JN0-649 Q&As

Enterprise Routing and Switching Professional (JNCIP-ENT)

QUESTION 1

Referring to the exhibit, you haveplaced the cos multifield classifier on all edge interfaces and configured the relevant CoS parameters. In this scenario, which two statements are correct? (Choose two.)

A. SSH traffic using the default port will be placed in the af forwarding classand accepted.

B. SSH traffic using the default port will be placed in the best-effort forwarding class and accepted.

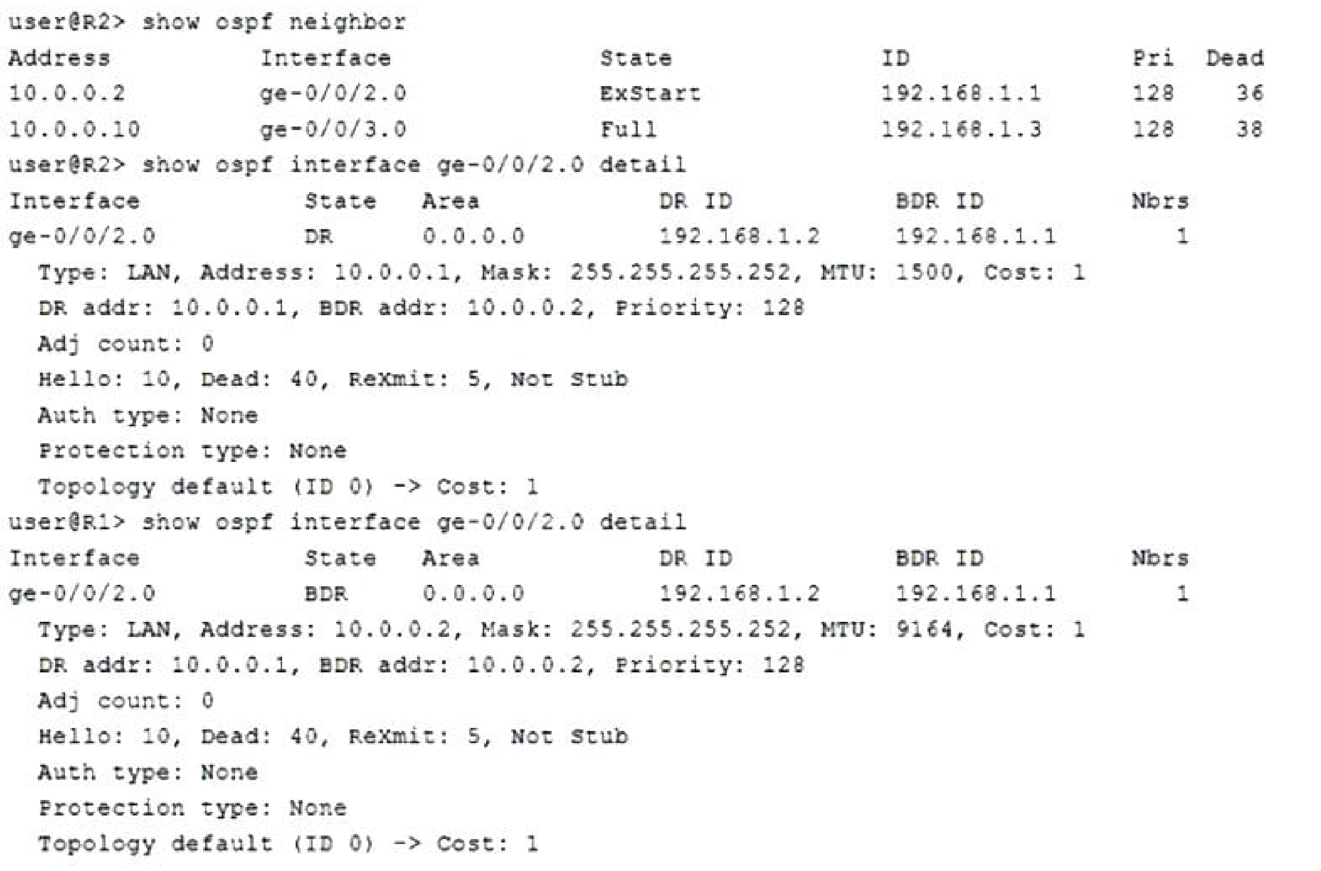
C. UDP traffic using the 16000 port will be placed in the voice forwarding class and accepted.

D. UDP traffic using the 16000 port will beplaced in the best-effort forwarding class and accepted.

Correct Answer: AC

QUESTION 2

You are running OSPF as your IGP. The interfaces connecting two routers are in the ExStart state. You notice that something is incorrect with the configuration. Referring to the exhibit, which statement is correct?



```
user@R2> show ospf neighbor
Address          Interface              State            ID               Pri  Dead
10.0.0.2         ge-0/0/2.0             ExStart          192.168.1.1      128    36
10.0.0.10        ge-0/0/3.0             Full             192.168.1.3      128    38
user@R2> show ospf interface ge-0/0/2.0 detail
Interface           State   Area            DR ID           BDR ID          Nbrs
ge-0/0/2.0          DR      0.0.0.0         192.168.1.2     192.168.1.1        1
  Type: LAN, Address: 10.0.0.1, Mask: 255.255.255.252, MTU: 1500, Cost: 1
  DR addr: 10.0.0.1, BDR addr: 10.0.0.2, Priority: 128
  Adj count: 0
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Protection type: None
  Topology default (ID 0) -> Cost: 1
user@R1> show ospf interface ge-0/0/2.0 detail
Interface           State   Area            DR ID           BDR ID          Nbrs
ge-0/0/2.0          BDR     0.0.0.0         192.168.1.2     192.168.1.1        1
  Type: LAN, Address: 10.0.0.2, Mask: 255.255.255.252, MTU: 9164, Cost: 1
  DR addr: 10.0.0.1, BDR addr: 10.0.0.2, Priority: 128
  Adj count: 0
  Hello: 10, Dead: 40, ReXmit: 5, Not Stub
  Auth type: None
  Protection type: None
  Topology default (ID 0) -> Cost: 1
```

A. The subnet mask is incorrect.

B. The MTU setting are incorrect.

C. The interface type is incorrect.

D. The IP addresses are incorrect.

Correct Answer: B

QUESTION 3

Your organization has recently acquired another company. You must carry all of the company\\'s existing VLANsacross the corporate backbone to the existing branch locations without changing addressing and with minimal configuration. Which technology will accomplish this task?

A. Q-in-Q all-in-one bundling

B. PVLAN isolated VLAN

C. MVRP registration normal

D. EVPN-VXLAN anycast gateway

Correct Answer: A

QUESTION 4

You are deploying an 802.1X solution and must determine what would happen if clients are unable to re-authenticate to the RADIUS server.

In this scenario, which configuration would provide access to the network if the supplicant is alreadyauthenticated?

A. move

B. permit

C. deny

D. sustain

Correct Answer: D

QUESTION 5

You are asked to establish interface level authentication for users connecting to your network. You must ensure that only corporate devices, identified by MAC addresses, are allowed to connect and authenticate. Authentication must be handled by a centralized server to increase scalability.

Which authentication method would satisfy this requirement?

A. MAC RADIUS

B. captive portal

C. 802.1X with single-secure supplicant mode

D. 802.1X with multiple supplicant mode

Correct Answer: A

https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/topic-map/mac-radius-authentication-switching-devices.html

You can configure MAC RADIUS authentication on an interface that also allows 802.1X authentication, or you can configure either authentication method alone.

If both MAC RADIUS and 802.1X authentication are enabled on the interface, the switch first sends the host three EAPoL requests to the host. If there is no response from the host, the switch sends the host\\'s MAC address to the RADIUS server to check whether it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the switch that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.