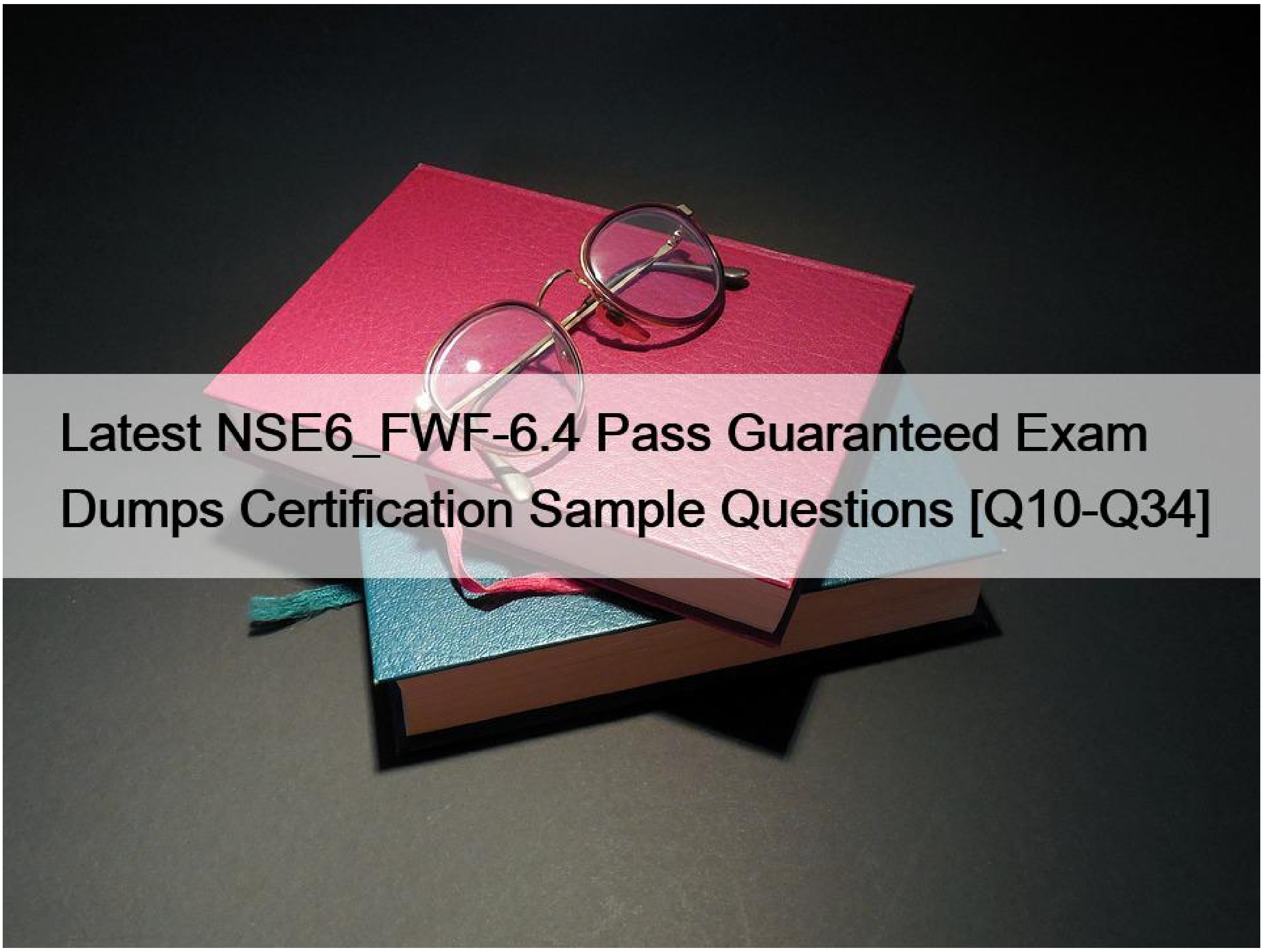
Latest NSE6_FWF-6.4 Pass Guaranteed Exam Dumps Certification Sample Questions [Q10-Q34



Latest NSE6_FWF-6.4 Pass Guaranteed Exam Dumps Certification Sample Questions
New NSE6_FWF-6.4 Test Materials & Valid NSE6_FWF-6.4 Test Engine

NEW QUESTION 10

When using FortiPresence as a captive portal, which two types of public authentication services can be used to access guest Wi-Fi? (Choose two.)
* Social networks authentication
* Software security token authentication
* Short message service authentication
* Hardware security token authentication
This information along with the social network authentication logins with Facebook, Google, Instagram, LinkedIn, or FortiPresence using your WiFi.

Captive Portal configurations for social media logins and internet access. You can add and manage sites using the integrated Google maps and manoeuvre your hardware infrastructure easily.

NEW QUESTION 11

Where in the controller interface can you find a wireless client&#8217;s upstream and downstream link rates?
* On the AP CLI, using the cw_diag ksta command
* On the controller CLI, using the diag wireless-controller wlac -d sta command
* On the AP CLI, using the cw_diag -d sta command
* On the controller CLI, using the WiFi Client monitor

NEW QUESTION 12

Which two statements about distributed automatic radio resource provisioning (DARRP) are correct? (Choose two.)
* DARRP performs continuous spectrum analysis to detect sources of interference. It uses this information to allow the AP to select the optimum channel.
* 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.
* DARRP measurements can be scheduled to occur at specific times.
* DARRP requires that wireless intrusion detection (WIDS) be enabled to detect neighboring devices.
According to Fortinet training: &#8220;When using DARRP, the AP selects the best channel available to use based on the scan results of BSSID/receive signal strength (RSSI) to AC&#8221; and &#8220;To set the running time for DARRP optimization, use the following CLI command within the wireless controller setting: set darrp-optimize {integer}. Note that DARRP doesn&#8217;t do continuous spectrum analysis&#8230;&#8221;

NEW QUESTION 13

Which factor is the best indicator of wireless client connection quality?
* Downstream link rate, the connection rate for the AP to the client
* The receive signal strength (RSS) of the client at the AP
* Upstream link rate, the connection rate for the client to the AP
* The channel utilization of the channel the client is using
SSI, or &#8220;Received Signal Strength Indicator,&#8221; is a measurement of how well your device can hear a signal from an access point or router. It&#8217;s a value that is useful for determining if you have enough signal to get a good wireless connection.

NEW QUESTION 14

Where in the controller interface can you find a wireless client&#8217;s upstream and downstream link rates?
* On the AP CLI, using the cw_diag ksta command
* On the controller CLI, using the diag wireless-controller wlac -d sta command
* On the AP CLI, using the cw_diag -d sta command
* On the controller CLI, using the WiFi Client monitor

NEW QUESTION 15

Which of the following is a requirement to generate analytic reports using on-site FortiPresence deployment?
* SQL services must be running
* Two wireless APs must be sending data
* DTLS encryption on wireless traffic must be turned off
* Wireless network security must be set to open

NEW QUESTION 16

Which administrative access method must be enabled on a FortiGate interface to allow APs to connect and function?
* Security Fabric
* SSH
* HTTPS
* FortiTelemetry

NEW QUESTION 17

Which two roles does FortiPresence analytics assist in generating presence reports? (Choose two.)
* Gathering details about on site visitors
* Predicting the number of guest users visiting on-site
* Comparing current data with historical records
* Reporting potential threats by guests on site

NEW QUESTION 18

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

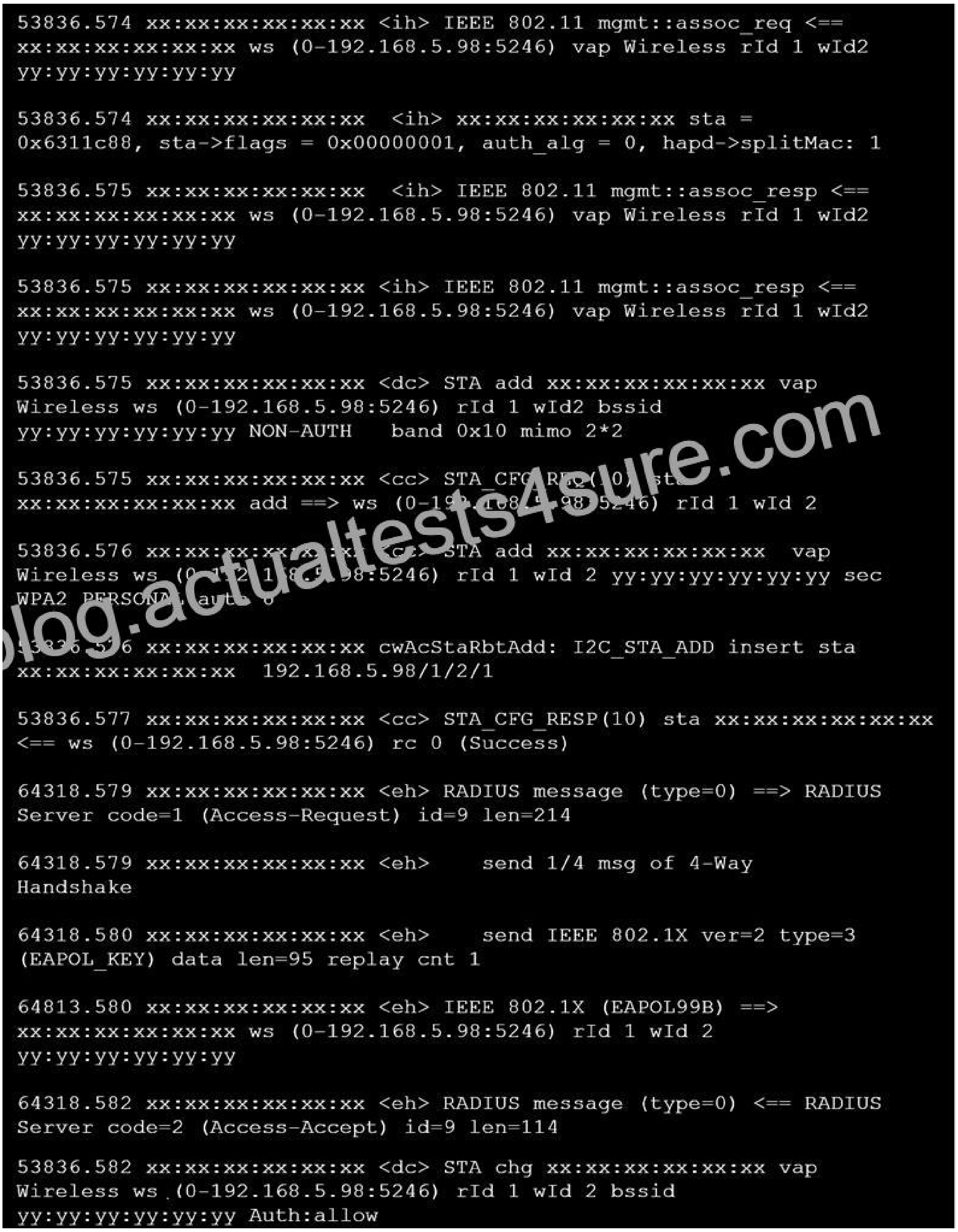
NEW QUESTION 19

Which statement describes FortiPresence location map functionality?
* Provides real-time insight into user movements
* Provides real-time insight into user online activity
* Provides real-time insight into user purchase activity
* Provides real-time insight into user usage stats

NEW QUESTION 20

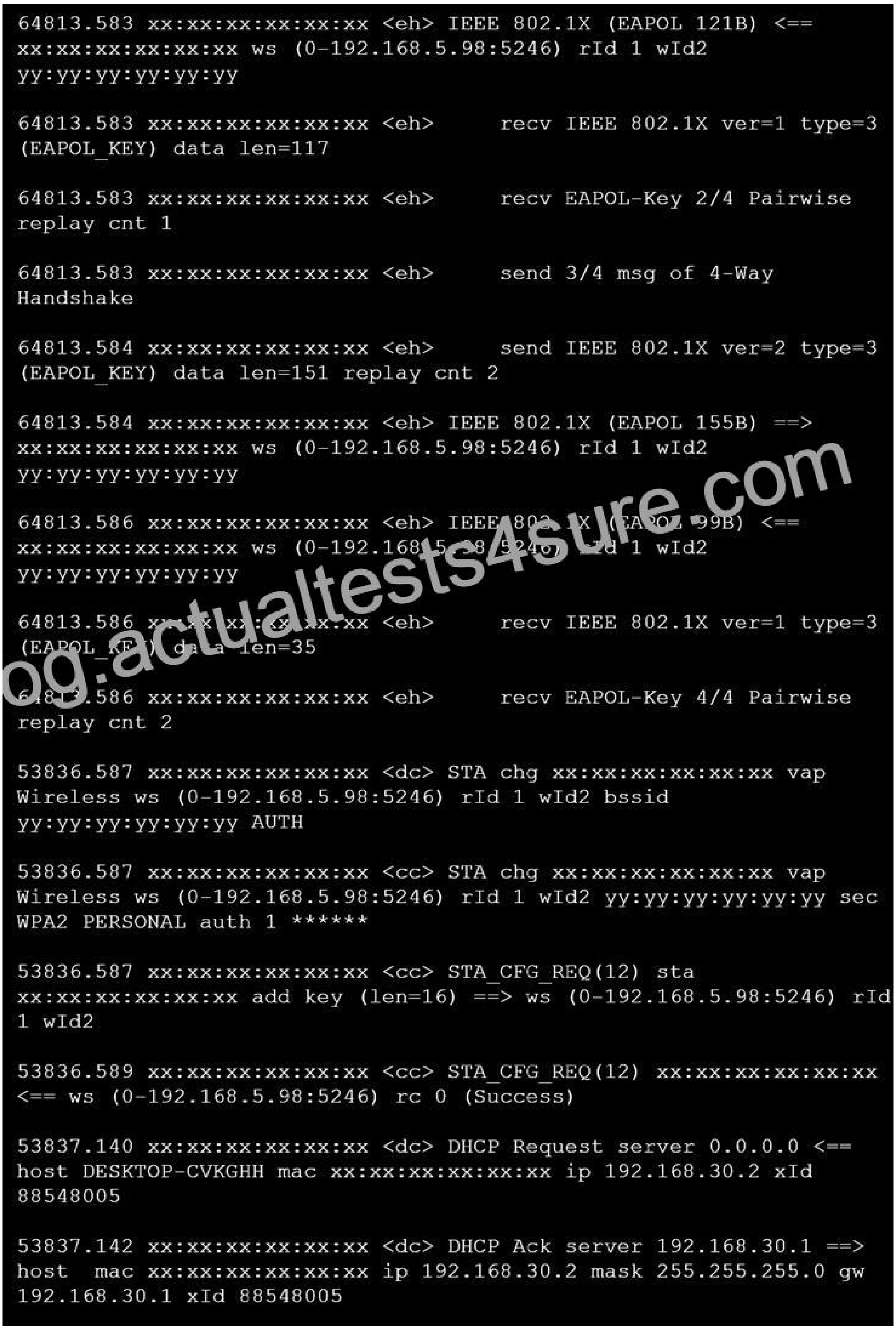
Refer to the exhibits.

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

64318.580 xx:xx:xx:xx:xx:xx <eh>    send IEEE 802.1X ver=2 type=3
(EAPOL_KEY) data len=95 replay cnt 1

64813.580 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL99B) ==>
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId 2
yy:yy:yy:yy:yy:yy

64318.582 xx:xx:xx:xx:xx:xx <eh> RADIUS message (type=0) <== RADIUS
Server code=2 (Access-Accept) id=9 len=114

53836.582 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 wId 2 bssid
yy:yy:yy:yy:yy:yy Auth:allow
```

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
WPA2 PERSONAL auth 1 ******

53836.587 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(12) sta
xx:xx:xx:xx:xx:xx add key (len=16) ==> ws (0-192.168.5.98:5246) rId
1 wId2

53836.589 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(12) xx:xx:xx:xx:xx:xx
<== ws (0-192.168.5.98:5246) rc 0 (Success)

53837.140 xx:xx:xx:xx:xx:xx <dc> DHCP Request server 0.0.0.0 <==
host DESKTOP-CVKGHH mac xx:xx:xx:xx:xx:xx ip 192.168.30.2 xId
88548005

53837.142 xx:xx:xx:xx:xx:xx <dc> DHCP Ack server 192.168.30.1 ==>
host  mac xx:xx:xx:xx:xx:xx ip 192.168.30.2 mask 255.255.255.0 gw
192.168.30.1 xId 88548005
```

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?

* WPA2 Enterprise
* WPA3 Enterprise

* WPA2 Personal and radius MAC filtering
* Open, with radius MAC filtering
Best security option is WPA2-AES.

NEW QUESTION 21

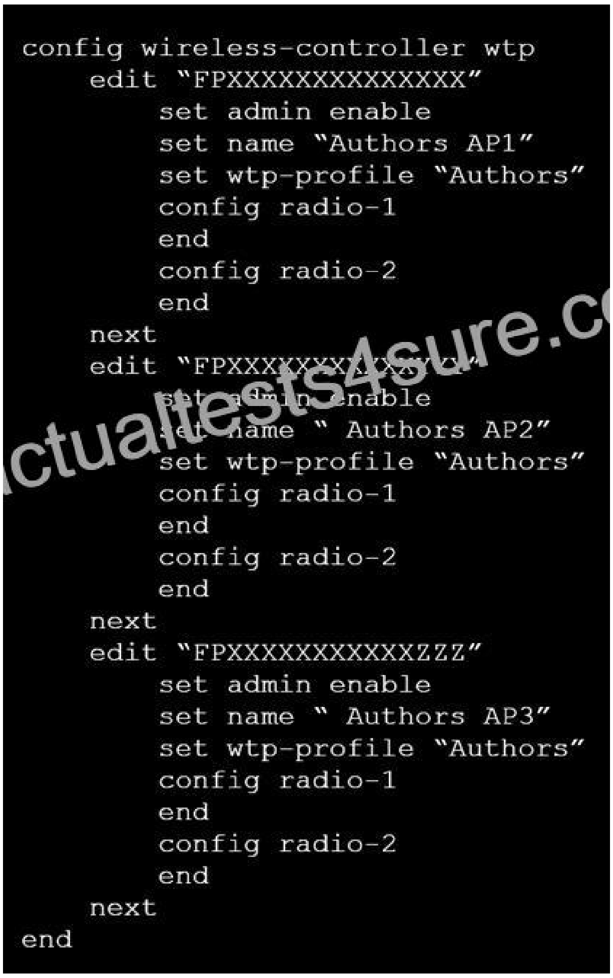
You are investigating a wireless performance issue and you are trying to audit the neighboring APs in the PF environment. You review the Rogue APs widget on the GUI but it is empty, despite the known presence of other APs.

Which configuration change will allow neighboring APs to be successfully detected?
* Enable Locate WiFi clients when not connected in the relevant AP profiles.
* Enable Monitor channel utilization on the relevant AP profiles.
* Ensure that all allowed channels are enabled for the AP radios.
* Enable Radio resource provisioning on the relevant AP profiles.
The ARRP (Automatic Radio Resource Provisioning) profile improves upon DARRP (Distributed Automatic Radio Resource Provisioning) by allowing more factors to be considered to optimize channel selection among FortiAPs. DARRP uses the neighbor APs channels and signal strength collected from the background scan for channel selection.

NEW QUESTION 22

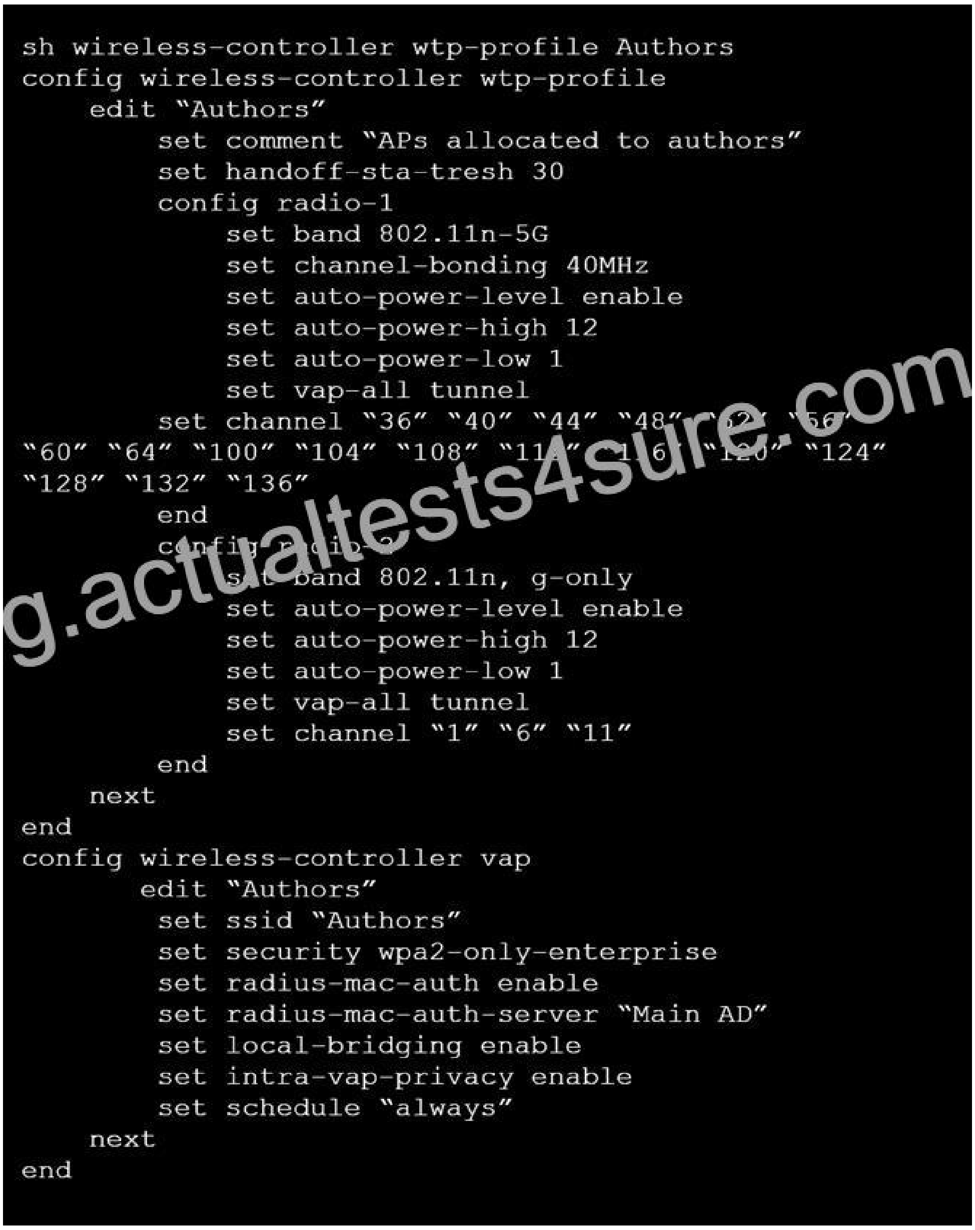
Refer to the exhibits.

Exhibit A



```
config wireless-controller wtp
    edit "FPXXXXXXXXXXXXXX"
        set admin enable
        set name "Authors AP1"
        set wtp-profile "Authors"
        config radio-1
        end
        config radio-2
        end
    next
    edit "FPXXXXXXXXXXXYYY"
        set admin enable
        set name " Authors AP2"
        set wtp-profile "Authors"
        config radio-1
        end
        config radio-2
        end
    next
    edit "FPXXXXXXXXXXXZZZ"
        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.)

* For both interfaces in the wtp-profile, configure set vaps to be &#8220;Authors&#8221;
* Disable intra-vap-privacy for the Authors vap-wireless network
* For both interfaces in the wtp-profile, configure vap-all to be manual
* Increase the transmission power of the AP radio interfaces

NEW QUESTION 23

Which two phases are part of the process to plan a wireless design project? (Choose two.)
* Project information phase
* Hardware selection phase
* Site survey phase
* Installation phase
Reference:

https://www.automation.com/en-us/articles/2015-2/wireless-device-network-planning-and-design

NEW QUESTION 24

When deploying a wireless network that is authenticated using EAP PEAP, which two configurations are required? (Choose two.)
* An X.509 certificate to authenticate the client
* An X.509 to authenticate the authentication server
* A WPA2 or WPA3 personal wireless network
* A WPA2 or WPA3 Enterprise wireless network

NEW QUESTION 25

When enabling security fabric on the FortiGate interface to manage FortiAPs, which two types of communication channels are established between FortiGate and FortiAPs? (Choose two.)
* Control channels
* Security channels
* FortLink channels
* Data channels
The control channel for managing traffic, which is always encrypted by DTLS. l The data channel for carrying client data packets.

NEW QUESTION 26

Which two phases are part of the process to plan a wireless design project? (Choose two.)
* Project information phase
* Hardware selection phase
* Site survey phase
* Installation phase

NEW QUESTION 27

What type of design model does FortiPlanner use in wireless design project?
* Architectural model
* Predictive model
* Analytical model
* Integration model
FortiPlanner will look familiar to anyone who has used architectural or home design software.

NEW QUESTION 28

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

- Broadcast
- Multicast

NSE6_FWF-6.4 Sample with Accurate & Updated Questions:
https://www.actualtests4sure.com/NSE6_FWF-6.4-test-questions.html]