



# JN0-347<sup>Q&As</sup>

Enterprise Routing and Switching, Specialist (JNCIS-ENT)

## Pass Juniper JN0-347 Exam with 100% Guarantee

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

<https://www.passapply.com/jn0-347.html>

100% Passing Guarantee  
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

Switch-1 in the exhibit receives a packet from User A with a destination MAC address of 00:26:88:02:74:47.

Which statement is correct in this scenario?

A.

Switch-1 floods the packet out ge-0/0/6, ge-0/0/7, ge-0/0/8, and ge-0/0/9.

B.

Switch-1 floods the packet out ge-0/0/7 and ge-0/0/8.

C.

Switch-1 floods the packet out ge-0/0/7, ge-0/0/8, and ge-0/0/9.

D.

Switch-1 sends the packet out ge-0/0/7 only.

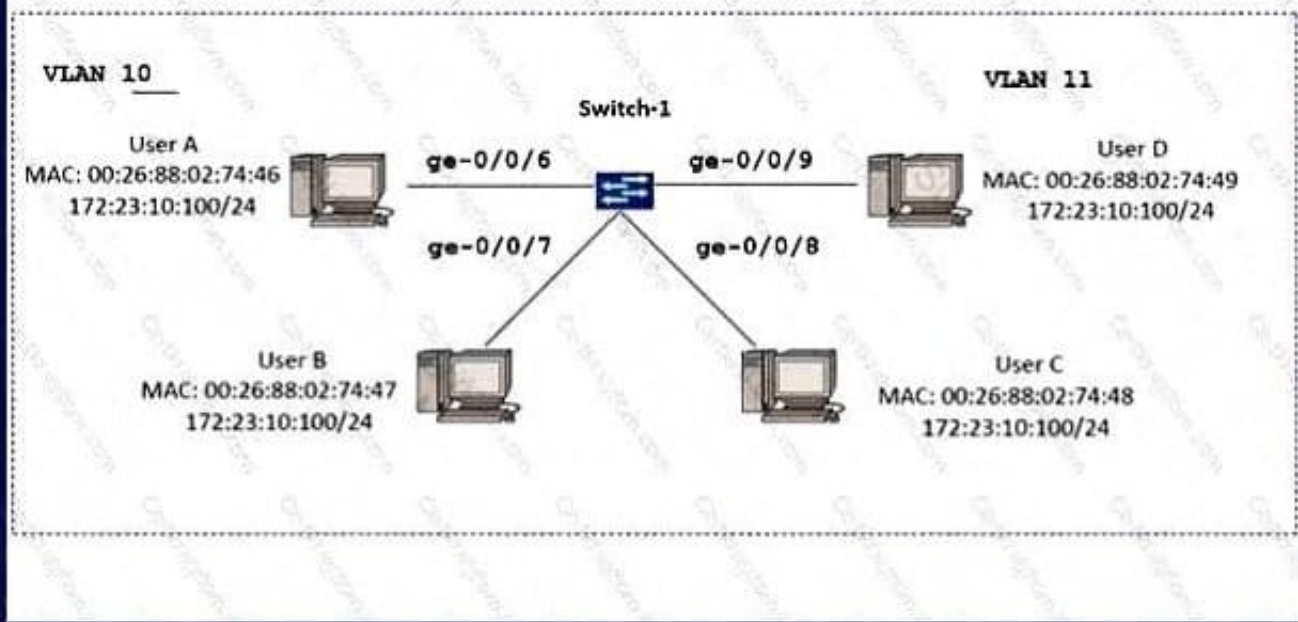


## Exhibit



Switch-1's Bridge Table

VLAN	MAC Address	Interface
10	00:26:88:02:74:46	ge-0/0/6
11	00:26:88:02:74:49	ge-0/0/9



Correct Answer: C

To forward a frame destined to that specific mac -address, it will know out of which port to send the frame. Flooding however occurs when the switch does not know of the destination mac - address? say the switch has not learnt that mac address yet; or maybe that specific entry expired so it got flushed away from the mac-address table. To ensure the frame reaches its intended destination, the switch will replicate that frame out of all ports, less the port where the frame was received that's flooding.

## QUESTION 2

You are a service provider and have multiple customers in a building. You are installing a new switch that can host all of your customers. However, you would like to ensure that one customer cannot see or broadcast to another customer. You would also like to have them use a common gateway IP address from the building. What should be used to provide



this access?

- A. VLAN
- B. private VLAN
- C. filter-based VLAN
- D. Layer 2 tunneling

Correct Answer: B

### QUESTION 3

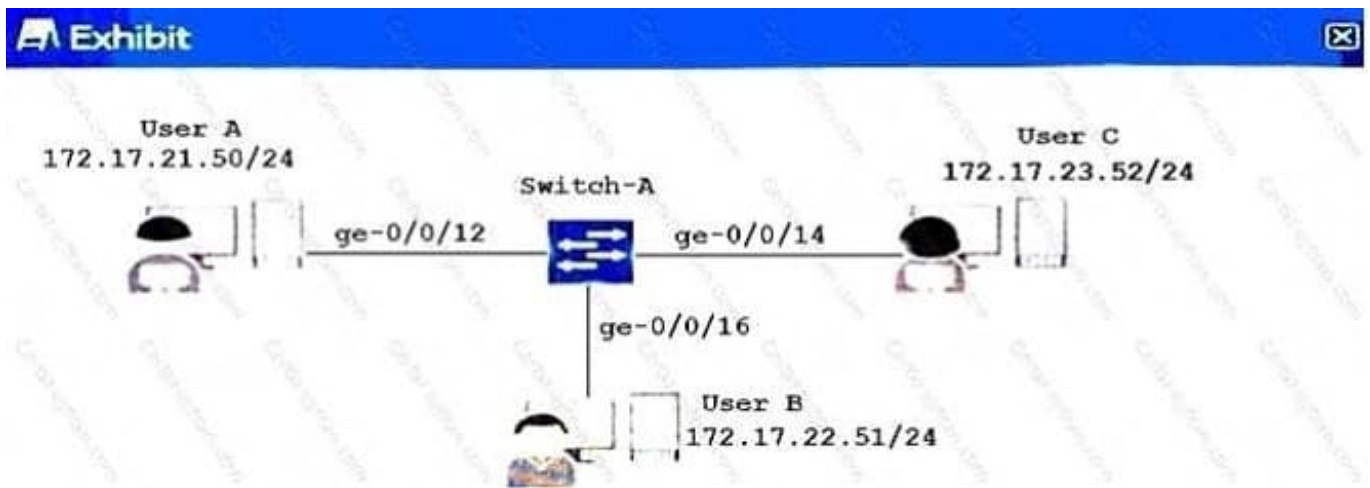
Which Junos feature allows you to combine multiple interfaces into a single bundle?

- A. VRRP
- B. Virtual Chassis
- C. LAG
- D. NSB

Correct Answer: C

### QUESTION 4

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 all switch ports connecting to the host devices as access ports associated with a common VLAN.
- B. Configure an IRB interface for each VLAN and associate it with its corresponding VLAN.
- C. Configure all switch ports connecting to the host devices as trunk ports associated with all VLANs.



D. Configure a port-based ACL that permits inter-VLAN routing for all configured VLANs.

Correct Answer: B

Configuring Routing Between VLANs on One Switch To segment traffic on a LAN into separate broadcast domains, you create separate virtual LANs (VLANs). Of course, you also want to allow these employees to communicate with people and resources in other VLANs. To forward packets between VLANs you normally you need a router that connects the VLANs. However, you can accomplish this on a Juniper Networks switch without using a router by configuring an integrated routing and bridging (IRB) interface (also known as a routed VLAN interface-- or RVI-- in versions of Junos OS that do not support Enhanced Layer 2 Software).

---

#### QUESTION 5

Which two port security features are dependent on the DHCP snooping database? (Choose two.)

- A. MAC limiting
- B. dynamic ARP inspection
- C. IP source guard
- D. storm control

Correct Answer: BC

B: Dynamic ARP inspection (DAI) prevents Address Resolution Protocol (ARP) spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made on the basis of the results of those comparisons.

C: IP source guard mitigates the effects of IP address spoofing attacks on the Ethernet LAN. With IP source guard enabled, the source IP address in the packet sent from an untrusted access interface is validated against the SourceDSN MAC address in the DHCP snooping database. The packet is forwarded if the source IP-MAC binding is valid; if the binding is not valid, the packet is discarded. You enable IP source guard on a VLAN. EX Series switches support IPv6 source guard also.

[Latest JN0-347 Dumps](#)

[JN0-347 PDF Dumps](#)

[JN0-347 VCE Dumps](#)