JN0-351 Q&As

Enterprise Routing and Switching Specialist (JNCIS-ENT)

Pass Juniper JN0-351 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/jn0-351.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper Official Exam Center

QUESTION 1

Given the exhibit, which two statements are correct regarding the graceful-restart state for the BGP groups? (Choose two.)

```
[edit]
user@host# shcw protocols bgp group IBGP
type internal;
local-address 7.7.7.7;
export noroutes-filter;
graceful-restart {
     restart-time 100;
}
neighbor 1.1.1.1 {
     accept-remote-nexthop;
     import fix-nexthop;
     family inet {
          unicast;
     }
     family inet6 {
          unicast;
     }
}
neighbor 2.2.2.2;
[edit]
user@host# shcw protocols bgp group EBGP
type external;
multipath;
neighbor 198.168.4.2 {
     family inet {
          unicast;
     }
     peer-as 100;
     local-as 15169;
     multipath;
}
neighbor 198.168.5.2 {
     family inet {
          unicast'
     }
     peer-as 100;
     local-as 15169;
     multipath;
}
neighbor 198.168.6.2 {
     family inet {
          unicast;
     }
     peer-as 100;
     local-as 15169;
     multipath;
}
[edit]
user@host# show routing-options graceful-restart
disable;
```

A. The graceful-restart capability will be enabled for group IBGP.

B. The graceful-restart capability will be disabled for group IBGP.

C. The graceful-restart capability will be disabled for group EBGP.

D. The graceful-restart capability will be enabled for group EBGP.

Correct Answer: AC

QUESTION 2

Which two port security mechanisms rely on an accurate DHCP snooping database to operate correctly? (Choose two.)

A. IP source guard

B. persistent MAC learning

C. MACsec

D. dynamic ARP inspection

Correct Answer: AD

QUESTION 3

You have DHCP snooping enabled but no entries are automatically created in the snooping database for an interface on your EX Series switch. What are two reasons for the problem? (Choose two.)

A. The device that is connected to the interface has performed a DHCPRELEASE.

B. MAC limiting is enabled on the interface.

C. The device that is connected to the interface has a static IP address.

D. Dynamic ARP inspection is enabled on the interface.

Correct Answer: BC

Explanation: The DHCP snooping feature in Juniper Networks\\' EX Series switches works by building a binding database that maps the IP address, MAC address, lease time, binding type, VLAN number, and interface information1. This

database is used to filter and validate DHCP messages from untrusted sources1.

However, there are certain conditions that could prevent entries from being automatically created in the snooping database for an interface:

MAC limiting: If MAC limiting is enabled on the interface, it could potentially interfere with the operation of DHCP snooping. MAC limiting restricts the number of MAC addresses that can be learned on a physical interface to prevent MAC

flooding attacks1. This could inadvertently limit the number of DHCP clients that can be learned on an interface, thus

preventing new entries from being added to the DHCP snooping database.

Static IP address: If the device connected to the interface is configured with a static IP address, it will not go through the DHCP process and therefore will not have an entry in the DHCP snooping database1. The DHCP snooping feature relies

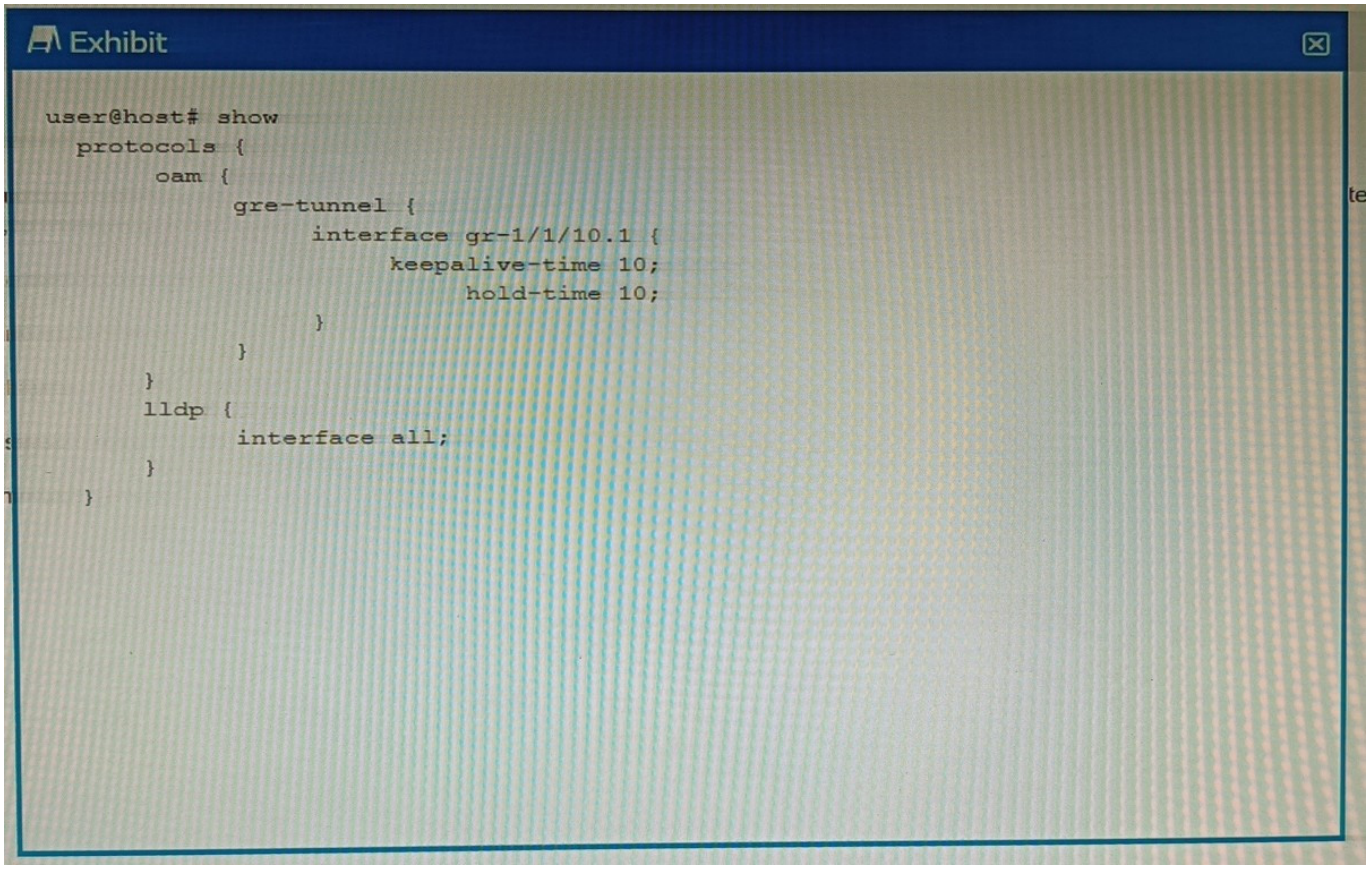
on monitoring DHCP messages to build its database1, so devices with static IP addresses that do not send DHCP messages will not have their information added.

Therefore, options B and C are correct. Options A and D are not correct because performing a DHCPRELEASE would simply remove an existing entry from the database1, and Dynamic ARP inspection (DAI) uses the information stored in the

DHCP snooping binding database but does not prevent entries from being created1.

QUESTION 4

Exhibit



You have configured a GRE tunnel. To reduce the risk of dropping traffic, you have configured a keepalive OAM probe to monitor the state of the tunnel; however, traffic drops are still occurring.

Referring to the exhibit, what is the problem?

A. For GRE tunnels, the OAM protocol requires that the BFD protocols also be used.

B. The "event link-adjacency-loss" option must be set.

C. LLDP needs to be removed from the gr-1/1/10.1 interface.

D. The hold-time value must be two times the keepalive-time value

Correct Answer: D

A keepalive OAM probe is a mechanism that can be used to monitor the state of a GRE tunnel and detect any failures in the tunnel path. A keepalive OAM probe consists of sending periodic packets from one end of the tunnel to the other and expecting a reply. If no reply is received within a specified time, the tunnel is considered down and the line protocol of the tunnel interface is changed to down1. To configure a keepalive OAM probe for a GRE tunnel, you need to specify two parameters: the keepalive-time and the hold-time. The keepalive-time is the interval between each keepalive packet sent by the local router. The hold-time is the maximum time that the local router waits for a reply from the remote router before declaring the tunnel down2. According to the Juniper Networks documentation, the hold-time value must be two times the keepalive-time value for a GRE tunnel2. This is because the hold-time value must account for both the round-trip time of the keepalive packet and the processing time of the remote router. If the hold-time value is too small, it may cause false positives and unnecessary tunnel flaps. In the exhibit, the configuration shows that the keepalive-time is set to 10 seconds and the hold-time is set to 15 seconds for the gr-1/1/10.1 interface. This means that the local router will send a keepalive packet every 10 seconds and will wait for 15 seconds for a reply from the remote router. However, this hold-time value is not two times the keepalive-time value, which violates the recommended configuration. This may cause traffic drops if the remote router takes longer than 15 seconds to reply. Therefore, option D is correct, because the hold-time value must be two times the keepalive-time value for a GRE tunnel. Option A is incorrect, because BFD is not required for GRE tunnels; BFD is another protocol that can be used to monitor tunnels, but it is not compatible with GRE keepalives3. Option B is incorrect, because the "event link- adjacency-loss" option is not related to GRE tunnels; it is an option that can be used to trigger an action when a link goes down4. Option C is incorrect, because LLDP does not need to be removed from the gr-1/1/10.1 interface; LLDP is a protocol that can be used to discover neighboring devices and their capabilities, but it does not interfere with GRE tunnels5. References:

1: Configuring Keepalive Time and Hold time for a GRE Tunnel Interface 2: keepalive | Junos OS | Juniper Networks 3: Configuring Bidirectional Forwarding Detection 4: event link-adjacency-loss | Junos OS | Juniper Networks 5: Understanding Link Layer Discovery Protocol

QUESTION 5

Which two statements about the root bridge election process are correct? (Choose two.)

A. The highest root bridge priority is preferred over lower root bridge priorities.

B. The highest root bridge identifier is preferred over lower root bridge identifiers.

C. The lowest root bridge priority is preferred over higher root bridge priorities.

D. The lowest root bridge identifier is preferred over higher root bridge identifiers.

Correct Answer: CD