.
C. The Variance value is greater than 4.
D. The backup path uses an interface with a different Hello Timer than the interface used by the Successor Route.

20. What command is used to enable EIGRP's Automatic Summarization feature?

A. Router(config-router)# ip summary-address eigrp [AS]
B. Router(config-if)# auto-summary
C. Router(config-if)# ip summary-address eigrp [AS]
D. Router(config-router)# auto-summary

21. What interface configuration mode command is issued to tell an interface to participate in an EIGRP for IPv6 routing process for Autonomous System (AS) 1?

A. Router(config-if)# ipv6 unicast-routing eigrp 1
B. Router(config-if)# unicast-routing 1
C. Router(config-if)# ipv6 eigrp 1
D. Router(config-if)# eigrp ipv6 1

22. Under what Named EIGRP configuration mode would you configure the Variance option?

A. Address-Family-Topology configuration mode
B. Address-Family configuration mode
C. Address-Family-Interface configuration mode
D. Service-Family configuration mode

23. Which of the following routing protocols support the SHA hashing algorithm?

A. EIGRP for IPv4
B. EIGRP for IPv6
C. Named EIGRP
D. All of the above

24. What is the effect of setting a router's OSPF routing process to a Priority of 0?

A. It causes that router to be elected as a DR.
B. It causes that router to be elected as a BDR.
C. It prevents that router from participating in a DR election.
D. It suspends the OSPF process on that router.

25. By default, if you set an OSPF interface's Hello timer to 10 seconds, what will be the value of the Dead timer?
A. 5 seconds
B. 20 seconds
C. 30 seconds
D. 40 seconds

26. What is the default Reference Bandwidth used by OSPF to calculate Cost?

A. 100 kbps
B. 100 Mbps
C. 1 Gbps
D. 10 Gbps

27. What is the default OSPF Network Type of a non-Frame Relay OSPF interface?
A. Point-to-Point
B. Point-to-Multipoint
C. NBMA
D. Broadcast

28. What LSA Type is used to inject networks from a separate autonomous system (AS) into an OSPF Stub or Totally Stubby Area?

A. Type 3
B. Type 4
C. Type 5
D. Type 7

29. What Cisco IOS command is used to change the default reference-bandwidth of an OSPF-speaking router?

A. reference-bandwidth [bandwidth_amount]
B. interface-cost [bandwidth_amount]
C. auto-metric reference-bandwidth [bandwidth_amount]
D. auto-cost reference-bandwidth [bandwidth_amount]

30. What types of packets are sent over an OSPF Virtual Link?

A. Data packets
B. OSPF packets
C. GRE packets
D. Data, OSPF, and GRE packets

31. What Cisco IOS command is used to perform OSPF route summarization on an ABR?

A. area range
B. prefix-list
C. summary-address
D. distribute-list

32. What OSPFv3 LSA Type is used to advertise an area's Link Local address?

A. Type 4
B. Type 7
C. Type 8
D. Type 9

33. What command is used to create an OSPFv3 routing process with the Address Families configuration approach?

A. router ospfv3 [process_id]
B. ipv6 ospf [process_id]
C. router ipv6 ospf [process_id]
D. ospfv3 [process_id]

34. Which of the following is a hashing option for OSPFv3 Address Families authentication?
    A. DES
    B. Plain Text
    C. AES
    D. SHA-1

35. What well-known port is used by BGP when establishing a session?

    A. TCP 179
    B. TCP 443
    C. TCP 137
    D. TCP 161

36. In which state does a BGP-enabled router wait for the receipt of a Keepalive message in order to completely establish the BGP session?

    A. Active
    B. Idle
    C. OpenSent
    D. OpenConfirm

37. Which BGP command allows us to change interface source address used when establishing a neighbor adjacency?

    A. update-interface
    B. session-source
    C. update-source
    D. set-source

38. Which category of BGP attributes must be present in all updates and are passed on to other BGP peers?

    A. Well-known discretionary
    B. Well-known mandatory
    C. Optional transitive
    D. Optional nontransitive

39. Which command allows us to disable the default BGP synchronization feature found in older Cisco IOS versions?

    A. no suppress
    B. no local preference
    C. no metric-type internal
    D. no synchronization

40. Which mechanism within Multiprotocol BGP (MP-BGP) allows BGP to carry multiple protocols at once?

A. Route reflectors
B. VPNv4
C. Address families
D. L2VPN

41. Which BGP feature allows us to reduce the number of BGP updates created, lowering resource usage on BGP-enabled devices?

A. Peer group
B. Multihop
C. Route reflector
D. Summarization

42. What is the default time-to-live (TTL) value used with external BGP (eBGP)?

A. 0
B. 5
C. 2
D. 1

43. Which BGP mechanism allows all internal BGP (iBGP) neighbors within an autonomous system to learn about all available routes without creating loops in the network, and without using a full-mesh configuration?

A. MP-BGP
B. Communities
C. Route reflectors
D. Filtering

44. Which optional keyword is used to suppress prefixes and present only an aggregate address in the BGP update?

A. no-summary
B. summary-only
C. aggregate-address
D. suppress-update

45. Which BGP command allows for routes to be received even if a router sees its own autonomous system number in the AS-Path section of a BGP update?

A. no-prepend
B. replace-as
C. allowas-in
D. local-as

46. Which protocol is used to automatically generate and exchange labels between multiprotocol label switching (MPLS) routers?

A. LFIB
B. LIB
C. LDP
D. LSR

47. Which structure within an MPLS Layer 3 VPN configuration determines which Virtual Routing and Forwarding (VRF) instance a VPNv4 route will be imported into?

A. Route Distinguisher
B. Route Target
C. Next Hop
D. VPN Label

48. Which of the following is NOT a valid format for a VPN Route Distinguisher in a VRF configuration?

A. ASN:nn
B. IP-address:nn
C. MAC:nn
D. 4BASN:nn

49. Which protocol is used to dynamically scale a network through use with Dynamic Multipoint VPNs?

A. NHRP
B. NBMA
C. NHC
D. DNS

50. When configuring a DMVPN hub, which command enables the router to support multicast traffic over the tunnel interfaces?

A. ip nhrp multicast tunnel
B. ip nhrp int tun0 multicast
C. ip nhrp traffic-type multicast
D. ip nhrp map multicast dynamic

51. Which command will require the TY line connections to authenticate a user with the local database of the router?

A. R1(config-line)# local authentication
B. R1(config-line)# vty local
C. R1(config-line)# login local
D. R1(config-line)# aaa login local

52. Which command allows us to configure a router to use a loopback address as the source for TACACS+ communication?

A. R1(config)# tacacs+ source Loopback 0
B. R1(config)# tacacs session source Loopback 0
C. R1(config)# ip tacacs source-interface Loopback 0
D. R1(config-tacacs)# source-interface Loopback 0

53. Which standard port is used by RADIUS for authentication purposes?

A. 1812
B. 1813
C. 1642
D. 1643

54. Which Cisco IOS command will display the hours during which a time-based ACL named AFTER-WORK is configured to be active?

A. R1# show acl periodic AFTER-WORK
B. R1# show periodic AFTER-WORK
C. R1# show active AFTER-WORK
D. R1# show time-range AFTER-WORK

55. Which command is correct when applying an IPv6 ACL named FILTER to an interface in the inbound direction?

A. R1(config-if)# ipv6 traffic-filter FILTER in
B. R1(config-if)# ipv6 access-list FILTER in
C. R1(config-if)# ipv6 access-group FILTER in
D. R1(config-if)# ipv6 FILTER access-list in

56. Which Unicast Reverse Path Forwarding (uRPF) mode verifies that a packet source IP arrives on the same interface the router would use to reach the IP address?

A. Verbose Mode
B. Loose Mode
C. Strict Mode
D. Asymmetric Mode

57. Which structure within a Control Plane Policing (CoPP) configuration is used to define the action which should be taken against policed traffic?

A. Policy Map
B. ACL
C. Class Map
D. Service Policy

58. The IPv6 RA Guard feature filters out which type of router advertisements in an IPv6 network?

A. Broadcast
B. Multicast
C. Unicast
D. Frame Relay

59. Where can we apply an IPv6 DHCPv6 guard policy?

A. Only on interface
B. Only a VLAN
C. On either an interface or a VLAN
D. Only globally

60. What is used by IPv6 nodes to discover the presence and link-layer addresses of other nodes which reside on the same link?

A. STP
B. LDP
C. NDP
D. ARP

61. Which feature allows us to filter inbound traffic on L2 switch ports that are not found in the IPv6 binding table?

A. IPv6 RA Guard
B. DHCPv6 Guard
C. IPv6 ND Inspection
D. IPv6 Source Guard

62. Which command will allow an administrator to connect to a Cisco device's VTY line only over port 22?

A. R1(config-line)# transport input telnet
B. R1(config-line)# transport input 22
C. R1(config-line)# transport input all
D. R1(config-line)# transport input ssh

63. When switching a router configuration from SSHv1 to SSHv2, which command is necessary in order to provide secure access?

A. R1(config)# crypto key generate rsa
B. R1(config)# generate rsa key
C. R1(config)# secure-access crypto key
D. R1(config)# input password rsa

64. Which well-known port number is commonly used to move files and images between a Cisco router and a TFTP server?

A. TCP 69
B. UDP 69
C. TCP 121
D. UDP 121

65. Which version of SNMP added the “inform” command in order to provide positive acknowledgement of message receipt?

A. SNMPv1
B. SNMPv1.5
C. SNMPv2c
D. SNMPv3

66. When Cisco IOS command configures a remote user to receive traps using communication configured for authentication without privacy?

A. R1(config)# snmp-server host 10.1.1.50 v3 priv
B. R1(config)# snmp-server host 10.1.1.50 v3 auth
C. R1(config)# snmp-server host 10.1.1.50 v3 noauth
D. R1(config)# snmp-server host 10.1.1.50 v3 authnopriv

67. Which Syslog command will configure a Cisco device for logging at the Warning level, and also those levels considered to be more severe?

A. R1(config)# logging level 2
B. R1(config)# logging level 3
C. R1(config)# logging level 4
D. R1(config)# logging level 5

68. What is the general rule of thumb when using Cisco debug commands?

A. Use a debug command that is as general as possible.
B. Use a debug command on a device as close to the source as possible.
C. Use a debug command on a device as close to the destination as possible.
D. Use a debug command that is as specific as possible.

69. Which Cisco IOS command allows us to specifically turn off conditional debugging that has been put in place for the GigabitEthernet 0/1 interface of a router?

A. R1# debug off interface gig 0/1
B. R1# no debug all
C. R1# undebug interface gig 0/1
D. R1# no debug condition interface gig 0/1

70. A device within our network that has a statically configured IP address has begun having communication issues. From a Cisco router acting as a DHCP server, how can we verify an issue with the IP address?

A. R1# show ip dhcp conflict
B. R1# show dhcp conflict
C. R1# show dhcp binding
D. R1# show excluded-address

71. Under what condition would the DHCP Relay Agent feature be required in order to make sure our network hosts are able to obtain an IP address through DHCP?

A. The host and DHCP server are in the same broadcast domain.
B. The hosts and DHCP server are in different broadcast domains.
C. The hosts and DHCP server are directly connected.
D. The hosts and DHCP server are not directly connected.

72. Below is a section of an IP SLA configuration that does not appear to be working properly. What should be done in order to correct the issue with the IP SLA probe?

```
R1# show ip sla con 1

***
Operation timeout (milliseconds): 5000
Type of operation to perform: udp-jitter
Target address/Source address: 10.1.1.50/0.0.0.0
Target port/Source port: 16500/0
Codec Packet size: 32
Control Packets: enabled
Schedule:
   Operation frequency (seconds): 5
   Next scheduled start time: Pending trigger
   Group scheduled: FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE

 ***
```

A. Configure a source port.
B. Configure a source address.
C. Configure the start time.
D. Configure an ageout time.

73. What is the definition of a floating static route?

A. A static route with an administrative distance higher than 0.
B. A static route with an administrative distance higher than 2.
C. A static route with an administrative distance higher than 1.
D. A static route with an administrative distance higher than 10.

74. Which version of NetFlow features a fixed packet format?

A. NetFlow v4
B. NetFlow v7
C. NetFlow v5
D. NetFlow v9

75. Which version of NetFlow would be preferred in a network using multicast media applications where ingress and egress monitoring is desired?

A. NetFlow v9
B. NetFlow v7
C. NetFlow v5
D. NetFlow v4

76. Which version of NetFlow allows us to use multiple flow monitors and exporters simultaneously on the same traffic?

A. NetFlow v9
B. NetFlow v10
C. IPFIX
D. Flexible NetFlow

77. Which section of Cisco DNA Center is dedicated to proactive issue detection?

A. Design
B. Assurance
C. Policy
D. Provision

78. Which tool within Cisco DNA Center Assurance allows us to collect network topology and routing data from discovered devices?

A. Analytics
B. Contextual Insight
C. Path Trace
D. Network Health

Questions and Answers

1. Which of the following sources of route information has the highest (i.e. the least believable) administrative distance?

   A. RIP
   B. External EIGRP
   C. OSPF
   D. Internal EIGRP

Answer: B
Explanation: The administrative distance (AD) of RIP is 120. The AD of External EIGRP (i.e. routes injected into EIGRP from a different autonomous system) is 170. OSPF's AD is 110, and Internal EIGRP (i.e. routes learned within an EIGRP autonomous system) has an AD of 90.

Video Reference: 1.1.1 Administrative Distance

2. What is the seed metric for EIGRP?

   A. 20
   B. 1
   C. Infinity
   D. 0

Answer: C
Explanation: A seed metric is assigned to a redistributed route by default if you don't configure a different metric for your redistributed route. The seed metric for OSPF is 20, while the seed metric of RIP and EIGRP is Infinity.

Video Reference: 1.1.2 Route Redistribution Fundamentals

3. Which of the following is not an option for assigning a metric to a routing protocol?

   A. Set a default metric for all routing sources being injected into a routing protocol.
   B. Set a metric using a Route Map.
   C. Specify a metric as part of the "redistribute" command.
   D. Specify a metric with a Route Tag.

Answer: D
Explanation: All of the options are valid for setting a metric for a routing protocol other than "Specify a metric with a Route Tag." A Tag can be assigned to a route, but it acts as a label rather than a metric.

Video Reference: 1.1.3 Mutual Route Redistribution Configuration

4. You wish to redistribute all routes within AS 1 into AS 2 with the exception of 192.168.1.0/24. Which of the following approaches can you use to selectively filter that route?

   A. Create an ACL to match the 192.168.1.0/24 network, and reference that ACL under a “route map deny” statement.
   B. Use the “filter-list 192.168.1.0/24” option as part of the “redistribute” command.
   C. Create an ACL to match the 192.168.1.0/24 network, and reference that network in a “distribute list” command.
   D. Use the “distribute-list 192.168.1.0/24” option as part of the “redistribute” command.

Answer: A
Explanation: A common way to filter a route from being redistributed is to match the network with an ACL. Then, that ACL can be referenced as part of a “route map deny” statement. For example, let’s say you enter the “access-list 1 permit 192.168.1.0 0.0.0.255” command to create an ACL with a number of 1. Then, you can create a route map with a command such as “route-map DEMO deny 10”. Then, in route-map configuration mode, you can reference ACL 1 with the command “match ip address 1”. However, to allow other routes to be redistributed, you should follow-up the initial “route-map” command with another “route-map” command having a higher sequence number, permitting all other routes, such as “route-map permit 20”.

Video Reference: 1.1.4 Route Redistribution with Route Maps

5. What route-map configuration mode command is used to set a route tag to a value of 10?

   A. create tag 10
   B. match tag 10
   C. tag mode 10
   D. set tag 10

Answer: D
Explanation: You can set a tag on a route with the route-map configuration mode command “set tag 10”. Then, you can use the route-map configuration mode command “match tag 10” to recognize (and possibly deny) routes that are marked with a tag of 10.

Video Reference: 1.1.5 Resolving Route Redistribution Issues

6. When redistributing IPv6 routes, which of the following is true?

A. By default, the “redistribute” command includes connected routes on interfaces enabled for the redistributed protocol.
B. By default, the “redistribute” command does not include connected routes on interfaces enabled for the redistributed protocol.
C. The “redistribute” command is used exclusively for redistributing IPv4 routes, while the “redistribute-v6” command is used for redistributing IPv6 routes.
D. If you wish to set a non-default metric on a redistributed route, the “metric” option must be used as part of the “redistribute” command.

Answer: B
Explanation: Unlike redistributing IPv4 routes, when redistributing IPv6 routes, the “redistribute” command does not include connected routes on interfaces enabled for the redistributed protocol. However, you could instruct the “redistribute” command to redistribute those routes with the “redistribute [routing_source] connected-interfaces” command.

Video Reference: 1.1.6 Redistributing IPv6 Routes

7. Where should Policy Based Routing (PBR) be applied on a router?

A. On a router’s egress interface
B. In a router’s global configuration mode
C. On a router’s ingress interface
D. In a router’s router configuration mode

Answer: C
Explanation: Although “Local PBR” can be applied in a router’s global configuration mode, PBR is applied on a router’s ingress interface.

Video Reference: 1.2.1 PBR Fundamentals

8. What configuration structure does PBR use to match traffic and specify behavior for that traffic?

A. policy-map
B. route-map
C. class-map
D. access-class

Answer: B

Explanation: A policy-map and class-map are used for quality of service (QoS). An access-class is used to limit incoming connections to a router's management plane. However, a route-map can match traffic and dictate how that matched traffic should be treated, and it's a route-map that's used by Policy Based Routing (PBR).

Video Reference: 1.2.2 PBR Configuration

9. Which of the following is true regarding VRF, by default?

   A. With VRF, virtual routers share an IP routing table.
   B. With VRF, virtual routers have their own IP routing table, but they also see routes in the physical router's IP routing table.
   C. With VRF, all virtual routers must be using the same IP routing protocol.
   D. With VRF, all virtual routers have their own independent IP routing tables.

Answer: D
Explanation: With Virtual Routing and Forwarding (VRF), each virtual router maintains its own unique IP routing table. Therefore, different virtual routers running on the same physical router can run different routing protocols. Also, by default, virtual routers cannot see routes in the physical router's IP routing table. However, it is possible to configure "leak maps" to allow specific routers in the physical router's IP routing table to appear in the IP routing table of a virtual router.

Video Reference: 1.3.1 VRF-lite Theory

10. In a VRF configuration, you wish view the IP routing table of a virtual router with a VRF instance name of "TENANT-A". What command would you use?

   A. show ip route vrf TENANT-A
   B. show address family ip4 TENANT-A
   C. show vrf TENANT-A ip route
   D. show virtual-instance TENANT-A ip route

Answer: A
Explanation: The "show ip route vrf TENANT-A" command is the appropriate command to view the IP routing table of the VRF instanced named "TENANT-A."

Video Reference: 1.3.2 VRF-lite Configuration

11. Which of the following protocols does EIGRP use to ensure delivery of routing updates?

A. STP
B. Dijkstra
C. RTP
D. DUAL

Answer: C
Explanation: EIGRP uses the Reliable Transport Protocol (RTP) to ensure delivery of routing updates to its neighbors. However, RTP is not used to confirm receipt of Hello messages. Spanning Tree Protocol (STP) is used to prevent a Layer 2 topological loop. The Dijkstra Algorithm is used by OSPF to select the shortest path to a destination network. The Diffusing Update Algorithm (DUAL) is used by EIGRP to select Successor and Feasible Successor routes.

Video Reference: 2.1.1 Review of EIGRP Fundamentals

12. What is EIGRP's default Hold Time on a LAN interface?

A. 5 seconds
B. 10 seconds
C. 15 seconds
D. 20 seconds

Answer: C
Explanation: On a LAN interface, EIGRP's default Hello Time is 5 seconds, and its default Hold Time is 15 seconds.

Video Reference: 2.1.2 EIGRP Timers

13. By default, EIGRP uses which of the following parameters to calculate its metric?

A. Delay and Load
B. Bandwidth and Delay
C. Bandwidth and Reliability
D. Bandwidth, Delay, Reliability, Load, and MTU

Answer: B
Explanation: By default, EIGRP uses Bandwidth and Delay to calculate its metric. However, EIGRP's K-values can be adjusted for its metric calculation causing the calculation to also include Reliability and Load. Although Maximum Transmission Unit (MTU) size does not factor into EIGRP's metric calculation directly, MTU size can be used as a tie breaker between two routes with equal metrics.

Video Reference: 2.1.3 EIGRP Metric Calculation

14. What is the name given to an EIGRP backup route that has met the Feasibility Condition?
    A. Feasible Successor Route
    B. Successor Route
    C. Standby Route
    D. DUAL Route

Answer: A
Explanation: An EIGRP Successor Route is the preferred route to a destination network, while an EIGRP Feasible Successor Route is a backup route that has met the Feasibility condition.

Video Reference: 2.1.5 EIGRP Feasibility Condition

15. EIGRP's Feasibility Condition requires a Feasible Successor's Reported Distance to be less than what?

    A. The Advertised Distance of the Successor Route
    B. The Administrative Distance of the Successor Route
    C. The Reported Distance of the Successor Route
    D. The Feasible Distance of the Successor Route

Answer: D
Explanation: EIGRP's Feasibility Condition requires a Feasible Successor's Reported Distance (RD) to be less than the Feasible Distance (FD) of the Successor Route (i.e. the preferred route).

Video Reference: 2.1.5 EIGRP Feasibility Condition

16. If an EIGRP router loses its Successor Route to a destination network and it has no Feasible Successor Route, what message does the router send out in an attempt to find an alternate path to the network?

    A. Hello
    B. Query
    C. Open
    D. Discover

Answer: B
Explanation: EIGRP sends out a Query message in an attempt to find an alternate route to a network if it loses its Successor Route to that network and it has no Feasible Successor Route. In

earlier versions of Cisco IOS, if the Query Reply was dropped on its way back to the sending router, the sending router might think that one or more downstream routers were unavailable. This resulted in a Stuck-In-Active (SIA) condition.

Video Reference: 2.1.6 EIGRP's Query Process

17. Which of the following is true of EIGRP for IPv4 neighbors?

    A. EIGRP neighbors must have matching Variance values
    B. EIGRP neighbors must have matching Process IDs (PIDs)
    C. EIGRP neighbors must have matching Autonomous System (AS) numbers
    D. EIGRP neighbors must have matching Hello and Hold Timers

Answer: C
Explanation: EIGRP neighbors do not need matching Variance values. Also, OSPF uses Process IDs, EIGRP does not. Instead, EIGRP must have matching Autonomous System (AS) numbers. Finally, while having matching Hello and Hold Timers is considered a best practice, it is not required for EIGRP. However, OSPF does require matching timer values.

Video Reference: 2.1.7 EIGRP for IPv4 – Traditional Configuration

18. What can be used in an EIGRP Stub Router configuration to allow selected routes to be advertised by the Stub Router?

    A. Leak Map
    B. Policy Map
    C. Class Map
    D. Service Policy

Answer: A
Explanation: A Route Map can be configured to identify specific routes. Then, that Route Map can be reference by a Leak Map in a Stub Router configuration to allow selected routes (i.e. the routes specified by the Route Map) to be advertised by the Stub Router.

Video Reference: 2.1.8 EIGRP Stub Routing

19. Under which condition will EIGRP not load balance across a backup path with the Variance feature?

A. The backup path's metric equals, but is not less than, the product of the Variance and the metric of the Successor Route.
B. The backup path does not meet the Feasibility Condition.
C. The Variance value is greater than 4.
D. The backup path uses an interface with a different Hello Timer than the interface used by the Successor Route.

Answer: B
Explanation: EIGRP's Variance feature will load balance across one or more backup paths if those backup paths have a metric that is equal to or less than the product of the Variance value and the metric (i.e. the Feasible Distance) of the Successor Route. However, a backup path will not be used for load balancing if it did not meet the Feasibility Condition.

Video Reference: 2.1.9 EIGRP Load Balancing

20. What command is used to enable EIGRP's Automatic Summarization feature?

A. Router(config-router)# ip summary-address eigrp [AS]
B. Router(config-if)# auto-summary
C. Router(config-if)# ip summary-address eigrp [AS]
D. Router(config-router)# auto-summary

Answer: D
Explanation: EIGRP's Auto Summarization feature causes EIGRP to advertise classful networks, rather than the subnets within those classful networks. This feature is enabled in router configuration mode with the "auto-summary" command.

Video Reference: 2.1.10 EIGRP Route Summarization

21. What interface configuration mode command is issued to tell an interface to participate in an EIGRP for IPv6 routing process for Autonomous System (AS) 1?

A. Router(config-if)# ipv6 unicast-routing eigrp 1
B. Router(config-if)# unicast-routing 1
C. Router(config-if)# ipv6 eigrp 1
D. Router(config-if)# eigrp ipv6 1

Answer: C

Explanation: The “ipv6 eigrp [AS]” command is issued in interface configuration mode to cause an interface to participate in an EIGRP for IPv6 routing process.

Video Reference: 2.1.11 EIGRP for IPv6 – Traditional Configuration

22. Under what Named EIGRP configuration mode would you configure the Variance option?

A. Address-Family-Topology configuration mode
B. Address-Family configuration mode
C. Address-Family-Interface configuration mode
D. Service-Family configuration mode

Answer: A
Explanation: With Named EIGRP, you can configure topology-wide features such as Route Redistribution and Variance under Address-Family-Topology configuration mode.

Video Reference: 2.1.12 Named EIGRP Configuration

23. Which of the following routing protocols support the SHA hashing algorithm?

A. EIGRP for IPv4
B. EIGRP for IPv6
C. Named EIGRP
D. All of the above

Answer: C
Explanation: While Named EIGRP supports both the MD5 and SHA hashing algorithms, EIGRP for IPv4 and EIGRP for IPv6 only support the MD5 hashing algorithm.

Video Reference: 2.1.13 EIGRP Authentication

24. What is the effect of setting a router’s OSPF routing process to a Priority of 0?

A. It causes that router to be elected as a DR.
B. It causes that router to be elected as a BDR.
C. It prevents that router from participating in a DR election.
D. It suspends the OSPF process on that router.

Answer: C
Explanation: On an OSPF network segment that elects a Designated Router (DR) and Backup Designated Router (BDR), the router on the network segment with the highest Priority is

elected as the DR. If the Priority values on all routers are the same, the router with the highest Router ID wins the DR election. However, if you do not wish for a router to participate in the DR election, you can set its Priority to 0.

Video Reference: 2.2.1 Review of OSPF Fundamentals

25. By default, if you set an OSPF interface's Hello timer to 10 seconds, what will be the value of the Dead timer?
    A. 5 seconds
    B. 20 seconds
    C. 30 seconds
    D. 40 seconds

Answer: D
Explanation: By default, an OSPF interface's Dead timer is four times the Hello timer. Therefore, if an OSPF interface's Hello timer is 10 seconds, its Dead timer would be 40 seconds (i.e. 10 * 4 = 40).

Video Reference: 2.2.2 OSPF Timers

26. What is the default Reference Bandwidth used by OSPF to calculate Cost?

    A. 100 kbps
    B. 100 Mbps
    C. 1 Gbps
    D. 10 Gbps

Answer: B
Explanation: OSPF calculates the Cost of an interface by dividing the interface's speed by OSPF's Reference Bandwidth. The default Reference Bandwidth used by OSPF is 100 Mbps. Since Cost must be an integer, interfaces speeds of 100 Mbps or greater all have a cost of 1 by default. Therefore, a best practice recommendation is to set OSPF's Reference Bandwidth to at least the bandwidth amount of the highest speed interface being used by OSPF.

Video Reference: 2.2.3 OSPF Metric Calculation

27. What is the default OSPF Network Type of a non-Frame Relay OSPF interface?
    A. Point-to-Point
    B. Point-to-Multipoint
    C. NBMA
    D. Broadcast

Answer: D
Explanation: The default OSPF Network Type on an Ethernet interface is Broadcast. The default OSPF Network Type on a non-Frame Relay interface is Point-to-Point, and the default OSPF Network Type on a Frame Relay physical interface is NBMA (Non-Broadcast Multiple Access).

Video Reference: 2.2.4 OSPF Network Types

28. What LSA Type is used to inject networks from a separate autonomous system (AS) into an OSPF Stub or Totally Stubby Area?

    A. Type 3
    B. Type 4
    C. Type 5
    D. Type 7

Answer: D
Explanation: Type 5 LSAs are typically used to inject networks from a separate AS into OSPF. However, an OSPF Stub or Totally Stubby Area cannot have Type 5 LSAs. As a result, Type 7 LSAs are used to inject those networks.

Video Reference: 2.2.5 OSPF LSAs and Area Types

29. What Cisco IOS command is used to change the default reference-bandwidth of an OSPF-speaking router?

    A. reference-bandwidth [bandwidth_amount]
    B. interface-cost [bandwidth_amount]
    C. auto-metric reference-bandwidth [bandwidth_amount]
    D. auto-cost reference-bandwidth [bandwidth_amount]

Answer: D
Explanation: OSPF's default Reference Bandwidth is 100 Mbps. Therefore, this value should typically be changed to a higher value, in order to calculate different Cost values for interface speeds greater than 100 Mbps. To set a non-default Reference Bandwidth, in router configuration mode you can used the command: auto-cost reference-bandwidth [bandwidth_amount], where the unit of measure for bandwidth_amount is Mbps.

Video Reference: 2.2.6 OSPFv2 Configuration

30. What types of packets are sent over an OSPF Virtual Link?

A. Data packets
B. OSPF packets
C. GRE packets
D. Data, OSPF, and GRE packets

Answer: B
Explanation: An OSPF Virtual Link can be used to logically connect a discontiguous OSPF Area to a Backbone Area. While an OSPF Virtual Link is a type of tunnel, it is not a GRE tunnel, and no GRE packets are sent. Only OSPF packets are logically sent over the Virtual Link, with the Data packets traveling over physical links.

Video Reference: 2.2.7 OSPF Virtual Links

31. What Cisco IOS command is used to perform OSPF route summarization on an ABR?

A. area range
B. prefix-list
C. summary-address
D. distribute-list

Answer: A
Explanation: Unlike EIGRP, which can perform route summarization on any router, OSPF can only perform route summarization on an Area Border Router (ABR) or an Autonomous System Boundary Router (ASBR). The command used to perform OSPF route summarization on an ABR is the "area range" command, and the command used to perform OSPF route summarization on an ASBR is the "summary-address" command.

Video Reference: 2.2.8 OSPF Route Summarization

32. What OSPFv3 LSA Type is used to advertise an area's Link Local address?

A. Type 4
B. Type 7
C. Type 8
D. Type 9

Answer: C
Explanation: OSPFv3 adds a couple of LSA types to those seen with OSPFv2. Specifically, Type 8 and Type 9 LSA types are added. A Type 8 LSA (a.k.a. a "Link LSA") is used to advertise Link Local

addresses within an OSPF area, while a Type 9 LSA (a.k.a. an “Intra Area Prefix LSA”) is used to advertise networks within an OSPF area.

Video Reference: 2.2.9 OSPFv3 Traditional Configuration

33. What command is used to create an OSPFv3 routing process with the Address Families configuration approach?

    A. router ospfv3 [process_id]
    B. ipv6 ospf [process_id]
    C. router ipv6 ospf [process_id]
    D. ospfv3 [process_id]

Answer: A
Explanation: The “ipv6 router ospf [process_id]” command is used to create an OSPFv3 routing process using the Traditional Configuration approach. However, the “router ospfv3 [process_id]” command is used to create an OSPFv3 routing process using the Address Families configuration approach.

Video Reference: 2.2.10 OSPFv3 Address Families Configuration

34. Which of the following is a hashing option for OSPFv3 Address Families authentication?
    A. DES
    B. Plain Text
    C. AES
    D. SHA-1

Answer: D
Explanation: Secure Hash Algorithm 1 (“SHA-1” or “sha1”) and Message Digest 5 (“MD5”) are the only hashing algorithms supported for OSPFv3 Address Families authentication.

Video Reference: 2.2.11 OSPF Authentication

35. What well-known port is used by BGP when establishing a session?

    A. TCP 179
    B. TCP 443
    C. TCP 137
    D. TCP 161

Answer: A

Explanation: BGP neighbor adjacencies are established using a manual configuration, pointing to a peer router. This communication takes place over TCP port 179. TCP allows BGP to handle fragmentation, sequencing, and provide reliability.

Video Reference: 2.3.1 Review of BGP Fundamentals

36. In which state does a BGP-enabled router wait for the receipt of a Keepalive message in order to completely establish the BGP session?

    A. Active
    B. Idle
    C. OpenSent
    D. OpenConfirm

Answer: D
Explanation: In the OpenConfirm state, BGP waits for the receipt of either a Keepalive or Notification message. If no Keepalive message arrives, the state will move back to Idle. If there is the receipt of a neighbor’s Keepalive message, the BGP session moves to the final Established state.

Video Reference: 2.3.2 BGP States and Timers

37. Which BGP command allows us to change interface source address used when establishing a neighbor adjacency?

    A. update-interface
    B. session-source
    C. update-source
    D. set-source

Answer: C
Explanation: The “update-source” command allows us to change the interface source address used when establishing a BGP session. By default, when establishing a neighbor adjacency with another BGP-enabled router, the session is formed using the IP address of the outgoing interface nearest to the neighbor. It’s common to create a loopback interface on a router and set this instead as the source of a BGP session. This helps guard against outages, in a case where there may be redundant links between BGP routers. If there are redundant links and one link goes down, the BGP session will also momentarily go down and establish a second session with the redundant interface, creating a network outage during this transition. Using a loopback interface as the source address ensures a seamless transition in a case such as this.

Video Reference: 2.3.3 Neighbor Formation

38. Which category of BGP attributes must be present in all updates and are passed on to other BGP peers?

  A. Well-known discretionary
  B. Well-known mandatory
  C. Optional transitive
  D. Optional nontransitive

Answer: B
Explanation: Well-known mandatory attributes must be present and understood by all BGP peers, and they are required to exist in the BGP update message. These attributes can be seen in the output of the "show ip bgp" command, and include attributes such as the origin, the autonomous system path, and the next-hop address.

Video Reference: 2.3.4 BGP Path Selection

39. Which command allows us to disable the default BGP synchronization feature found in older Cisco IOS versions?

  A. no suppress
  B. no local preference
  C. no metric-type internal
  D. no synchronization

Answer: D
Explanation: A BGP router with synchronization enabled will only advertise a route learned from an internal BGP (iBGP) peer to an external BGP (eBGP) peer when there is an exact match of that route learned from an IGP (such as EIGRP or OSPF) in the routing table. The "no synchronization" command will specifically disable this feature, although by default this is already disabled in newer Cisco IOS versions.

Video Reference: 2.3.5 BGP Synchronization

40. Which mechanism within Multiprotocol BGP (MP-BGP) allows BGP to carry multiple protocols at once?

  A. Route reflectors
  B. VPNv4
  C. Address families
  D. L2VPN

Answer: C
Explanation: Address families allow MP-BGP to carry multiple protocols at once. BGP will default to an IPv4 address family if none is indicated, dedicated to carrying IPv4 routes. Other address families can be defined for other protocols depending on the IOS platform in use, including IPv6, VPNv4 and VPNv6 address families.

Video Reference: 2.3.6 IPv4 and IPv6 Address Families

41. Which BGP feature allows us to reduce the number of BGP updates created, lowering resource usage on BGP-enabled devices?

    A. Peer group
    B. Multihop
    C. Route reflector
    D. Summarization

Answer: A
Explanation: BGP peer groups allow us to group neighbors together in order to share configurations and policies. When BGP creates updates, a separate update is created for each neighbor. Peer groups can simplify our configuration and use less device resources, since updates will be processed for the peer group as a whole rather than for each separate neighbor.

Video Reference: 2.3.7 BGP Peer Groups

42. What is the default time-to-live (TTL) value used with external BGP (eBGP)?

    A. 0
    B. 5
    C. 2
    D. 1

Answer: D
Explanation: External BGP (eBGP) by default requires two BGP-enabled routers to be directly connected to one another in order to properly establish a neighbor adjacency. This is because the default TTL value is 1 when using eBGP. The BGP multihop feature can be used to overcome this, allowing us to configure a higher TTL value.

Video Reference: 2.3.8 BGP Multihop

43. Which BGP mechanism allows all internal BGP (iBGP) neighbors within an autonomous system to learn about all available routes without creating loops in the network, and without using a full-mesh configuration?

A. MP-BGP
B. Communities
C. Route reflectors
D. Filtering

Answer: C
Explanation: Internal BGP (iBGP) neighbors do not add their own autonomous system number to the BGP update messages sent out. For this reason, any routes learned from another iBGP neighbor will not be advertised to any other iBGP neighbor, which would require a full-mesh network to overcome. An alternative to this a BGP route reflector, which allows us to point to other iBGP routers in order to specifically forward routes that would not normally be sent.

Video Reference: 2.3.9 BGP Route Reflectors

44. Which optional keyword is used to suppress prefixes and present only an aggregate address in the BGP update?

A. no-summary
B. summary-only
C. aggregate-address
D. suppress-update

Answer: B
Explanation: BGP can advertise a summarized route through the “aggregate-address” command. By default, the summary address, along with all other prefixes, will be advertised in the BGP updates sent out to peers. These prefixes can be suppressed so that BGP updates only send out the summarized route to peers by appending the “summary-only” keyword when configuring the aggregate address.

Video Reference: 2.3.10 BGP Route Summarization

45. Which BGP command allows for routes to be received even if a router sees its own autonomous system number in the AS-Path section of a BGP update?

A. no-prepend
B. replace-as
C. allowas-in
D. local-as

Answer: C
Explanation: The Allow AS feature overrides the default behavior where a BGP router will discard a prefix in which its own autonomous system number is seen in the AS-Path. This is a built-in loop prevention mechanism that can be overridden with the “allowas-in” command.

Video Reference: 2.3.11 Influencing Path Selection

46. Which protocol is used to automatically generate and exchange labels between multiprotocol label switching (MPLS) routers?

   A. LFIB
   B. LIB
   C. LDP
   D. LSR

Answer: C
Explanation: Label Distribution Protocol (LDP) allows an MPLS router to generate labels for its prefixes, which are advertised to MPLS neighbors. LDP first establishes a neighbor adjacency with another LDP-capable device before exchanging labels. These labels allow MPLS-enabled routers to determine how data is forwarded in the network, rather than basing those decisions on IP addressing information.

Video Reference: 3.1.1 Overview of MPLS

47. Which structure within an MPLS Layer 3 VPN configuration determines which Virtual Routing and Forwarding (VRF) instance a VPNv4 route will be imported into?

   A. Route Distinguisher
   B. Route Target
   C. Next Hop
   D. VPN Label

Answer: B
Explanation: A Route Target (RT) is an 8-byte value added to a prefix within MPLS Layer 3 VPNs. The typical format is the autonomous system number followed by the customer site number, separated by a colon (e.g. 65100:1). The RT is attached to a prefix, creating a VPNv4 route that is sent over MP-BGP to a peer. The RT informs the receiving peer about which VRF the VPNv4 route should be imported into.

Video Reference: 3.1.2 MPLS Layer 3 VPN

48. Which of the following is NOT a valid format for a VPN Route Distinguisher in a VRF configuration?

   A. ASN:nn
   B. IP-address:nn
   C. MAC:nn
   D. 4BASN:nn

Answer: C
Explanation: A Route Distinguisher (RD) is used to identify a VRF routing instance. The accepted formats for specifying an RD include: ASN:nn, IP-address:nn, and 4BASN:nn.

Video Reference: 3.1.3 VRF-Aware Routing with MPLS Layer 3 VPN Configuration

49. Which protocol is used to dynamically scale a network through use with Dynamic Multipoint VPNs?

   A. NHRP
   B. NBMA
   C. NHC
   D. DNS

Answer: A
Explanation: The next-hop resolution protocol (NHRP) is functionally similar to how DNS works. This is an ARP-like protocol that allows DMVPN spokes to directly communicate with one another. This is a client-server model where the DMVPN hub maintains an NHRP database for each spoke, allowing for the spokes to build direct tunnels between themselves.

Video Reference: 3.2.1 DMVPN Overview

50. When configuring a DMVPN hub, which command enables the router to support multicast traffic over the tunnel interfaces?

   A. ip nhrp multicast tunnel
   B. ip nhrp int tun0 multicast
   C. ip nhrp traffic-type multicast
   D. ip nhrp map multicast dynamic

Answer: D

Explanation: The command “ip nhrp map multicast dynamic” allows the next-hop resolution protocol (NHRP) to automatically add routers to the multicast NHRP mappings. This is used when spoke routers need to initiate mGRE and IPsec tunnels to register their NHRP mappings.

Video Reference: 3.2.2 DMVPN Configuration

51. Which command will require the VTY line connections to authenticate a user with the local database of the router?

    A. R1(config-line)# local authentication
    B. R1(config-line)# vty local
    C. R1(config-line)# login local
    D. R1(config-line)# aaa login local

Answer: C
Explanation: While under line configuration mode, the command “login local” configures the lines to authenticate incoming sessions to the local user database on the router.

Video Reference: 4.1.1 Local Database

52. Which command allows us to configure a router to use a loopback address as the source for TACACS+ communication?

    A. R1(config)# tacacs+ source Loopback 0
    B. R1(config)# tacacs session source Loopback 0
    C. R1(config)# ip tacacs source-interface Loopback 0
    D. R1(config-tacacs)# source-interface Loopback 0

Answer: C
Explanation: While under global configuration mode, the command “ip tacacs source-interface” allows us to specify a particular interface as the source address for TACACS logging messages. It’s a best practice to set the source to a local loopback interface, so that log messages are more easily interpreted.

Video Reference: 4.1.2 TACACS+

53. Which standard port is used by RADIUS for authentication purposes?

A. 1812
B. 1813
C. 1642
D. 1643

Answer: A
Explanation: RADIUS commonly uses port 1812 for authentication and 1813 for accounting, as defined by the Internet Engineering Task Force (IETF). Some RADIUS servers also use 1645 for authentication and 1646 for accounting, so this the server configuration should be verified when implementing RADIUS in a network. It is possible to change these values when configuring RADIUS within Cisco IOS.

Video Reference: 4.1.3 RADIUS

54. Which Cisco IOS command will display the hours during which a time-based ACL named AFTER-WORK is configured to be active?

A. R1# show acl periodic AFTER-WORK
B. R1# show periodic AFTER-WORK
C. R1# show active AFTER-WORK
D. R1# show time-range AFTER-WORK

Answer: D
Explanation: The command "show time-range" followed by the name of a particular ACL will display the hours during which it is configured to be active. The output will show the days and times during which the ACL will be enforced.

Video Reference: 4.2.1 IPv4 ACLs

55. Which command is correct when applying an IPv6 ACL named FILTER to an interface in the inbound direction?

A. R1(config-if)# ipv6 traffic-filter FILTER in
B. R1(config-if)# ipv6 access-list FILTER in
C. R1(config-if)# ipv6 access-group FILTER in
D. R1(config-if)# ipv6 FILTER access-list in

Answer: A
Explanation: When applying an IPv6 ACL to an interface, rather than using the "access-group" command as we do with IPv4 ACLs, we instead need to use the "ipv6 traffic-filter" command.

Video Reference: 4.2.2 IPv6 Traffic Filters

56. Which Unicast Reverse Path Forwarding (uRPF) mode verifies that a packet source IP arrives on the same interface the router would use to reach the IP address?

    A. Verbose Mode
    B. Loose Mode
    C. Strict Mode
    D. Asymmetric Mode

Answer: C
Explanation: Using strict mode in uRPF means that the router will verify that the same interface on which the packet was received can be used to reach the packet's source IP address. If this is true, and there is a route in the routing table for the source, the packet will be permitted. By contrast, loose mode only checks to see if there is a route available in the routing table, and is not concerned with which interface is used to reach the source.

Video Reference: 4.2.3 uRPF

57. Which structure within a Control Plane Policing (CoPP) configuration is used to define the action which should be taken against policed traffic?

    A. Policy Map
    B. ACL
    C. Class Map
    D. Service Policy

Answer: A
Explanation: With a CoPP configuration, an ACL is used to identify particular traffic, which is classified and grouped using a Class Map. A Policy Map is used to define actions which should be taken against the traffic, such as rate-limiting or dropping. A Service Policy is then used to enable policing on the control plane interface.

Video Reference: 4.2.4 CoPP

58. The IPv6 RA Guard feature filters out which type of router advertisements in an IPv6 network?

    A. Broadcast
    B. Multicast

C. Unicast
D. Frame Relay

Answer: B
Explanation: In IPv6 networks, devices periodically send out router advertisement (RA) messages via multicast. These help network nodes determine information about the LAN, including the default gateway, network prefix lists, and more. The IPv6 RA Guard feature can filter these more specifically so that rogue advertisements cannot be introduced into the network.

Video Reference: 4.2.5 IPv6 RA Guard

59. Where can we apply an IPv6 DHCPv6 guard policy?

A. Only on interface
B. Only a VLAN
C. On either an interface or a VLAN
D. Only globally

Answer: C
Explanation: DHCPv6 guard uses a policy, similar to the way that IPv6 RA Guard works. This can be applied on a per-interface basis or at the VLAN level, applying the policy itself to the selected interfaces.

Video Reference: 4.2.6 DHCPv6 Guard

60. What is used by IPv6 nodes to discover the presence and link-layer addresses of other nodes which reside on the same link?

A. STP
B. LDP
C. NDP
D. ARP

Answer: C
Explanation: Neighbor Discovery Protocol (NDP) is used for IPv6 traffic, and it allows different nodes on the same link to advertise themselves to neighboring devices. It also allows them to learn information from these neighbors. These NDP messages are unsecure and susceptible to attacks, which is a case where we would use IPv6 ND Inspection/Snooping for protection. By snooping these messages, we can build a reference table called a DHCPv6 Snooping Binding Table which will help protect against things such as cache poisoning, DoS, and redirect attacks.

Video Reference: 4.2.7 IPv6 Neighbor Discovery Inspection/Snooping

61. Which feature allows us to filter inbound traffic on L2 switch ports that are not found in the IPv6 binding table?

    A. IPv6 RA Guard
    B. DHCPv6 Guard
    C. IPv6 ND Inspection
    D. IPv6 Source Guard

Answer: D
Explanation: IPv6 Source Guard is a first-hop security feature used for IPv6 networks that filters inbound traffic on a L2 switch. It references the IPv6 binding table, which is populated by an inspection feature such as ND inspection or IPv6 snooping. If the inbound traffic is not found in the binding table, the traffic will be denied, helping to protect against spoofing and DoS attacks.

Video Reference: 4.2.8 IPv6 Source Guard

62. Which command will allow an administrator to connect to a Cisco device's VTY line only over port 22?

    A. R1(config-line)# transport input telnet
    B. R1(config-line)# transport input 22
    C. R1(config-line)# transport input all
    D. R1(config-line)# transport input ssh

Answer: D
Explanation: SSH uses standard TCP port 22 for communication. Although the "transport input all" command will allow all methods of connection to the VTY line, in order to only allow SSH we would need to say "transport input ssh" under line configuration mode. It's a best practice to disallow less secure telnet connections in this manner.

Video Reference: 5.1.1 Console and VTY Lines

63. When switching a router configuration from SSHv1 to SSHv2, which command is necessary in order to provide secure access?

    A. R1(config)# crypto key generate rsa
    B. R1(config)# generate rsa key
    C. R1(config)# secure-access crypto key
    D. R1(config)# input password rsa

Answer: A
Explanation: While under global configuration mode, the command “crypto key generate rsa” will create an RSA key used for secure access within SSHv2. Entering this command will prompt you for the key modulus size in bits. SSHv2 requires the RSA key pair size to be greater than or equal to 768 bits.

Video Reference: 5.1.2 Remote Access Protocols

64. Which well-known port number is commonly used to move files and images between a Cisco router and a TFTP server?

A. TCP 69
B. UDP 69
C. TCP 121
D. UDP 121

Answer: B
Explanation: Trivial File Transfer Protocol (TFTP) is a standard used for transferring files. This protocol uses UDP communication over well-known port 69, as opposed to File Transfer Protocol (FTP) which uses TCP for communication over well-known port 21. The UDP communication used with TFTP makes this a faster method of file transfer.

Video Reference: 5.1.3 File Transfer Protocols

65. Which version of SNMP added the “inform” command in order to provide positive acknowledgement of message receipt?

A. SNMPv1
B. SNMPv1.5
C. SNMPv2c
D. SNMPv3

Answer: C
Explanation: The key advantage of SNMPv2c over SNMPv1 is the addition of the “informs” command. The original version of SNMP uses TRAP messages which are sent between SNMP entities without any acknowledgement or confirmation of receipt, meaning you have no assurance that the TRAP was received. SNMPv2c added an INFORM message, which is essentially a TRAP message that requires an entity to acknowledge that the TRAP was received.

Video Reference: 5.2.1 SNMPv2c

66. Which Cisco IOS command configures a remote user to receive traps using communication configured for authentication without privacy?

A. R1(config)# snmp-server host 10.1.1.50 v3 priv
B. R1(config)# snmp-server host 10.1.1.50 v3 auth
C. R1(config)# snmp-server host 10.1.1.50 v3 noauth
D. R1(config)# snmp-server host 10.1.1.50 v3 authnopriv

Answer: B
Explanation: The "auth" keyword configures a remote user to receive traps at the "authNoPriv" security level when using the SNMPv3 security model, meaning that authentication is used but encryption for privacy is not. SNMPv3 added both authentication and encryption, which can be used together or individually.

Video Reference: 5.2.2 SNMPv3

67. Which Syslog command will configure a Cisco device for logging at the Warning level, and also those levels considered to be more severe?

A. R1(config)# logging level 2
B. R1(config)# logging level 3
C. R1(config)# logging level 4
D. R1(config)# logging level 5

Answer: C
Explanation: Syslog levels range from most severe Level 0 (Emergency) through informational Level 7 (Debugging). Warning conditions are specified as Level 4 severity. Configuring a Cisco device for Syslog Level 4 (Warning) logging means that messages at Level 4 and those numerically lower are logged. This means that Levels 0-4 are collected, ranging from Emergency to Warning.

Video Reference: 5.3.1 Syslog Log Entries

68. What is the general rule of thumb when using Cisco debug commands?

A. Use a debug command that is as general as possible.
B. Use a debug command on a device as close to the source as possible.
C. Use a debug command on a device as close to the destination as possible.
D. Use a debug command that is as specific as possible.

Answer: D

Explanation: Debug commands have the ability to overwhelm system resources, because they can generate lots of information very quickly. It's a best practice to be as specific as possible when using debug commands, so as to limit the output to pertinent information.

Video Reference: 5.3.2 Debug Output

69. Which Cisco IOS command allows us to specifically turn off conditional debugging that has been put in place for the GigabitEthernet 0/1 interface of a router?

A. R1# debug off interface gig 0/1
B. R1# no debug all
C. R1# no debug condition interface gig 0/1
D. R1# undebug interface gig 0/1

Answer: C
Explanation: The command "no debug condition interface gig 0/1" will specifically remove conditional debugging that has been configured for the GigabitEthernet 0/1 interface. Although "no debug all" will also remove the condition, this also turns off all possible debugging in a global manner.

Video Reference: 5.3.3 Conditional Debug Output

70. A device within our network that has a statically configured IP address has begun having communication issues. From a Cisco router acting as a DHCP server, how can we verify an issue with the IP address?

A. R1# show ip dhcp conflict
B. R1# show dhcp conflict
C. R1# show dhcp binding
D. R1# show excluded-address

Answer: A
Explanation: "show ip dhcp conflict" command will display information about any IP address conflicts detected during DHCP negotiation. If we have a statically assigned IP address on a host that is within the range of our DHCP pool, it's possible that this IP address can also be assigned by the DHCP server, particularly if we fail to create an IP address exclusion within the DHCP pool to reserve the address.

Video Reference: 5.4.2 Cisco IOS DHCP Server

71. Under what condition would the DHCP Relay Agent feature be required in order to make sure our network hosts are able to obtain an IP address through DHCP?

A. The host and DHCP server are in the same broadcast domain.
B. The hosts and DHCP server are in different broadcast domains.
C. The hosts and DHCP server are directly connected.
D. The hosts and DHCP server are not directly connected.

Answer: B
Explanation: DHCP negotiation starts when a client sends out a broadcast message in order to obtain IP addressing. If the hosts and DHCP server lie within two different broadcast domains (e.g. different subnets), the broadcast messages will not be able to reach the DHCP server. This can be overcome with the DHCP Relay Agent feature of IOS (ip helper-address), which allows a router to forward DHCP messages from hosts towards the DHCP server, and vice versa.

Video Reference: 5.4.3 DHCP Relay Agent

72. Below is a section of an IP SLA configuration that does not appear to be working properly. What should be done in order to correct the issue with the IP SLA probe?

```
R1# show ip sla con 1

***
Operation timeout (milliseconds): 5000
Type of operation to perform: udp-jitter
Target address/Source address: 10.1.1.50/0.0.0.0
Target port/Source port: 16500/0
Codec Packet size: 32
Control Packets: enabled
Schedule:
   Operation frequency (seconds): 5
   Next scheduled start time: Pending trigger
   Group scheduled: FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE

 ***
```

A. Configure a source port.
B. Configure a source address.
C. Configure the start time.
D. Configure an ageout time.

Answer: C
Explanation: The output snippet indicates that this probe has not yet started, as evidenced by the “Next scheduled start time: Pending Trigger” section. The probe needs to be started by either specifying a specific start time, or by using the “start-time now” option to immediately trigger the probe.

Video Reference: 5.5.1 Jitter Measurements

73. What is the definition of a floating static route?

A. A static route with an administrative distance higher than 0.
B. A static route with an administrative distance higher than 2.
C. A static route with an administrative distance higher than 1.
D. A static route with an administrative distance higher than 10.

Answer: C
Explanation: The default administrative distance of a static route is 1. By manually configuring a static route with an administrative distance higher than 1, we are creating a floating static route. This is useful in cases where we want to provide a static backup route for a primary link. An example of this would be configuring two ISP connections and using tracking objects to automatically switch between those in the case of a failure.

Video Reference: 5.5.2 Tracking Objects

74. Which version of NetFlow features a fixed packet format?

A. NetFlow v4
B. NetFlow v7
C. NetFlow v5
D. NetFlow v9

Answer: C
Explanation: NetFlow v5 has a fixed packet format that is always the same. This makes v5 compatible with most all NetFlow collection device and software packages. NetFlow v5 is the most popular version for this reason, although NetFlow v9 continues to gain popularity. NetFlow v9 features a dynamic packet format and uses templates to inform the NetFlow collector about the format of the flows being exported.

Video Reference: 5.6.1 NetFlow version 5

75. Which version of NetFlow would be preferred in a network using multicast media applications where ingress and egress monitoring is desired?

A. NetFlow v9
B. NetFlow v7
C. NetFlow v5
D. NetFlow v4

Answer: A
Explanation: NetFlow v9 adds the ability to report on multicast traffic, both ingress and egress monitoring. Using NetFlow v9 allows you to add policies such as bandwidth restriction and quality of service rules to restrict multicast traffic.

Video Reference: 5.6.2 NetFlow version 9

76. Which version of NetFlow allows us to use multiple flow monitors and exporters simultaneously on the same traffic?

A. NetFlow v9
B. NetFlow v10
C. IPFIX
D. Flexible NetFlow

Answer: D
Explanation: Flexible NetFlow allows for the exportation of multiple types of flow records against the same traffic. This is useful in cases where two different departments might be interested in monitoring separate aspects of the network traffic, while keeping the flow records as concise as possible.

Video Reference: 5.6.3 Flexible NetFlow

77. Which section of Cisco DNA Center is dedicated to proactive issue detection?

A. Design
B. Assurance
C. Policy
D. Provision

Answer: B
Explanation: The Assurance section of Cisco DNA Center uses artificial intelligence and machine learning to try and predict services issues in the network in a proactive manner. This works by

collecting network telemetry from devices under the control of DNA Center in order to gain insights into the network.

Video Reference: 5.7.1 Network and Device Health Monitoring

78. Which tool within Cisco DNA Center Assurance allows us to collect network topology and routing data from discovered devices?

    A. Analytics
    B. Contextual Insight
    C. Path Trace
    D. Network Health

Answer: C
Explanation: The Path Trace tool within Cisco DNA Center Assurance allows us to create a visual representation of the path between two hosts or Layer 3 interfaces. This essentially works as a graphical version of the traceroute command, displaying the path through our known topology.

Video Reference: 5.7.2 Connectivity Monitoring