Free Questions for NSE6_FWF-6.4 by certsinside

Shared by Acevedo on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

How are wireless clients assigned to a dynamic VLAN configured for hash mode?

Options:

A- Using the current number of wireless clients connected to the SSID and the number of IPs available in the least busy VLAN

B- Using the current number of wireless clients connected to the SSID and the number of clients allocated to each of the VLANs

C- Using the current number of wireless clients connected to the SSID and the number of VLANs available in the pool

D- Using the current number of wireless clients connected to the SSID and the group the FortiAP is a member of

Answer:

C

Explanation:

VLAN from the VLAN pool based on a hash of the current number of SSID clients and the number of entries in the VLAN pool.

Question 2

Question Type: MultipleChoice

Which statement is correct about security profiles on FortiAP devices?

Options:

A- Security profiles on FortiAP devices can use FortiGate subscription to inspect the traffic

B- Only bridge mode SSIDs can apply the security profiles

C- Disable DTLS on FortiAP

D- FortiGate performs inspection the wireless traffic

Answer:

B

Question 3

Question Type: MultipleChoice

When deploying a wireless network that is authenticated using EAP PEAP, which two configurations are required? (Choose two.)

Options:

A- An X.509 certificate to authenticate the client

B- An X.509 to authenticate the authentication server

C- A WPA2 or WPA3 personal wireless network

D- A WPA2 or WPA3 Enterprise wireless network

Answer:

B, D

Question 4

Question Type: **MultipleChoice**

What is the first discovery method used by FortiAP to locate the FortiGate wireless controller in the default configuration?

Options:

A- DHCP

B- Static

C- Broadcast

D- Multicast

Answer:

B

Question 5

Question Type: **MultipleChoice**

A tunnel mode wireless network is configured on a FortiGate wireless controller.

Which task must be completed before the wireless network can be used?

Options:

A- The wireless network interface must be assigned a Layer 3 address

B- Security Fabric and HTTPS must be enabled on the wireless network interface

C- The wireless network to Internet firewall policy must be configured

D- The new network must be manually assigned to a FortiAP profile.

Answer:

C

Explanation:

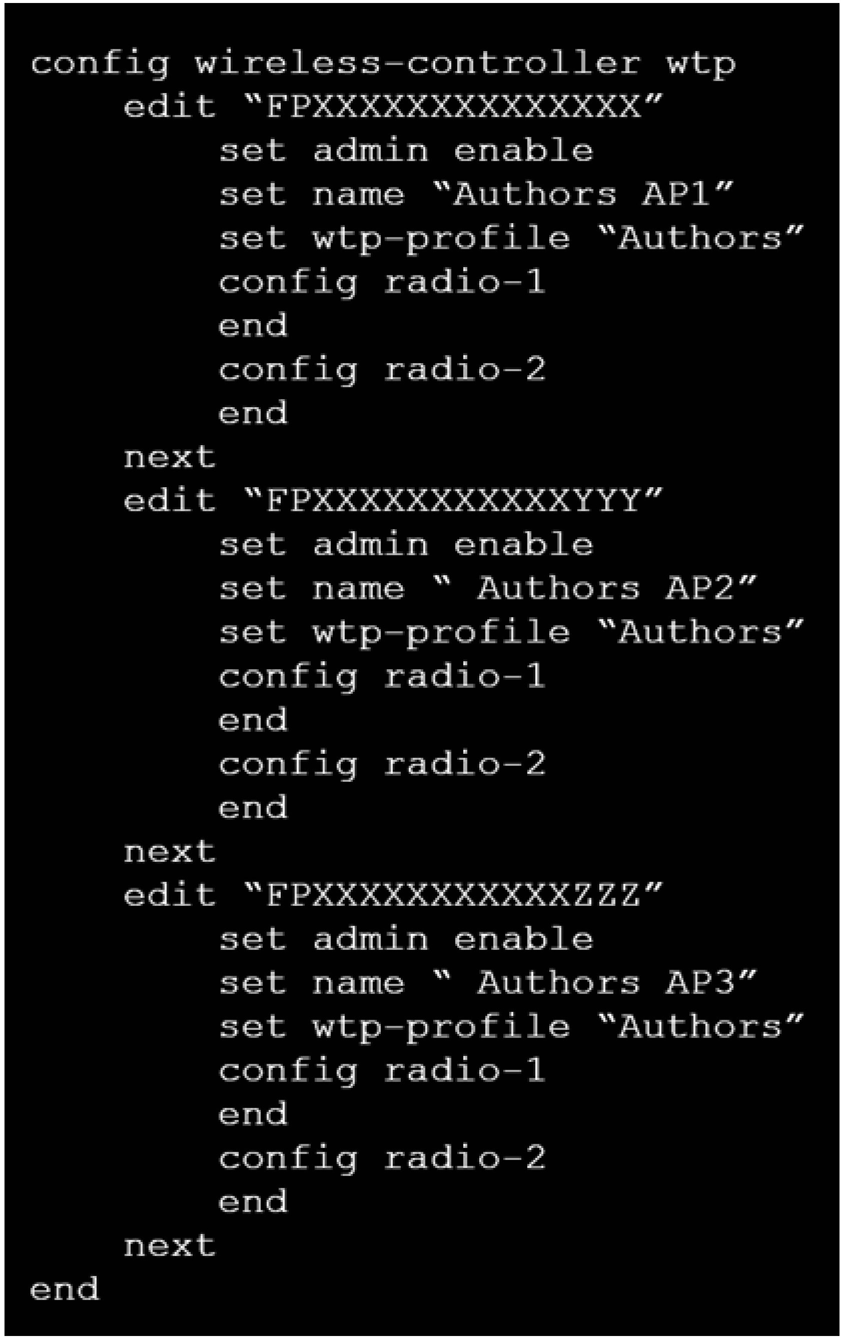
A FortiGate unit is an industry leading enterprise firewall. In addition to consolidating all the functions of a network firewall, IPS, anti-malware, VPN, WAN optimization, Web filtering, and application control in a single platform, FortiGate also has an integrated Wi-Fi controller.

Question 6

Question Type: **MultipleChoice**

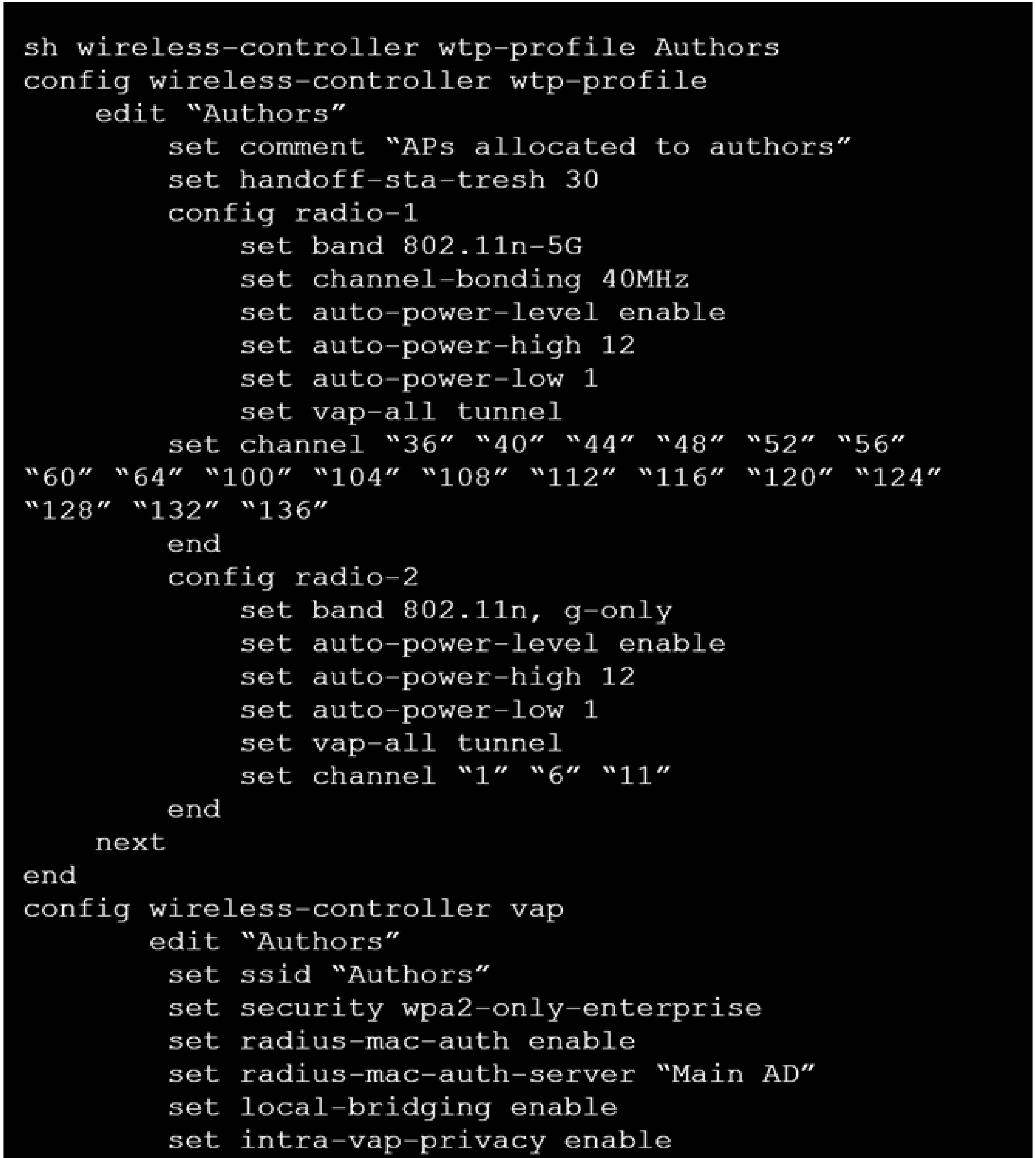
Refer to the exhibits.

Exhibit A



```
config wireless-controller wtp
    edit “FPXXXXXXXXXXXXX”
        set admin enable
        set name “Authors AP1”
        set wtp-profile “Authors”
        config radio-1
        end
        config radio-2
        end
    next
    edit “FPXXXXXXXXXXYYY”
        set admin enable
        set name “ Authors AP2”
        set wtp-profile “Authors”
        config radio-1
        end
        config radio-2
        end
    next
    edit “FPXXXXXXXXXXZZZ”
        set admin enable
        set name “ Authors AP3”
        set wtp-profile “Authors”
        config radio-1
        end
        config radio-2
        end
    next
end
```

Exhibit B



```
sh wireless-controller wtp-profile Authors
config wireless-controller wtp-profile
    edit “Authors”
        set comment “APs allocated to authors”
        set handoff-sta-tresh 30
        config radio-1
            set band 802.11n-5G
            set channel-bonding 40MHz
            set auto-power-level enable
            set auto-power-high 12
            set auto-power-low 1
            set vap-all tunnel
        set channel “36” “40” “44” “48” “52” “56”
“60” “64” “100” “104” “108” “112” “116” “120” “124”
“128” “132” “136”
        end
        config radio-2
            set band 802.11n, g-only
            set auto-power-level enable
            set auto-power-high 12
            set auto-power-low 1
            set vap-all tunnel
            set channel “1” “6” “11”
        end
    next
end
config wireless-controller vap
       edit “Authors”
        set ssid “Authors”
        set security wpa2-only-enterprise
        set radius-mac-auth enable
        set radius-mac-auth-server “Main AD”
        set local-bridging enable
        set intra-vap-privacy enable
```

A wireless network has been created to support a group of users in a specific area of a building. The wireless network is configured but users are unable to connect to it. The exhibits show the relevant controller configuration for the APs and the wireless network.

Which two configuration changes will resolve the issue? (Choose two.)

Options:

A- For both interfaces in the wtp-profile, configure set vaps to be ''Authors''

B- Disable intra-vap-privacy for the Authors vap-wireless network

C- For both interfaces in the wtp-profile, configure vap-all to be manual

D- Increase the transmission power of the AP radio interfaces

Answer:

A, C

Question 7

Question Type: **MultipleChoice**

As a network administrator, you are responsible for managing an enterprise secure wireless LAN. The controller is based in the United States, and you have been asked to deploy a number of managed APs in a remote office in Germany.

What is the correct way to ensure that the RF channels and transmission power limits are appropriately configured for the remote APs?

Options:

A- Configure the APs individually by overriding the settings in Managed FortiAPs

B- Configure the controller for the correct country code for Germany

C- Clone a suitable FortiAP profile and change the county code settings on the profile

D- Create a new FortiAP profile and change the county code settings on the profile

Answer:

C

Question 8

Question Type: MultipleChoice

Which of the following is a requirement to generate analytic reports using on-site FortiPresence deployment?

Options:

A- SQL services must be running

B- Two wireless APs must be sending data

C- DTLS encryption on wireless traffic must be turned off

D- Wireless network security must be set to open

Answer:

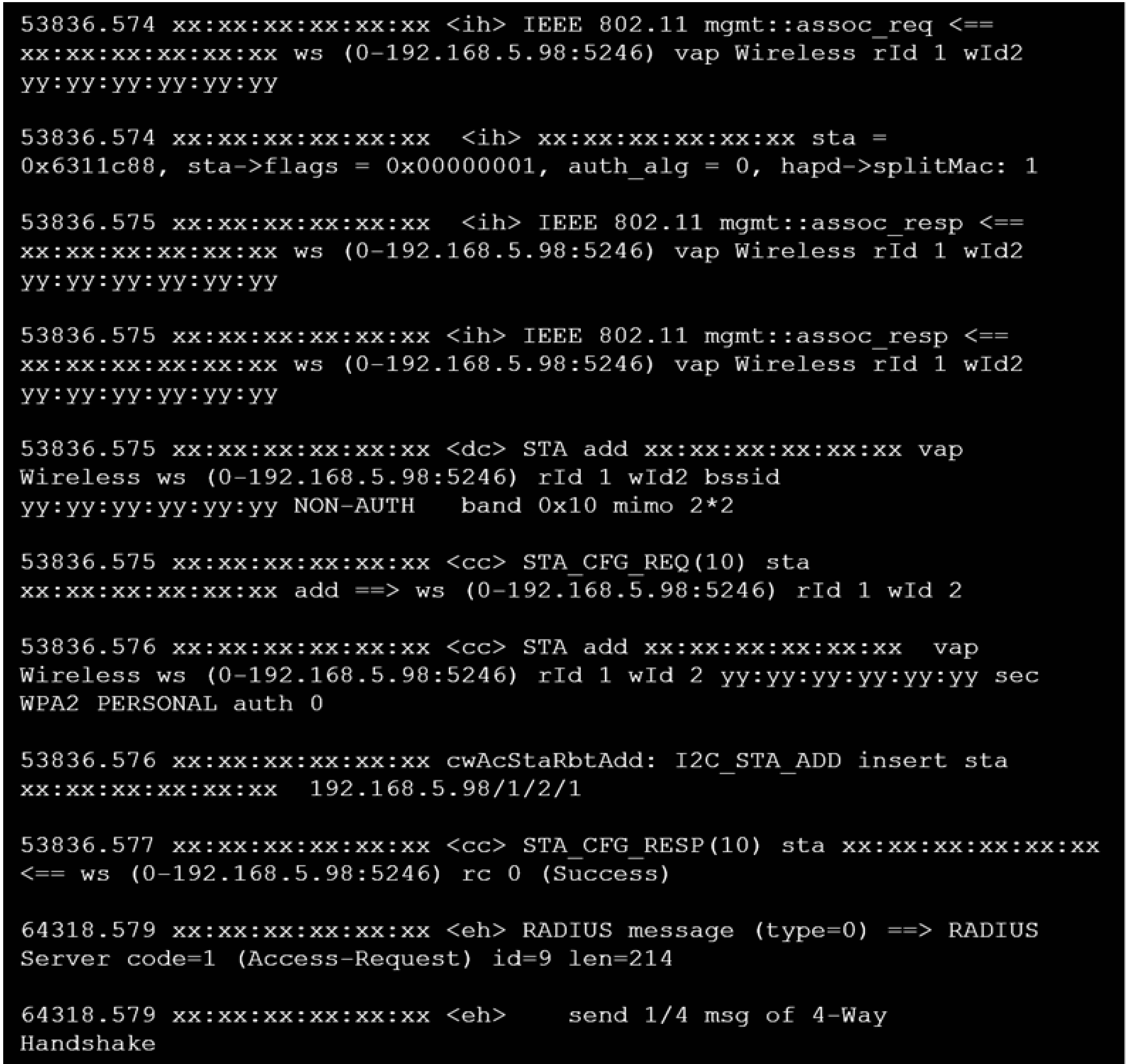
A

Question 9

Question Type: **MultipleChoice**

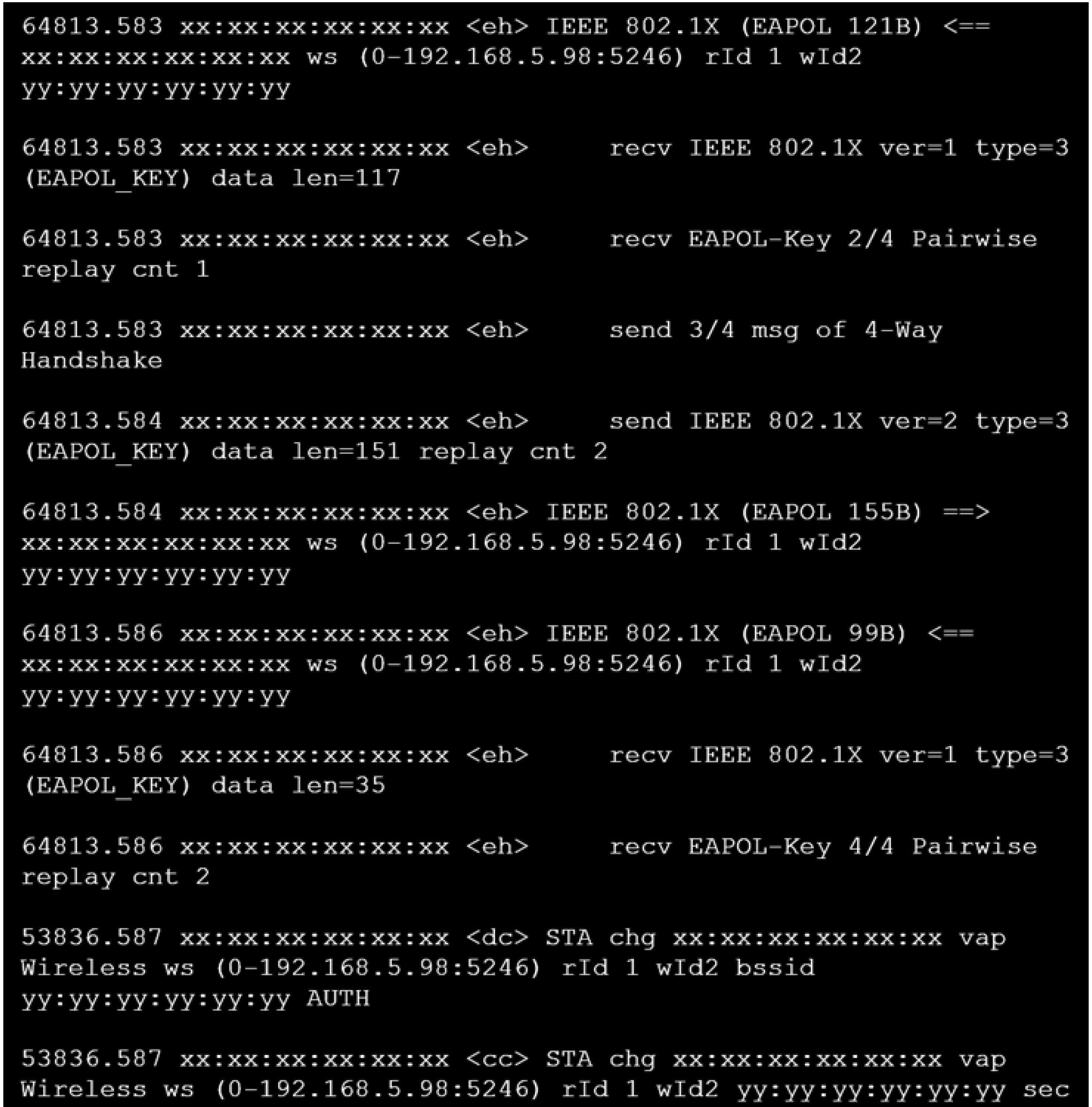
Refer to the exhibits.

Exhibit A



```
53836.574 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc_req <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rId 1 wId2
yy:yy:yy:yy:yy:yy

53836.574 xx:xx:xx:xx:xx:xx  <ih> xx:xx:xx:xx:xx:xx sta =
0x6311c88, sta->flags = 0x00000001, auth_alg = 0, hapd->splitMac: 1

53836.575 xx:xx:xx:xx:xx:xx  <ih> IEEE 802.11 mgmt::assoc_resp <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rId 1 wId2
yy:yy:yy:yy:yy:yy

53836.575 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc_resp <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rId 1 wId2
yy:yy:yy:yy:yy:yy

53836.575 xx:xx:xx:xx:xx:xx <dc> STA add xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId2 bssid
yy:yy:yy:yy:yy:yy NON-AUTH   band 0x10 mimo 2*2

53836.575 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(10) sta
xx:xx:xx:xx:xx:xx add ==> ws (0-192.168.5.98:5246) rId 1 wId 2

53836.576 xx:xx:xx:xx:xx:xx <cc> STA add xx:xx:xx:xx:xx:xx  vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId 2 yy:yy:yy:yy:yy:yy sec
WPA2 PERSONAL auth 0

53836.576 xx:xx:xx:xx:xx:xx cwAcStaRbtAdd: I2C_STA_ADD insert sta
xx:xx:xx:xx:xx:xx  192.168.5.98/1/2/1

53836.577 xx:xx:xx:xx:xx:xx <cc> STA_CFG_RESP(10) sta xx:xx:xx:xx:xx:xx
<== ws (0-192.168.5.98:5246) rc 0 (Success)

64318.579 xx:xx:xx:xx:xx:xx <eh> RADIUS message (type=0) ==> RADIUS
Server code=1 (Access-Request) id=9 len=214

64318.579 xx:xx:xx:xx:xx:xx <eh>    send 1/4 msg of 4-Way
Handshake
```

Exhibit B



```
64813.583 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 121B) <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.583 xx:xx:xx:xx:xx:xx <eh>    recv IEEE 802.1X ver=1 type=3
(EAPOL_KEY) data len=117

64813.583 xx:xx:xx:xx:xx:xx <eh>    recv EAPOL-Key 2/4 Pairwise
replay cnt 1

64813.583 xx:xx:xx:xx:xx:xx <eh>    send 3/4 msg of 4-Way
Handshake

64813.584 xx:xx:xx:xx:xx:xx <eh>    send IEEE 802.1X ver=2 type=3
(EAPOL_KEY) data len=151 replay cnt 2

64813.584 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 155B) ==>
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 99B) <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh>    recv IEEE 802.1X ver=1 type=3
(EAPOL_KEY) data len=35

64813.586 xx:xx:xx:xx:xx:xx <eh>    recv EAPOL-Key 4/4 Pairwise
replay cnt 2

53836.587 xx:xx:xx:xx:xx:xx <dc> STA chg xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId2 bssid
yy:yy:yy:yy:yy:yy AUTH

53836.587 xx:xx:xx:xx:xx:xx <cc> STA chg xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId2 yy:yy:yy:yy:yy:yy sec
```

The exhibits show the diagnose debug log of a station connection taken on the controller CLI.

Which security mode is used by the wireless connection?

Options:

A- WPA2 Enterprise

B- WPA3 Enterprise

C- WPA2 Personal and radius MAC filtering

D- Open, with radius MAC filtering

Answer:

C

Question 10

Question Type: **MultipleChoice**

Which statement describes FortiPresence location map functionality?

Options:

A- Provides real-time insight into user movements

B- Provides real-time insight into user online activity

C- Provides real-time insight into user purchase activity

D- Provides real-time insight into user usage stats

Answer:

A