



# NSE7\_SAC-6.2<sup>Q&As</sup>

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.passapply.com/nse7\\_sac-6-2.html](https://www.passapply.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.

```
config wireless-controller wtp-profile
edit "Main Networks - FAP-320C"
    set comment "Profile with standard networks"
    config platform
        set type 320C
    end
    set handoff-rssi 30
    set handoff-sta-thresh 30
    set ap-country GB
    set allowaccess https ssh
    set login-passwd-change yes
    config radio-1
        set band 802.11n,g-only
        set channel-utilization enable
        set wids-profile "default-wids-apscan-enabled"
        set darrp enable
        set frequency-handoff enable
        set ap-handoff enable
        set vap-all disable
        set vaps "Guest" "Corporate"
        set channel "1" "6" "11"
    end
    config radio-2
        set band 802.11ac
        set channel-bonding 40MHz
        set channel-utilization enable
        set wids-profile "default-wids-apscan-enabled"
        set darrp enable
        set frequency-handoff enable
        set ap-handoff enable
        set vap-all disable
        set vaps "Guest" "Corporate"
        set channel "36" "44" "52"
    end
end
next
end
```

In the WTP profile configuration shown in the exhibit, the AP profile is assigned to two FAP-320 APs that are installed in an open plan office.

1.

The first AP has 32 clients associated to the 5GHz radios and 22 clients associated to the 2.4GHz radio.

2.

The second AP has 12 clients associated to the 5GHz radios and 20 clients associated to the 2.4GHz radio.



A dual band-capable client enters the office near the first AP and the first AP measures the new client at -33 dBm signal strength. The second AP measures the new client at -43 dBm signal strength.

In the new client attempts to connect to the corporate wireless network, to which AP radio will the client be associated?

- A. The second AP 5GHz interface.
- B. The first AP 2.4GHz interface.
- C. The first AP 5GHz interface.
- D. The second AP 2.4GHz interface.

Correct Answer: A

---

## QUESTION 2

Which two EAP methods can use MSCHAPV2 for client authentication? (Choose two.)

- A. PEAP
- B. EAP-TTLS
- C. EAP-TLS
- D. EAP-GTC

Correct Answer: AC

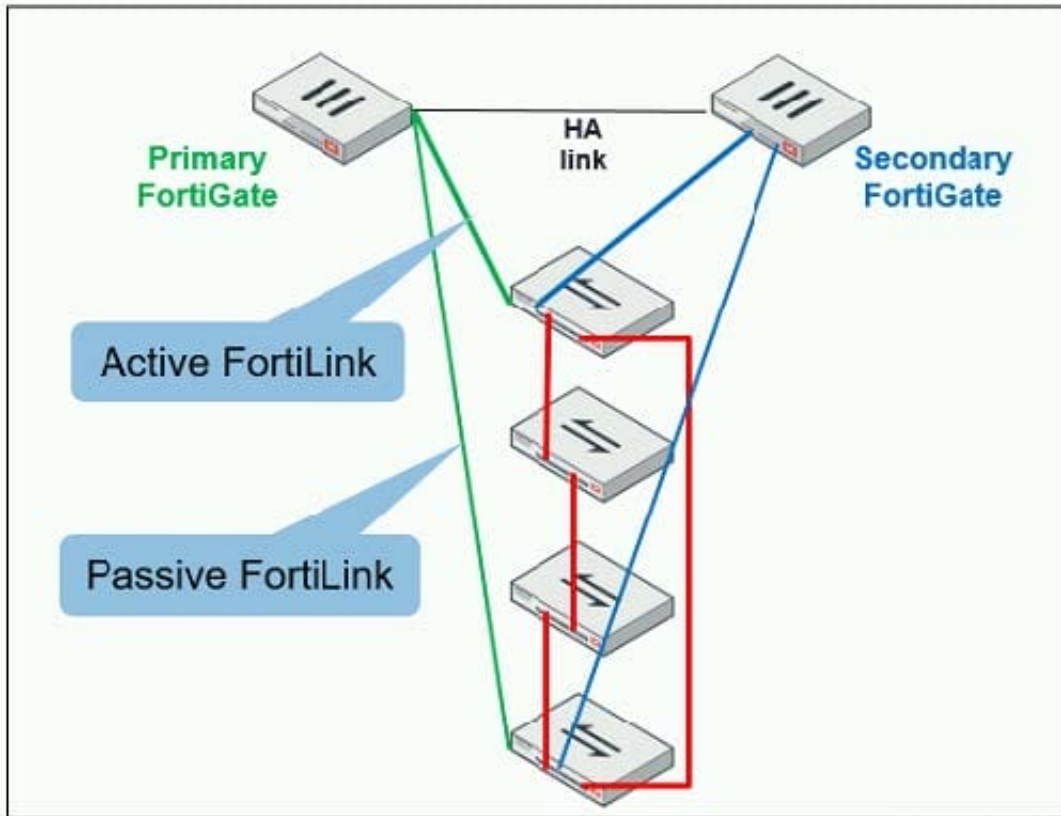
Reference: [https://help.fortinet.com/fauth/3-3/Content/FortiAuthenticator%203\\_3%20Admin%20Guide/500/501\\_EAP.htm](https://help.fortinet.com/fauth/3-3/Content/FortiAuthenticator%203_3%20Admin%20Guide/500/501_EAP.htm)

---

## 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

Refer to the exhibit.



```
FortiGate # diagnose switch-controller switch-info 802.1X
Managed Switch : S224EPTF18001736

port2 : Mode: port-based (mac-by-pass disable)
Link: Link up
Port State: unauthorized: ( )
Dynamic Authorized Vlan : 0
EAP pass-through mode : Enable
Quarantine VLAN (4093) detection : Enable
Native Vlan : 10
Allowed Vlan list: 10,4093
Untagged Vlan list: 4093
Guest VLAN :
Auth-Fail Vlan :

Sessions info:
00:09:0f:02:02:02      Type=802.1x,,state=AUTHENTICATING,etime=0,eap_cnt=0 params:reAuth=3600
```

A host machine connected to port2 on FortiSwitch cannot connect to the network. All ports on FortiSwitch are assigned a security policy to enforce 802.1X port authentication. While troubleshooting the issue, the administrator runs the debug command and obtains the output shown in the exhibit.

Which two scenarios are the likely cause of this issue? (Choose two.)

- A. The host machine is not configured for 802.1X port authentication.
- B. The host machine does not support 802.1X authentication.
- C. The host machine is quarantined due to a security incident.
- D. The host machine is configured with wrong VLAN ID.

Correct Answer: AB

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46428>

## 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 VCE Dumps](#)

[NSE7\\_SAC-6.2 Study Guide](#)

[NSE7\\_SAC-6.2 Exam Questions](#)