Free Questions for JN0-351 by go4braindumps

Shared by Gilbert on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two events cause a router to advertise a connected network to OSPF neighbors? (Choose two.)

Options:

A- When an OSPF adjacency is established.

B- When an interface has the OSPF passive option enabled.

C- When a static route to the 224.0.0.6 address is created.

D- When a static route to the 224.0.0.5 address is created.

Answer:

A, D

Explanation:

Ais correct because when an OSPF adjacency is established, a router will advertise a connected network to OSPF neighbors.An OSPF adjacency is a logical relationship between two routers that agree to exchange routing information using the OSPF protocol1.To

establish an OSPF adjacency, the routers must be in the same area, have compatible parameters, and exchange hello packets1.Once an OSPF adjacency is formed, the routers will exchange database description (DBD) packets, which contain summaries of their link-state databases (LSDBs)1.The LSDBs include information about the connected networks and their costs2. Therefore, when an OSPF adjacency is established, a router will advertise a connected network to OSPF neighbors through DBD packets.

Dis correct because when a static route to the 224.0.0.5 address is created, a router will advertise a connected network to OSPF neighbors.The 224.0.0.5 address is the multicast address for all OSPF routers3.A static route to this address can be used to send OSPF hello packets to all OSPF neighbors on a network segment3.This can be useful when the network segment does not support multicast or when the router does not have an IP address on the segment3.When a static route to the 224.0.0.5 address is created, the router will send hello packets to this address and establish OSPF adjacencies with other routers on the segment3. As explained above, once an OSPF adjacency is formed, the router will advertise a connected network to OSPF neighbors through DBD packets.

Question 2

Question Type: MultipleChoice

What are two reasons for creating multiple areas in OSPF? (Choose two.)

Options:

A- to reduce the convergence time

B- to increase the number of adjacencies in the backbone

C- to increase the size of the LSDB

D- to reduce LSA flooding across the network

Answer:

A, D

Explanation:

Option A is correct. Creating multiple areas in OSPF can help to reduce the convergence time . This is because changes in one area do not affect other areas, so fewer routers need to run the SPF algorithm in response to a change.

Option D is correct. Creating multiple areas in OSPF can help to reduce Link State Advertisement (LSA) flooding across the network. This is because LSAs are not flooded out of their area of origin.

Question 3

Question Type: MultipleChoice

Which two statements are correct about using firewall filters on EX Series switches? (Choose two.)

Options:

A- You can deploy only stateless firewall filters on an EX Series switch.

B- You can only apply firewall filters to Layer 2 traffic on an EX Series switch.

C- You can apply firewall filters to both Layer 2 and Layer 3 traffic on an EX Series switch.

D- You can deploy both stateless and stateful firewall filters on an EX Series switch.

Answer:

A, C

Explanation:

Ais correct because you can deploy only stateless firewall filters on an EX Series switch.A stateless firewall filter is a filter that evaluates each packet individually based on the header information, such as source and destination addresses, protocol, and port numbers1.A stateless firewall filter does not keep track of the state or context of a packet flow, such as the sequence number, flags, or session information1.EX Series switches support only stateless firewall filters, which are also called access control lists (ACLs) or packet filters2.

Cis correct because you can apply firewall filters to both Layer 2 and Layer 3 traffic on an EX Series switch.Layer 2 traffic is traffic that is switched within a VLAN or a bridge domain, while Layer 3 traffic is traffic that is routed between VLANs or networks3.EX Series switches support three types of firewall filters: port (Layer 2) firewall filters, VLAN firewall filters, and router (Layer 3) firewall filters4. You can

apply these filters to different interfaces and directions to control the traffic entering or exiting the switch.

Question 4

Question Type: MultipleChoice

Which two mechanisms are part of building and maintaining a Layer 2 bridge table? (Choose two.)

Options:

A- blocking

B- flooding

C- learning

D- listening

Answer:

B, C

Explanation:

Option B is correct.Flooding is a mechanism used in Layer 2 bridging where the switch sends incoming packets to all its ports except for the port where the packet originated1.This is done when the switch doesn't know the destination MAC address or when the packet is a broadcast or multicast1.

Option C is correct.Learning is another mechanism used in Layer 2 bridging where the switch learns the source MAC addresses of incoming packets and associates them with the port on which they were received23.This information is stored in a MAC address table, also known as a bridge table23.

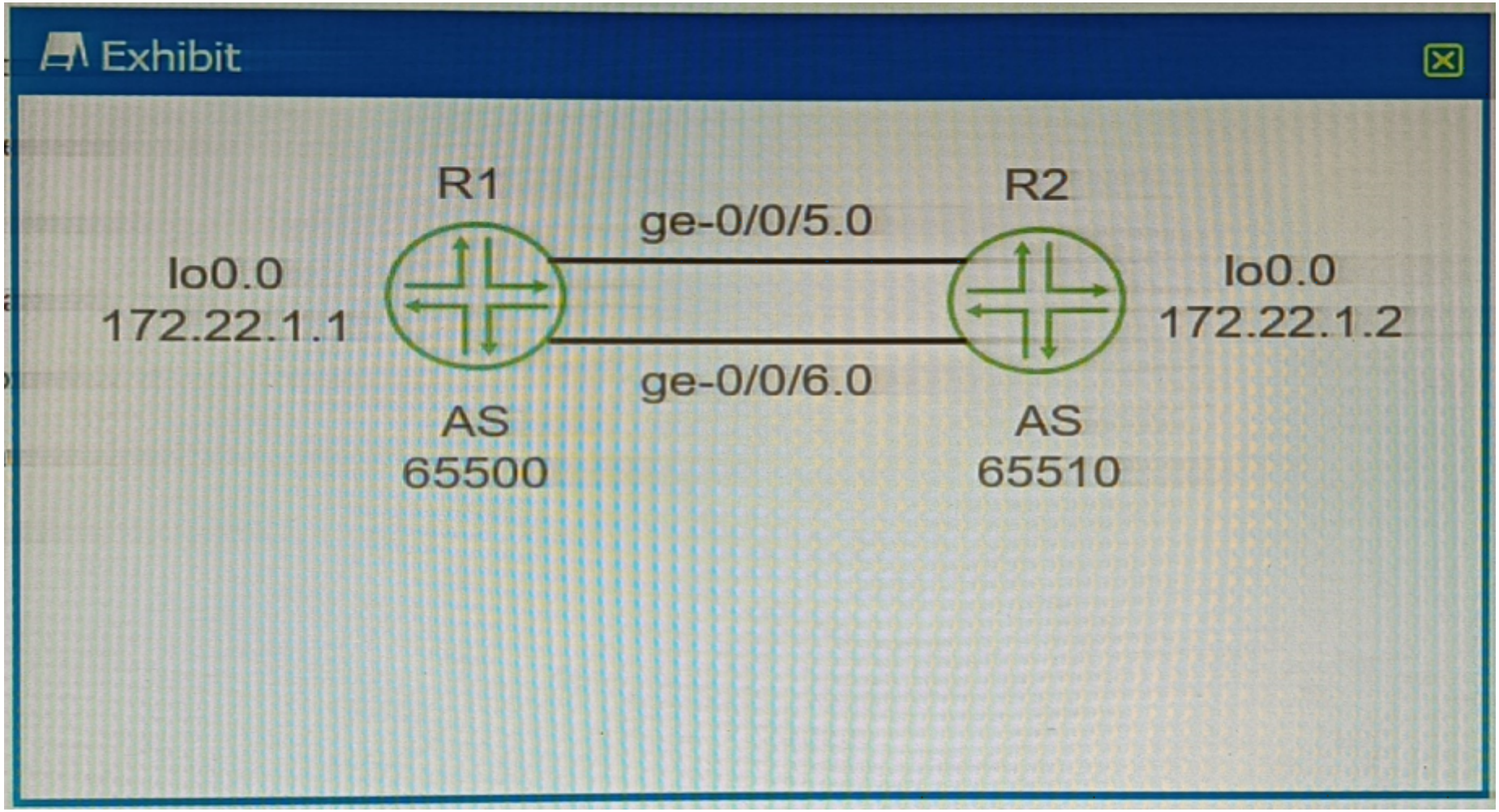
Option A is incorrect.Blocking is a state in Spanning Tree Protocol (STP) used to prevent loops in a network2.It's not a mechanism used in building and maintaining a Layer 2 bridge table2.

Option D is incorrect.Listening is also a state in Spanning Tree Protocol (STP) where the switch listens for BPDUs to make sure no loops occur in the network before transitioning to the learning state2.It's not a mechanism used in building and maintaining a Layer 2 bridge table2.

Question 5

Question Type: MultipleChoice

Exhibit.



You want to enable redundancy for the EBGP peering between the two routers shown in the exhibit. Which three actions will you perform in this scenario? (Choose three.)

Options:

A- Configure BGP multihop.

B- Configure loopback interface peering.

C- Configure routes for the peer loopback interface IP addresses.

D- Configure an MD5 peer authentication.

E- Configure a cluster ID.

Answer:

A, B, C

Explanation:

Ais correct because you need to configure BGP multihop to enable redundancy for the EBGP peering between the two routers.BGP multihop is a feature that allows BGP peers to establish a session over multiple hops, instead of requiring them to be directly connected1.By default, EBGP peers use a time-to-live (TTL) value of 1 for their packets, which means that they can only reach adjacent neighbors1.However, if you configure BGP multihop with a higher TTL value, you can allow EBGP peers to communicate over multiple routers in between1. This can provide redundancy in case of a link failure or a router failure between the EBGP peers.

Bis correct because you need to configure loopback interface peering to enable redundancy for the EBGP peering between the two routers.Loopback interface peering is a technique that uses loopback interfaces as the source and destination addresses for BGP sessions, instead of physical interfaces2.Loopback interfaces are virtual interfaces that are always up and reachable as long as the

router is operational2.By using loopback interface peering, you can avoid the dependency on a single physical interface or link for the BGP session, and use multiple paths to reach the loopback address of the peer2. This can provide redundancy and load balancing for the EBGP peering.

Cis correct because you need to configure routes for the peer loopback interface IP addresses to enable redundancy for the EBGP peering between the two routers.Routes for the peer loopback interface IP addresses are necessary to ensure that the routers can reach each other's loopback addresses over multiple hops2.You can use static routes or dynamic routing protocols to advertise and learn the routes for the peer loopback interface IP addresses2. Without these routes, the routers will not be able to establish or maintain the BGP session using their loopback interfaces.

Question 6

Question Type: MultipleChoice

Which two types of tunnels are able to be created on all Junos devices? (Choose two.)

Options:

A- STP

B- GRE

C- IP-IP

D- IPsec

Answer:

B, D

Explanation:

Junos devices support various types of tunnels for different purposes12.

Option B is correct.Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network1.Junos devices support GRE tunnels1.

Option D is correct.IPsec (Internet Protocol Security) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session1.Junos devices support IPsec tunnels1.

Option A is incorrect. Spanning Tree Protocol (STP) is not a type of tunnel.It's a network protocol designed to prevent loops in a bridged Ethernet local area network2.

Option C is incorrect.While Junos devices do support IP-IP (also known as IP tunneling), it's not supported on all Junos devices1.

Question 7

Question Type: MultipleChoice

What is a purpose of using a spanning tree protocol?

Options:

A- to look up MAC addresses

B- to eliminate broadcast storms

C- to route IP packets

D- to tunnel Ethernet frames

Answer:

B

Explanation:

A broadcast storm is a network condition where a large number of broadcast packets are sent and received by multiple devices, causing congestion and performance degradation1.A broadcast storm can occur when there are loops in the network topology, meaning that there are multiple paths between two devices2.

A spanning tree protocol is a network protocol that prevents loops from being formed when switches or bridges are interconnected via multiple paths.It does this by creating a logical tree structure that spans all the devices in the network, and disabling or blocking the links that are not part of the tree, leaving a single active path between any two devices3.

By eliminating loops, a spanning tree protocol also eliminates broadcast storms, as broadcast packets will not be forwarded endlessly along the looped paths.Instead, broadcast packets will be sent only along the tree structure, reaching each device once and avoiding congestion3.

Question 8

Question Type: MultipleChoice

What is the default MAC age-out timer on an EX Series switch?

Options:

A- 30 minutes

B- 30 seconds

C- 300 minutes

D- 300 seconds

Answer:

D

Explanation:

The default MAC age-out timer on an EX Series switch is300 seconds12.The MAC age-out timer is the maximum time that an entry can remain in the MAC table before it "ages out," or is removed31.This configuration can influence efficiency of network resource use by affecting the amount of traffic that is flooded to all interfaces1.When traffic is received for MAC addresses no longer in the Ethernet routing table, the router floods the traffic to all interfaces1.