Juniper
JN0-649
Enterprise Routing and Switching Professional (JNCIP-ENT)

Questions&AnswersPDF

ForMoreInformation:
https://www.certswarrior.com/

Features:

- ➤ 90DaysFreeUpdates
- ➤ 30DaysMoneyBackGuarantee
- ➤ InstantDownloadOncePurchased
- ➤ 24/7OnlineChat Support
- ➤ ItsLatestVersion

Latest Version: 6.1

Question: 1

You are troubleshooting a BGP connection.
Referring to the exhibit, which two statements are correct? (Choose two.)

```
user@router> show log messages | match notification
Dec 22 19:22:29 router rpd[7394]: bgp_process_open:4185: NOTIFICATION sent to
192.168.1.4 (Internal AS 65000): code 2 (Open Message Error) subcode 2 (bad peer AS
number), Reason: peer 192.168.1.4 (Internal AS 65000) claims 65100, 65000 configured
Dec 22 19:22:33 router rpd[7394]: bgp_pp_recv:4798: NOTIFICATION sent to 192.168.1.4+
56774 (proto): code 2 (Open Message Error) subcode 2 (bad peer AS number), Reason: no
group for 192.168.1.4+56774 (proto) from AS 65100 found (peer as mismatch)in master
(ge-0/0/1.0), dropping him
Dec 22 19:23:29 router kernel: tcp_auth_ok: Packet from 192.168.1.5:64047 missing MD5
digest
Dec 22 19:23:30 router kernel: tcp_auth_ok: Packet from 192.168.1.6:56201 missing MD5
digest
---(more)---
```

A. Packet fragmentation is preventing the session from establishing.
B. The 192.168.1.5 peer has a misconfigured MD5 key.
C. The ge-0/0/1 interface is disabled.
D. The 192.168.1.4 peer has a misconfigured autonomous system number.
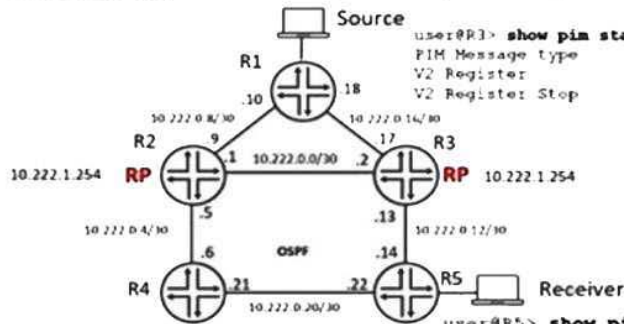
Answer: BD

Question: 2

Referring to the exhibit, anycast RP is implemented to ensure multicast service availability. The source is currently sending multicast traffic using group 239.1.1.1 and R3 is receiving PIM register messages, but R2 does not have active source information.
In this scenario, what are two methods to receive the active source information on R2? (Choose two.)

```
user@R1> show pim statistics | match "(PIM Message type)|(V2 Register)"
PIM Message type        Received        Sent  Rx errors
V2 Register                    0          857          0
V2 Register Stop               0            0          0
```

```
user@R3> show pim statistics | match "(PIM Message type)|(V2 Register)"
PIM Message type        Received        Sent  Rx errors
V2 Register                  857            0          0
V2 Register Stop               0            0          0
```

```
user@R5> show pim join
...
Group: 239.1.1.1
    Source: 10.222.3.2
    Flags: sparse,spt
    Upstream interface: ge-0/0/12.0
```

A. Configure an RP set in PIM on R1, allowing R1 to forward PIM register messages to R2 and R3 in the set.
B. Configure an MSDP protocol between R2 and R3.
C. Configure an RP set in PIM on R2 and R3, allowing the RPs to forward PIM register messages to the other RPs in the set.
D. Configure an MSDP protocol between R1 and R2.

Answer: A, C

Explanation:
https://www.juniper.net/documentation/us/en/software/junos/multicast/topics/ref/statement/rp-setedit-protocols-pim.html

Question: 3

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
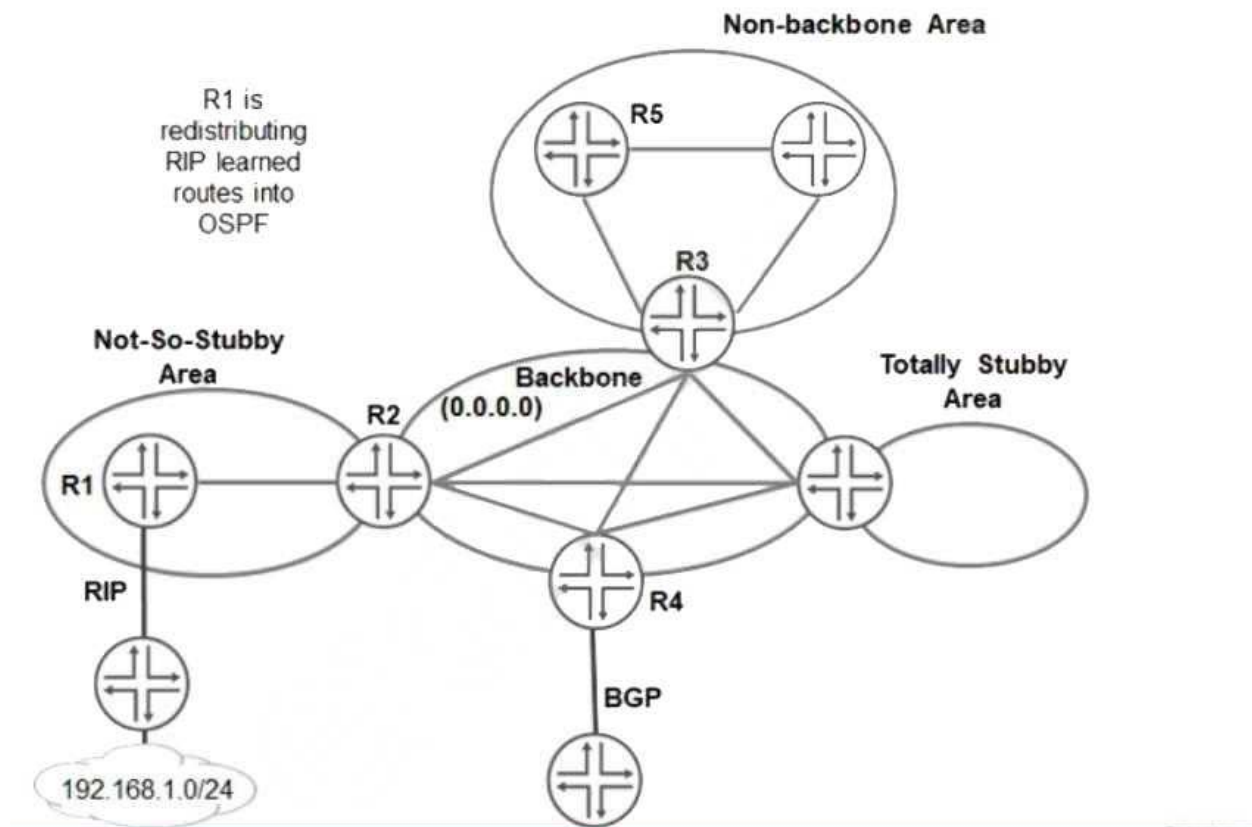D. 802.1X with multiple supplicant mode

Answer: A

Explanation:

https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/topic-map/macradius-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.

Question: 4

Referring to the exhibit, which LSA type is used to advertise 192.168.1.0/24 to R5?

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

Answer: A

Explanation:
Area-1 has no external connections. However, Area-1 has static route (172.16.31.0/24) that are not internal OSPF route. You can limit the external route advertisements to the area and advertise the static routes by designating the area an NSSA. In an NSSA, the ASBR (vMX1) generates NSSA external (Type 7) LSAs and floods them into the NSSA, where they are contained.
Type-7 LSAs allow an NSSA to support the presence of ASBR and their corresponding external routing information. The ABR (vMX2) converts Type-7 LSAs into Type-5 External LSAs and leaks them to the other areas, but external routes from other areas are not advertised within the NSSA.
An admin should check this and change it
https://www.packetswitch.co.uk/configuring-junos-ospf-stub-and-nssa-areas/
https://www.juniper.net/documentation/us/en/software/junos/ospf/topics/ref/statement/nssa-editprotocols-ospf.html

Question: 5

You enable the Multiple VLAN Registration Protocol (MVRP) to automate the creation and management of virtual LANs.
Which statement is correct in this scenario?

A. The forbidden mode does not register or declare VLANs.
B. When enabled, MVRP affects all interfaces.
C. Timers dictate when link state changes are propagated.
D. MVRP works with RSTP and VSTP.

Answer: A

Explanation:
The forbidden mode does not register or declare VLANs. You can change the registration mode of a specific interface to forbidden. An interface in forbidden registration mode does not participate in MVRP even if MVRP is enabled on the switch.
https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topicmap/mvrp.html
MVRP is disabled by default on the switches and, when enabled, affects only trunk interfaces. Once you enable MVRP, all VLAN interfaces on the switch belong to MVRP (the default normal registration mode) and those interfaces accept PDU messages and send their own PDU messages. forbidden—The interface does not register or declare VLANS (except statically configured VLANs).

CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee

Instant Download after Purchase

90 Days Free Updates

PDF Format Digital Download

24/7 Live Chat Support

Latest Syllabus Updates

For More Information – Visit link below:

https://www.certswarrior.com

16 USD Discount Coupon Code: U89DY2AQ