



NSE7_SAC-6.2^{Q&As}

Fortinet NSE 7 - Secure Access 6.2

Pass Fortinet NSE7_SAC-6.2 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse7_sac-6-2.html

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

Refer to the exhibit.

Examine the packet capture shown in the exhibit, which contains a RADIUS access request packet sent by FortiSwitch to a RADIUS server.

```
> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
> Ethernet II, Src: Vmware_96:70:b5 (00:50:56:96:70:b5), Dst: Vmware_96:d8:76 (00:50:56:96:d8:76)
> Internet Protocol Version 4, Src: 10.0.1.254, Dst: 10.0.1.150
> User Datagram Protocol, Src Port: 48704, Dst Port: 1812
✓ RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x96 (150)
  Length: 122
  Authenticator: 49a700a9981a2eb044bf811f482412a0
  [The response to this request is in frame 2]
  ✓ Attribute Value Pairs
    > AVP: l=18 t=NAS-Identifier(32): S124DP3X16008048
    > AVP: l=19 t=User-Name(1): 00-E0-4C-36-0D-5E
    > AVP: l=34 t=User-Password(2): Encrypted
    > AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
    > AVP: l=19 t=Calling-Station-Id(31): 00-E0-4C-36-0D-5E
    > AVP: l=6 t=Service-Type(6): Call-Check(10)
```

Why does the User-Name field in the RADIUS access request packet contain a MAC address?

- A. The FortiSwitch interface is configured for 802.1X port authentication with MAC address bypass, and the connected device does not support 802.1X.
- B. FortiSwitch authenticates itself using its MAC address as the user name.
- C. The connected device is doing machine authentication.
- D. FortiSwitch is replying to an access challenge packet sent by the RADIUS server and requesting the client MAC address.

Correct Answer: D

QUESTION 2

What does DHCP snooping MAC verification do?

- A. Drops DHCP release packets on untrusted ports
- B. Drops DHCP packets with no relay agent information (option 82) on untrusted ports
- C. Drops DHCP offer packets on untrusted ports



D. Drops DHCP packets on untrusted ports when the client hardware address does not match the source MAC address

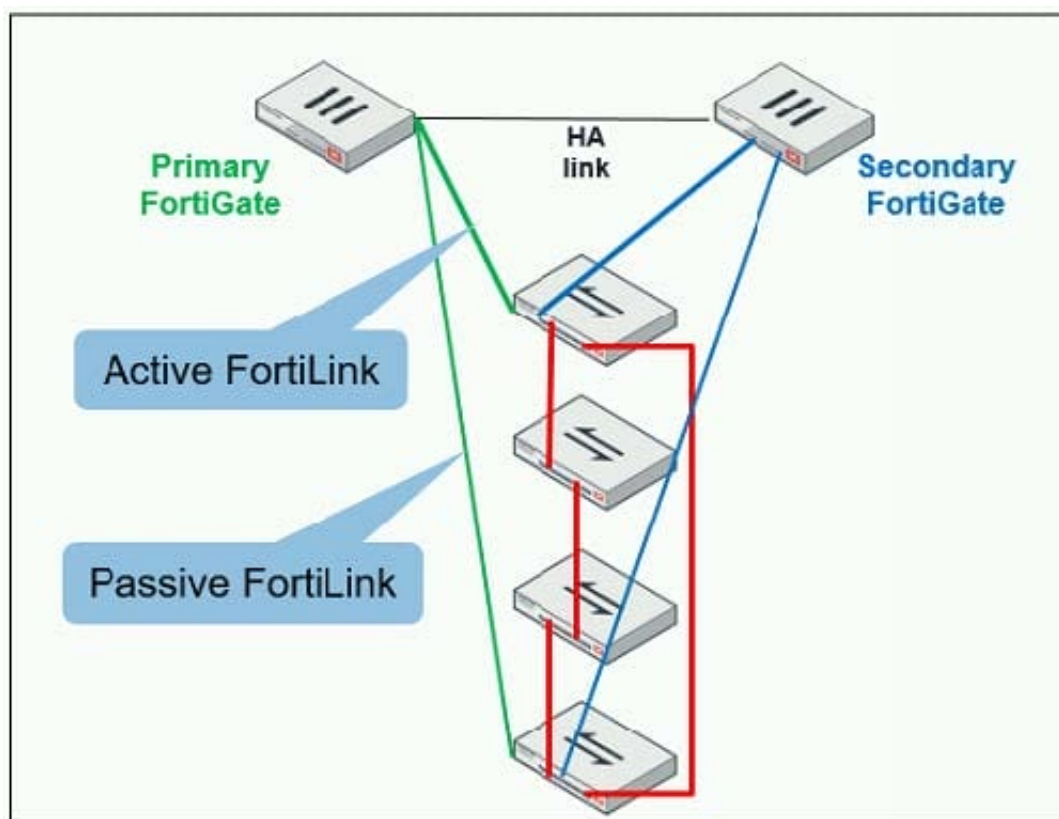
Correct Answer: D

Reference: <https://docs.fortinet.com/document/fortiswitch/6.4.2/administration-guide/335964/dhcpsnooping> (note)

QUESTION 3

Refer to the exhibit.

The exhibit shows two FortiGate devices in active-passive HA mode, including four FortiSwitch devices connected to a ring.



Which two configurations are required to deploy this network topology? (Choose two.)

- A. Configure link aggregation interfaces on the FortiLink interfaces.
- B. Configure the trunk interfaces on the FortiSwitch devices as MCLAG-ISL.
- C. Enable `fortilink-split-interface` on the FortiLink interfaces.
- D. Enable STP on the FortiGate interfaces.

Correct Answer: CD

Reference: <https://www.fortinetguru.com/2019/07/fortilink-configuration-using-the-fortigate-gui/>

**QUESTION 4**

Examine the following output from the FortiLink real-time debug.

```
FortiGate# diagnose debug application fortilinkd 3
fl_node_apply_switch_port_fgt_properties_update_with_portname[977]:port properties are different for
port(port9) in switch(FS108D3W17002387) old(0x1) new(0x1)o-peer-port() n-peer-port(port2) o-peer-device() n-
peer-device(FGVMEVBB6ITDAO1B)
... flp_event_handler[605]:node: port2 received event 110 state FL_STATE_READY switchname flags 0x26a
... flp_event_handler[605]:node: port2 received event 111 state FL_STATE_READY switchname flags 0x26a
... flp_send_pkt[339]:pkt-sent {type(5) flag=0xe2 node(port2) sw(port2) len(26)smac: 0: c:29:51:dd:a0
dmac:70:4c:a5:24:ba:4f
```

Based on the output, what is the status of the communication between FortiGate and FortiSwitch?

- A. FortiGate is unable to authorize the FortiSwitch.
- B. FortiGate is unable to establish FortiLink tunnel to manage the FortiSwitch.
- C. FortiGate is unable to located a previously managed FortiSwitch.
- D. The FortiLink heartbeat is up.

Correct Answer: D

QUESTION 5

Refer to the exhibit.

Examine the output of the debug command and port configuration shown in the exhibit.



Debug command output

```
# diagnose switch-controller switch-info mac-table
FS108D3W17002387      0 :
    MAC address      Interface      vlan
=====
78:2b:cb:d8:36:68    port1      4094
```

Port configuration

```
config switch-controller managed-switch
  edit FS108D3W17002387
    config ports
      edit port1
        set learning-limit 1
        set discard-mode all-tagged
        set arp-inspection-trust untrusted
      end
    end
```

FortiGate learned the MAC address 78:2b:cb:d8:36:68 dynamically.

What action does FortiSwitch take if there is an untagged frame coming to port1 will different MAC address?

- A. The frame is accepted and assigned to the quarantine VLAN.
- B. The frame is accepted and FortiSwitch will update its mac address table with the new MAC address.
- C. The frame is dropped.
- D. The frame is accepted and assigned to the user VLAN.

Correct Answer: A

[NSE7_SAC-6.2 PDF Dumps](#)

[NSE7_SAC-6.2 Practice
Test](#)

[NSE7_SAC-6.2 Exam
Questions](#)