- **Vendor:** Fortinet
- **Exam Code:** NSE6_FWF-6.4
- **Exam Name:** Fortinet NSE 6 - Secure Wireless LAN 6.4
- **New Updated Questions from Braindump2go**
- **(Updated in September/2021)**

QUESTION 1
What type of design model does FortiPlanner use in wireless design project?

A. Architectural model
B. Predictive model
C. Analytical model
D. Integration model

Answer: A
Explanation:
FortiPlanner will look familiar to anyone who has used architectural or home design software.
Reference: http://en.hackdig.com/?7883.htm

QUESTION 2
Refer to the exhibits.
Exhibit A

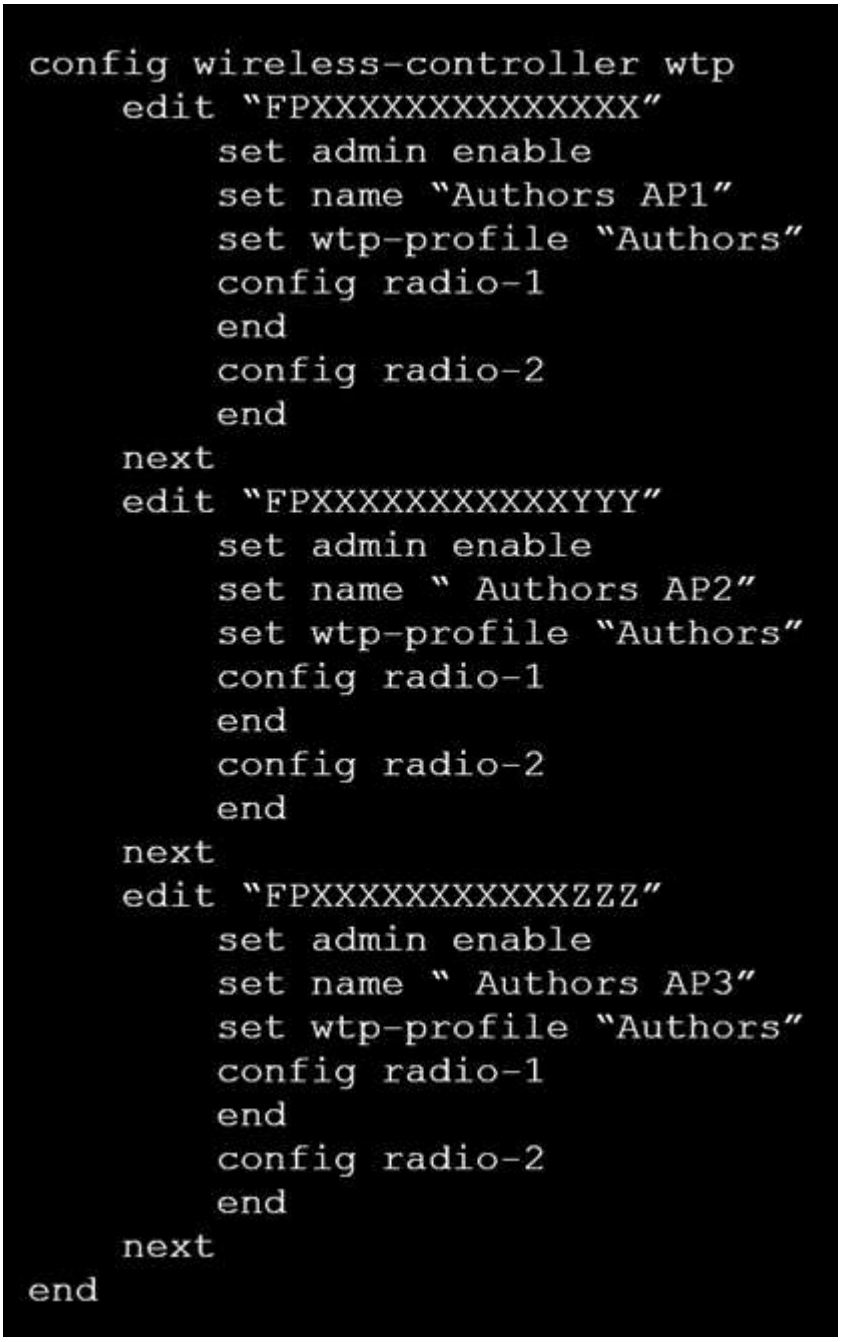
config wireless-controller wtp
edit "FPXXXXXXXXXXXXX"
set admin enable
set name "Authors AP1"
set wtp-profile "Authors"
config radio-1
end
config radio-2
end
next
edit "FPXXXXXXXXXXYYY"
set admin enable
set name " Authors AP2"
set wtp-profile "Authors"
config radio-1
end
config radio-2
end
next
edit "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
        set schedule "always"
    next
end
```

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.)

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: BC

QUESTION 3
A tunnel mode wireless network is configured on a FortiGate wireless controller.
Which task must be completed before the wireless network can be used?

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.
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/723e20ad-5098-11e9-94bf-00505692583a/FortiWiFi_and_FortiAP-6.2.0-Configuration_Guide.pdf

QUESTION 4
Which statement is correct about security profiles on FortiAP devices?

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
Explanation:
https://docs.fortinet.com/document/fortiap/6.4.0/fortiwifi-and-fortiap-configuration-guide/47321/fortiap-s-bridge-mode-security-profiles

QUESTION 5
How are wireless clients assigned to a dynamic VLAN configured for hash mode?

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.
Reference: https://docs.fortinet.com/document/fortiap/7.0.1/fortiwifi-and-fortiap-configuration-guide/376326/configuring-dynamic-user-vlan-assignment

QUESTION 6

Which two statements about distributed automatic radio resource provisioning (DARRP) are correct? (Choose two.)

A. DARRP performs continuous spectrum analysis to detect sources of interference. It uses this information to allow the AP to select the optimum channel.
B. DARRP performs measurements of the number of BSSIDs and their signal strength (RSSI). The controller then uses this information to select the optimum channel for the AP.
C. DARRP measurements can be scheduled to occur at specific times.
D. DARRP requires that wireless intrusion detection (WIDS) be enabled to detect neighboring devices.

Answer: AD
Explanation:
DARRP (Distributed Automatic Radio Resource Provisioning) technology ensures the wireless infrastructure is always optimized to deliver maximum performance. Fortinet APs enabled with this advanced feature continuously monitor the RF environment for interference, noise and signals from neighboring APs, enabling the FortiGate WLAN Controller to determine the optimal RF power levels for each AP on the network. When a new AP is provisioned, DARRP also ensures that it chooses the optimal channel, without administrator intervention.
Reference: http://www.corex.at/Produktinfos/FortiOS_Wireless.pdf

QUESTION 7
Which factor is the best indicator of wireless client connection quality?

A. Downstream link rate, the connection rate for the AP to the client
B. The receive signal strength (RSS) of the client at the AP
C. Upstream link rate, the connection rate for the client to the AP
D. The channel utilization of the channel the client is using

Answer: B
Explanation:
SSI, or "Received Signal Strength Indicator," is a measurement of how well your device can hear a signal from an access point or router. It's a value that is useful for determining if you have enough signal to get a good wireless connection.
Reference: https://www.metageek.com/training/resources/understanding-rssi.html

QUESTION 8
When configuring Auto TX Power control on an AP radio, which two statements best describe how the radio responds? (Choose two.)

A. When the AP detects any other wireless signal stronger that -70 dBm, it will reduce its transmission power until it reaches the minimum configured TX power limit.
B. When the AP detects PF Interference from an unknown source such as a cordless phone with a signal stronger that -70 dBm, it will increase its transmission power until it reaches the maximum configured TX power limit.
C. When the AP detects any wireless client signal weaker than -70 dBm, it will reduce its transmission power until it reaches the maximum configured TX power limit.
D. When the AP detects any interference from a trusted neighboring AP stronger that -70 dBm, it will reduce its transmission power until it reaches the minimum configured TX power limit.

Answer: AC
Explanation:
https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/wireless/ap_wireless_signalstrength_c.html

QUESTION 9

Refer to the exhibits.
Exhibit A.

```
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
        config radio-1
            set band 802.11n
            set power-level 50
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set vap-all manual
            set vaps "Main-Wifi" "Contractors" "Guest"
"Wifi_IOT" "Wifi_POS" "Staff" "Students"
            set channel "1" "6" "11"
        end
        config radio-2
            set band 802.11ac
            set channel-bonding 40MHz
            set power-level 60
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set vap-all manual
            set vaps "Main-Wifi" "Contractors" "Guest"
"Wifi_IOT" "Wifi_POS" "Staff" "Students"
            set channel "36" "44" "52" "60"
        end
    next
end
```

Exhibit B.

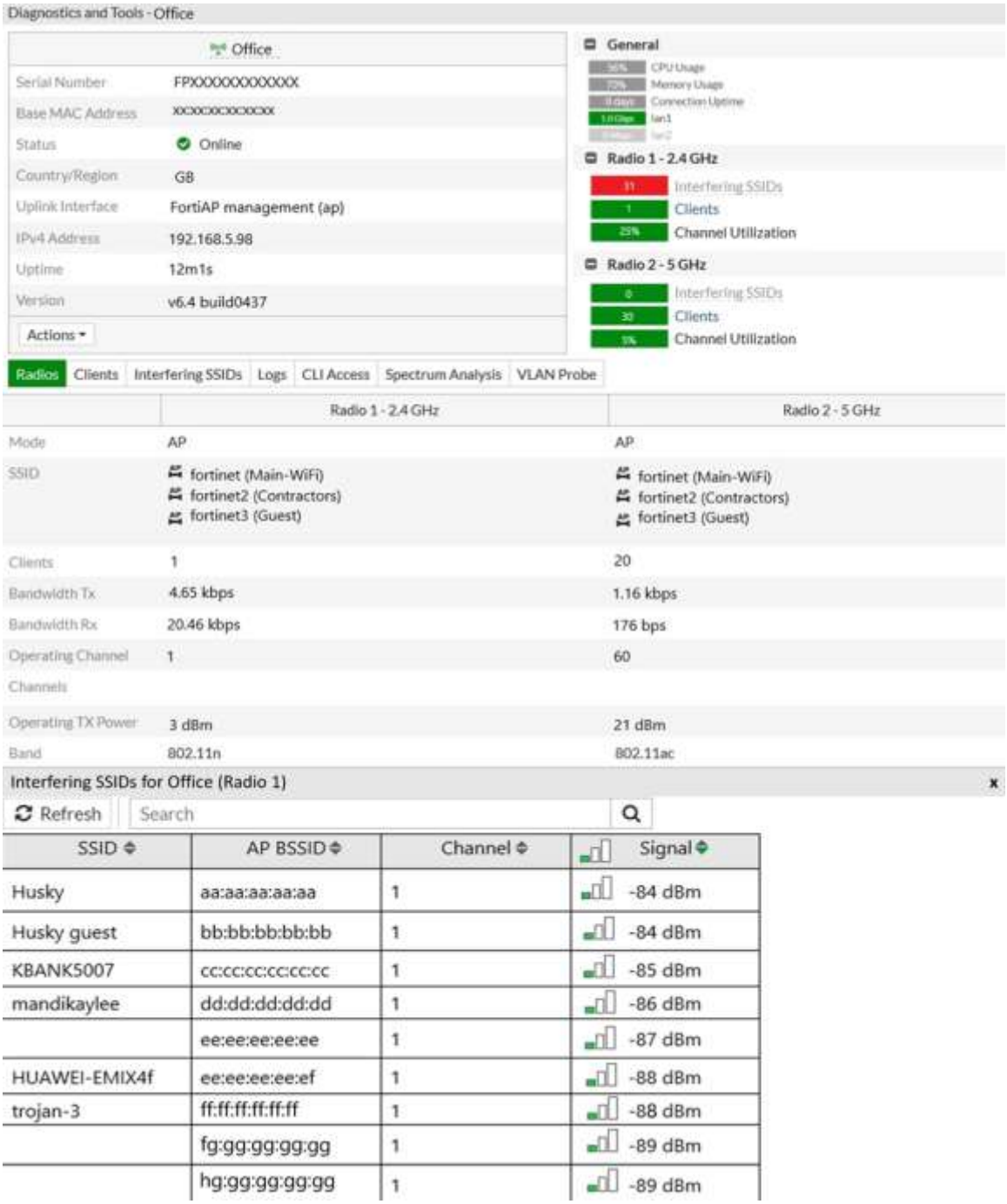

Exhibit C.

```
# get wireless-controller rf-analysis FPXXXXXXXXXXXXX

WTP: Office 0-192.168.5.98:5246

     channel    rssi-total   rf-score     overlap-ap    interfere-ap    chan-utilization
         1          100          6            13             13              63%
         2          23           10           0              22              47%
         3          15           10           0              22              15%
         4          24           10           0              22              15%
         5          51           10           0              22              41%
         6          223          1            9              9               75%
         7          52           10           0              17              47%
         8          32           10           0              17              13%
         9          27           10           0              19              10%
         10         45           10           0              19              28%
         11         177          1            8              10              65%
         12         46           10           0              10              34%
         13         45           10           2              10              70%
         14         14           10           0              10               0%
         36         16           10           2              2               0%
         44         83           7            5              5               0%
```

A wireless network has been installed in a small office building and is being used by a business to connect its wireless clients. The network is used for multiple purposes, including corporate access, guest access, and connecting point-of-sale and IoT devices.
Users connecting to the guest network located in the reception area are reporting slow performance. The network administrator is reviewing the information shown in the exhibits as part of the ongoing investigation of the problem. They show the profile used for the AP and the controller RF analysis output together with a screenshot of the GUI showing a summary of the AP and its neighboring APs.
To improve performance for the users connecting to the guest network in this area, which configuration change is most likely to improve performance?

A. Increase the transmission power of the AP radios
B. Enable frequency handoff on the AP to band steer clients
C. Reduce the number of wireless networks being broadcast by the AP
D. Install another AP in the reception area to improve available bandwidth

Answer: A

QUESTION 10
Which two statements about background rogue scanning are correct? (Choose two.)

A. A dedicated radio configured for background scanning can support the connection of wireless clients
B. When detecting rogue APs, a dedicated radio configured for background scanning can suppress the rogue AP
C. Background rogue scanning requires DARRP to be enabled on the AP instance
D. A dedicated radio configured for background scanning can detect rogue devices on all other channels in its configured frequency band.

Answer: AB
Explanation:
To enable rogue AP scanning
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/723e20ad-5098-11e9-94bf-00505692583a/FortiWiFi_and_FortiAP-6.2.0-Configuration_Guide.pdf