

DUMPS ARENA

Enterprise Routing and Switching, Specialist

Juniper JN0-348

Version Demo

Total Demo Questions: 10

Total Premium Questions: 93

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

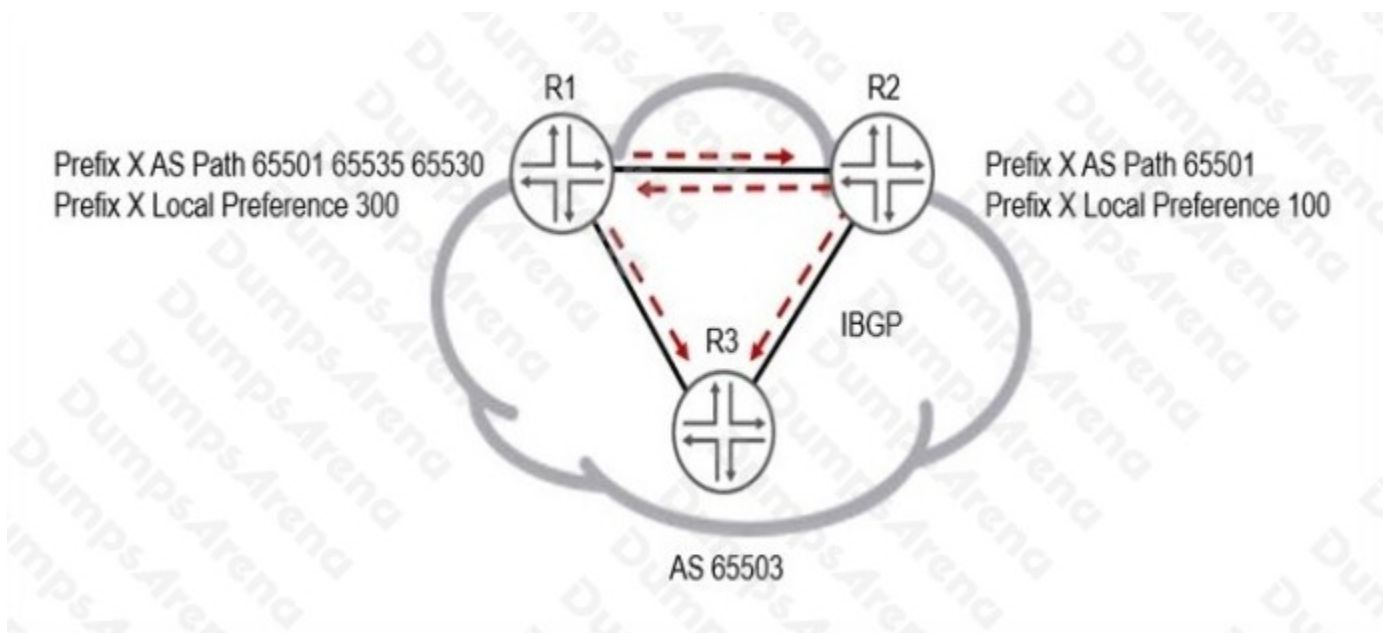
You want to use filter-based forwarding (FBF) to forward traffic sourced from subnet 10.0.0.0/24 to a specific destination. Which two routing instance types would enable you to accomplish this task? (Choose two.)

- A. virtual switch
- B. virtual routing and forwarding
- C. virtual router
- D. forwarding

ANSWER: C D

QUESTION NO: 2

Click the Exhibit button.



Both the R1 and R2 devices are advertising prefix X into AS 65503 with the BGP attributes shown in the exhibit.

Which statement is correct in this scenario?

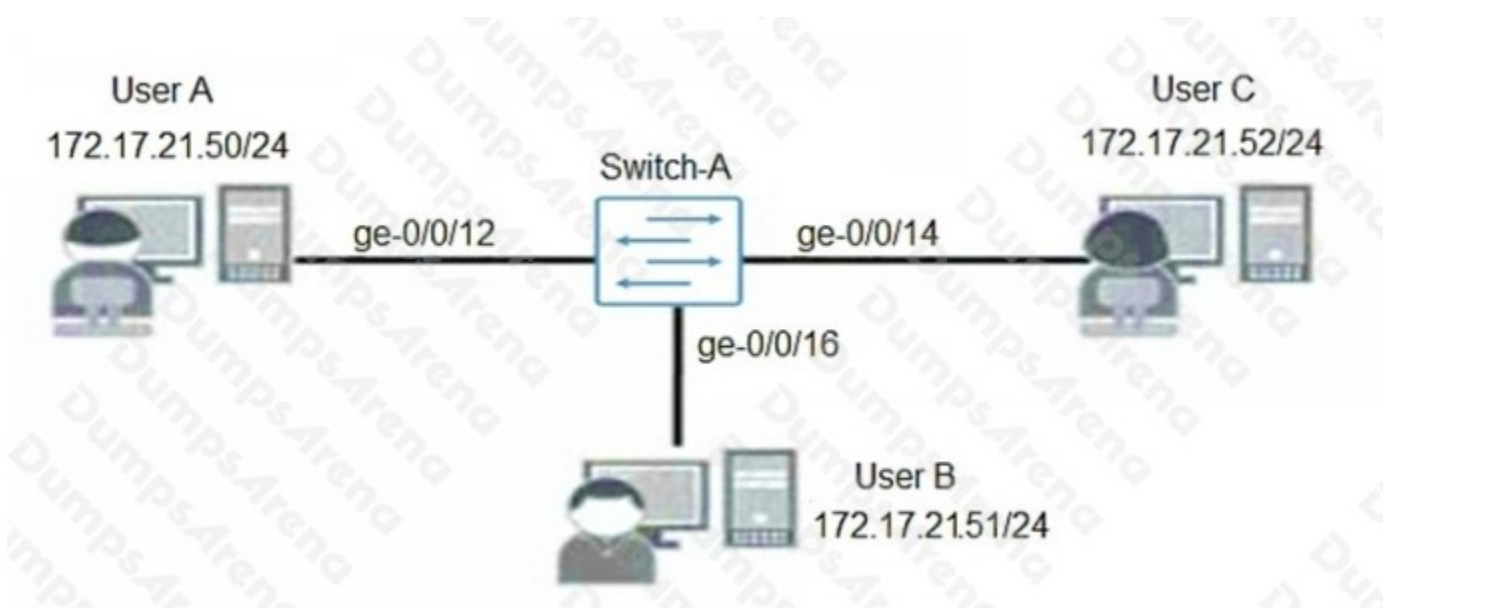
- A. R2's version of prefix X will be active because of the local preference attribute.
- B. R1's version of prefix X will be active because of the local preference attribute.

- C. R1's version of prefix X will be active because of the AS path attribute.
- D. R2's version of prefix X will be active because of the AS path attribute.

ANSWER: D

QUESTION NO: 3

Click the Exhibit button.



In the exhibit, each IP subnet in the network is associated with a unique VLAN ID.

Which action will ensure that Host C will communicate with Host A and Host B?

- A. Configure an IRB interface for each VLAN and associate it with its corresponding VLAN
- B. Configure a port-based ACL that permits inter-VLAN routing for all configured VLANs
- C. Configure all switch ports connecting to the host devices as trunk ports associated with all VLANs
- D. Configure all switch ports connecting to the host devices as access ports associated with a common VLAN

ANSWER: A

QUESTION NO: 4

Click the Exhibit button.

```
[edit routing-options]
user@host# show
static {
  defaults {
    preference 180;
  }
  route 0.0.0.0/0 {
    next-hop 172.30.25.1;
    qualified-next-hop 172.30.25.5 {
      preference 7;
    }
  }
}
```

Which statement is true about the configuration shown in the exhibit?

- A. The preference for the 172.30.25.1 next hop is 5.
- B. The preferred next hop is 172.30.25.5.
- C. The preference for the 172.30.25.1 next hop is 7.
- D. 172.30.25.1 is the preferred next hop.

ANSWER: B

QUESTION NO: 5

Your network is configured with dynamic ARP inspection (DAI) using the default parameters for all the DHCP and ARP related configurations. You just added a new device connected to a trunk port and configured it to obtain an IP address using DHCP.

Which two statements are correct in this scenario? (Choose two.)

- A. The DHCP server assigns the IP addressing information to the new device.
- B. DAI validates the ARP packets for the new device against the DHCP snooping database.

- C. The ARP request and response packets for the new device will bypass DAI.
- D. DHCP snooping adds the DHCP assigned IP address for the new device to its database.

ANSWER: A B

QUESTION NO: 6

Click the Exhibit button.

```
Nov  3 15:39:56.388955 SPF post spf cleanup finished
Nov  3 15:39:56.388959 Cleanup elapsed time 0.000064s
Nov  3 15:39:56.388965 Total elapsed time 0.003092s
Nov  3 15:39:56.388967 Finished full SPF refresh for topology default
Nov  3 15:39:56.388969 task_job_delete: delete background job Route recal
timer for task OSPF
Nov  3 15:39:56.388971 background dispatch completed job Route recalc timer
for task OSPF
Nov  3 15:40:02.900115 task_process_events: rcv ready for OSPF
I/O./var/run/ppmd_control
Nov  3 15:40:02.900227 task_process_events: rcv ready for OSPF
I/O./var/run/ppmd_control
Nov  3 15:40:02.900242 task_timer_uset: timer OSPF
I/O./var/run/ppmd_control_PFM Hold <Touched> set to offset 2:00 at 15:42:02
Nov  3 15:40:02.900244 OSPF packet ignored: area mismatch (0.0.0.1) from
192.168.150.254 on intf ge-0/0/1.0 area 1.0.0.0
Nov  3 15:40:02.900246 OSPF rcvd Hello 192.168.150.254 -> 224.0.0.5 (ge-
0/0/1.0 IFL 72 area 1.0.0.0)
Nov  3 15:40:02.900344 Version 2, length 44, ID 10.254.254.254, area 0.0.0.1
Nov  3 15:40:02.900346 checksum 0x8a7a, authtype 0
Nov  3 15:40:02.900348 mask 255.255.255.0, hello_ivl 10, opts 0x12, prio 128
Nov  3 15:40:02.900350 dead_ivl 40, DR 192.168.150.254, BDR 0.0.0.0
Nov  3 15:40:02.900374 task_timer_uset: timer OSPF_internal timer <Touched>
set to offset 5 at 15:40:07
Nov  3 15:40:04.225141 task_process_events: rcv ready for OSPF
I/O./var/run/ppmd_control
Nov  3 15:40:04.225293 task_process_events: rcv ready for OSPF
I/O./var/run/ppmd_control
Nov  3 15:40:04.225350 task_timer_uset: timer OSPF
I/O./var/run/ppmd_control_PFM Hold <Touched> set to offset 2:00 at 15:42:04
Nov  3 15:40:04.225352 OSPF periodic xmit from 192.168.150.253 to 224.0.0.5
(IFL 72 area 1.0.0.0)
Nov  3 15:40:06.025582 task_process_events: rcv ready for OSPF
I/O./var/run/ppmd_control
Nov  3 15:40:06.025685 task_process_events: rcv ready for OSPF
I/O./var/run/ppmd_control
Nov  3 15:40:06.025713 task_timer_uset: timer OSPF
I/O./var/run/ppmd_control_PFM Hold <Touched> set to offset 2:00 at 15:42:06
Nov  3 15:40:06.025715 OSPF periodic xmit from 172.16.128.253 to 224.0.0.5
(IFL 71 area 1.0.0.0)
```

Based on the traceoptions output shown in the exhibit, what is the problem with the adjacency?

- A.** connectivity
- B.** authentication mismatch
- C.** MTU mismatch
- D.** area mismatch

ANSWER: D

QUESTION NO: 7

Click the Exhibit button.

```
user@router> show bgp neighbor 192.168.200.2
Peer: 192.168.200.2+179 AS 11685 Local: 192.168.200.1+49469 AS 7029
  Type: External      State: Established      Flags: <ImportEval Sync>
  Last State: OpenConfirm  Last Event: RecvKeepAlive
  Last Error: None
  Options: <Preference AddressFamily PeerAS LocalAS Rib-group Refresh>
  Address families configured: inet-unicast inet-vpn-unicast 12vpn-signaling
  Holdtime: 90 Preference: 170 Local AS: 7029 Local System AS: 0
  Number of flaps: 0
  Peer ID: 10.8.241.31      Local ID: 10.8.241.30      Active Holdtime: 90
  Keepalive Interval:30      Group index: 0      Peer index: 0
  BFD: disabled, down
  Local Interface: xe-0/2/3.0
  NLRI for restart configured on peer: inet-unicast inet-vpn-unicast 12vpn
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Stale routes from peer are kept for: 300
  Peer does not support Restarter functionality
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 11685)
  Peer does not support Addpath
  Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
    Active prefixes:          0
    Received prefixes:        0
    Accepted prefixes:        0
    Suppressed due to damping: 0
    Advertised prefixes:      0
  Last traffic (seconds): Received 17 Sent 17 Checked 17
  Input messages: Total 2 Updates 1 Refreshes 0 Octets 42
  Output messages: Total 3 Updates 0 Refreshes 0 Octets 136
  Output Queue[0]: 0
```

Your router is configured to peer with your ISP's router using BGP. You can only control your BGP configuration.

Which address families are negotiated between the two BGP peers shown in the exhibit?

- A. inet-unicast inet-vpn-unicast 12vpn-signaling
- B. inet-unicast
- C. inet-vpn-unicast
- D. inet-unicast inet-vpn-unicast 12vpn

ANSWER: B

QUESTION NO: 8

What are two interarea OSPF LSA types? (Choose two.)

- A. Type 1 router LSAs
- B. Type 3 summary LSAs
- C. Type 4 ASBR summary LSAs
- D. Type 2 network LSAs

ANSWER: B C

QUESTION NO: 9

Which two situations would cause dynamic ARP inspection to drop traffic? (Choose two.)

- A. if no IP-to-MAC address entry exists in the DHCP snooping database
- B. if the IP address in the ARP packet is deemed invalid
- C. if the requested MAC address exceeds the configured limit on the port
- D. if the ARP packet comes from a port that has been configured as trusted

ANSWER: A B

QUESTION NO: 10

You have a conference room with an open network port that is used by employees to connect to the network. You are concerned about rogue switches being connected to this port.

Which two features should you enable on your switch to limit access to this port? (Choose two.)

- A. DHCP snooping
- B. dynamic ARP inspection
- C. MAC limiting
- D. 802.1X

ANSWER: A B