



- Expert Verified, Online, **Free**.

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.

Suggested Answer: AD

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

Community vote distribution

BC (100%)

 **tochno** Highly Voted 3 years, 2 months ago

I would say correct answers are B and C.

According to Fortinet training: "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" and "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't do continuous spectrum analysis..."

upvoted 7 times

 **afons0** Highly Voted 3 years, 2 months ago

B and C are the correct ones.


upvoted 6 times

 **Kevin_Howard** Most Recent 5 months, 1 week ago

Selected Answer: BC

According to Fortinet training: "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" and "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't do continuous spectrum analysis..."

upvoted 3 times

 **evilCorpBot7494** 9 months, 1 week ago

Selected Answer: BC

Study guide Page 169

"When using DARRP, the AP selects the best channel available to use based on the scan results of BSSID/received signal strength indicator (RSSI) to AC."

"Uses background scans every 600 seconds"

"AP reevaluates channel selection every 84600 seconds"

"Configure Schedule using CLI to specify when to run DARRP scan"

upvoted 1 times

 **Manuel2493** 1 year, 10 months ago

Correct Answer: BC

Page 169 Study Guide

upvoted 1 times

 **Robin997** 1 year, 11 months ago

Selected Answer: BC

B & C are correct
upvoted 1 times

🗨️ **Robin997** 1 year, 11 months ago

Selected Answer: BC

B & D - P.168
upvoted 1 times

🗨️ **p3dr01n** 2 years, 1 month ago

Selected Answer: BC

Study guide pjavascript:void(0)age 168
upvoted 1 times

🗨️ **zic1** 2 years, 2 months ago

I thnk its BC but its AP, not Controler who do optimization
upvoted 1 times

🗨️ **kinge2** 2 years, 11 months ago

Selected Answer: BC

B and C are correct
upvoted 1 times

🗨️ **LordRouter** 3 years, 1 month ago

A & D are both incorrect, so B & C is the correct answer.
upvoted 2 times

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

Suggested Answer: B

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>



Community vote distribution

C (100%)

  **afons0** Highly Voted 1 year, 8 months ago



Correct is C

upvoted 7 times

  **Manuel2493** Most Recent 4 months, 3 weeks ago

C is Correct Study Guide

upvoted 2 times

  **Robin997** 5 months, 3 weeks ago

Selected Answer: C



C

upvoted 1 times

  **zic1** 8 months, 3 weeks ago

according doc, up rate is the good answer

upvoted 2 times

  **kinge2** 1 year, 5 months ago

C is correct



upvoted 1 times

  **Kevin_Howard** 1 year, 5 months ago

Selected Answer: C

Correct is C (Pag 258 of study guide)

upvoted 2 times

  **endoor** 1 year, 8 months ago

Afons0 is rocking every question here people. Feel free to verify but he's 100% right every time

upvoted 1 times

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 than -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 than -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 than -70 dBm, it will reduce its transmission power until it reaches the minimum configured TX power limit.

Suggested Answer: AC

Reference:

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Firmware/wireless/ap_wireless_signalstrength_c.html

Community vote distribution

AD (100%)

evilCorpBot7494 3 months ago

Selected Answer: AD

A & D.

Automatic Mechanism:

- If interference is detected, controller reduces AP TX power until auto-power-low threshold
- If interference is not detected, or is detected and removed, controller increases AP TX power until auto-power-high threshold

So pretty much the first point covers both A & D, while the second one covers nothing mentioned in the answers.

upvoted 1 times

Robin997 1 year, 5 months ago

Selected Answer: AD

A & D -

upvoted 2 times

zic1 1 year, 8 months ago

only one is true

upvoted 1 times

kinge2 2 years, 5 months ago

sorry meant to say A and D is more accurate

upvoted 2 times

kinge2 2 years, 5 months ago

A and C seems correct

upvoted 1 times

afons0 2 years, 8 months ago

C its correct if you change reduce by INCREASE "it will INCREASE its transmission power until it reaches the maximum configured TX power limit."

If not i thing D its more correct than C.

upvoted 4 times

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
```

prw709528

Exhibit B.

Office	
Serial Number	FPXXXXXXXXXXXX
Base MAC Address	xx:xx:xx:xx:xx:xx
Status	✔ Online
Country/Region	GB
Uplink Interface	FortiAP management (ap)
IPv4 Address	192.168.5.98
Uptime	12m1s
Version	v6.4 build0437
Actions ▾	

General

- 56% CPU Usage
- 70% Memory Usage
- 0 days Connection Uptime
- 1.0 Gbps lan1
- 0 Mbps lan2

Radio 1 - 2.4 GHz

- 31 Interfering SSIDs
- 1 Clients
- 25% Channel Utilization

Radio 2 - 5 GHz

- 0 Interfering SSIDs
- 30 Clients
- 5% Channel Utilization

- Radios
Clients
Interfering SSIDs
Logs
CLI Access
Spectrum Analysis
VLAN Probe

	Radio 1 - 2.4 GHz	Radio 2 - 5 GHz
Mode	AP	AP
SSID	<ul style="list-style-type: none"> AP fortinet (Main-WiFi) AP fortinet2 (Contractors) AP fortinet3 (Guest) 	<ul style="list-style-type: none"> AP fortinet (Main-WiFi) AP fortinet2 (Contractors) AP fortinet3 (Guest)
Clients	1	20
Bandwidth Tx	4.65 kbps	1.16 kbps
Bandwidth Rx	20.46 kbps	176 bps
Operating Channel	1	60
Channels		
Operating TX Power	3 dBm	21 dBm
Band	802.11n	802.11ac

Interfering SSIDs for Office (Radio 1) x

↻ Refresh
Search
🔍

SSID	AP BSSID	Channel	Signal
Husky	aa:aa:aa:aa:aa	1	📶 -84 dBm
Husky guest	bb:bb:bb:bb:bb	1	📶 -84 dBm
KBANK5007	cc:cc:cc:cc:cc	1	📶 -85 dBm
mandikaylee	dd:dd:dd:dd:dd	1	📶 -86 dBm
	ee:ee:ee:ee:ee	1	📶 -87 dBm
HUAWEI-EMIX4f	ee:ee:ee:ee:ef	1	📶 -88 dBm
trojan-3	ff:ff:ff:ff:ff	1	📶 -88 dBm
	fg:gg:gg:gg:gg	1	📶 -89 dBm
	hg:gg:gg:gg:gg	1	📶 -89 dBm

[raw709528]

```
# get wireless-controller rf-analysis FPXXXXXXXXXXXXXXXXX
WTP: Office 0-192.168.5.98:5246
```

channel	rsssi-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

Suggested Answer: A

Community vote distribution



Robin997 5 months, 3 weeks ago

Selected Answer: A

A is correct
upvoted 1 times

p3dr01n 7 months, 1 week ago

Selected Answer: A

A.
set power-level 60 is on 5Ghz radio, so increase power will be OK.
upvoted 1 times

p3dr01n 7 months, 1 week ago

A.
set power-level 60 is on 5Ghz radio, so increase power will be OK.
upvoted 1 times

atidd 7 months, 2 weeks ago

Selected Answer: A

Frequency handoff according to the docs will move a client to the 5GHz band. not the other way around. All the clients are already on 5GHz. The power level is set to 50 and 60%. changing that should do the trick.
upvoted 1 times

Nomorg 9 months ago

Selected Answer: D

I think D is correct.

A) it is on max powerlevel (23dbm) on the 5GHz band for Country Code GB. (Increasing the power level on 2,4Ghz band will do nothing for us because of CU.

B) reporting clients are on the 5Ghz band - we would not want to push clients to 2,4.

C)Only broadcasting 3 SSIDs, thats common



D) the only thing that makes sense to me.

upvoted 2 times

  **draven76** 1 year ago

Not clear to me: while frequency handoff is not completely configured (it's missing the "set frequency-handoff enable" command that is disabled by default), that would result in making clients switch to 2.4 GHz (from exhibit B you can see that almost all clients are connected to 5 GHz and users are already reporting issues so, I think, guests are on 5 GHz?). But 2.4 GHz has a lot of Interfering SSIDs. As the users are complaining about a specific area, maybe it's the power level too low. I'd go for A



upvoted 1 times

  **kinge2** 1 year, 5 months ago

Selected Answer: B



B COORECT

upvoted 1 times

  **kinge2** 1 year, 5 months ago

B is correct



upvoted 1 times

  **3993** 1 year, 6 months ago

Selected Answer: B

STUDY 298

upvoted 1 times

  **3993** 1 year, 6 months ago

Selected Answer: B

PAGE 258

upvoted 2 times

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.

Suggested Answer: AB

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

Community vote distribution

AC (63%)

BC (38%)

evilCorpBot7494 8 months, 4 weeks ago

Selected Answer: AC

According to study guide , A & C are correct.

A) is correct because putting one of the Radios in the AP in background scanning mode makes it work as a normal Radio that broadcasts SSIDs, but every 600 seconds performs scans for rogue APs. This has a bad detection rate and can make packets be dropped in the wireless network, but half-asses the monitoring requirement. The point is yeah, background scanning allows for clients to connect to the wireless. Using a dedicated radio does not, it performs foreground scans and that is all it does.

C) is correct because, according to page 177, background scanning is automatic if DARRP is enabled.

B) is not correct because if the radio is configured for background scanning, it can not suppress the rogue AP. Fortinet pretty much says they even can't detect rogue APs while in this mode, so suppressing is out of the question. In page 180 it says "Suppressing Rogue APs Requires dedicated monitor mode - Not possible with background scans"

D is not correct because, as I understand according to page 177, it checks for all channels every 20 ms, not just for the ones it has configured.
upvoted 1 times

okay_1 1 year, 3 months ago

The correct answer is B and C

upvoted 1 times

saber12 1 year, 7 months ago

Option A and Option C.

B is wrong because Background don't do suppress AP, but dedicated monitor is doing suppress AP.

upvoted 2 times

diaz9019 1 year, 11 months ago

Selected Answer: AC

Option A and Option C.

upvoted 2 times

diaz9019 1 year, 11 months ago

Option A and Option C.

upvoted 1 times

Robin997 1 year, 11 months ago

Selected Answer: BC

B & C - But Im not sure. Shitty Question. All of them are wrong to me.

upvoted 2 times

🗨️ **marathawarrior** 1 year, 12 months ago

B and D are more correct than the rest. Option A is definitely incorrect because, in dedicated monitor mode, the radio can not support the connection of wireless clients, and option C is not mandatory for rogue scanning.

upvoted 4 times

🗨️ **S00z** 2 years ago

I think D is definitely correct. On page 177 in study guide, it says "By default, a scan period starts every 600 seconds, and each second a different channel is monitored for 20 ms until all channels have been checked".

Answer A could be correct if it means that the AP is still supporting wireless clients, since you have two radios. Page 176 in study guide says you can have one radio for scanning and one for normal use. But not sure if that is "background scanning".

Answer C could be correct if it means that background scanning is automatically enabled when DARRP is enabled. But the answer does not remotely say that.

I'd go with A and D.

upvoted 1 times

🗨️ **p3dr01n** 2 years, 1 month ago

Selected Answer: AC

- A. YES - Background scanning support wifi clients.
- B. NO - Suppress rogue AP only in dedicated monitor mode
- C. YES - Background rogue scanning requires DARRP
- D. NO - Background scanning only detect on selected channel

upvoted 2 times

🗨️ **DC095** 11 months, 1 week ago

D is correct background scanning spends scans each channel in the given radio's frequency for intervals of 20ms. C is incorrect. Enabling DARRP automatically enables background scanning, but Background scanning can also be enabled via a WIDS profile without DARRP enabled on the WTP profile

upvoted 1 times

🗨️ **zic1** 2 years, 2 months ago

B and D

upvoted 1 times

🗨️ **draven76** 2 years, 6 months ago

Dedicated radios do not do background scanning: A, B and D should be wrong. One of them has to be right, however... Have to check C.

upvoted 1 times

🗨️ **PeteW** 2 years, 11 months ago

I think all the answers are wrong. A dedicated radio per def cannot support clients and does active scanning and not background scanning. A dedicated radio can suppress rogue AP but isn't doing a background scan. Background scanning is enabled if DARRP is implemented but can be enabled without DARRP.

upvoted 3 times

🗨️ **re_john** 2 years, 11 months ago

Selected Answer: BC

B and C

upvoted 1 times

🗨️ **kinge2** 2 years, 11 months ago

Answer is B and C, as per study guide - Background scanning require DARRP for rogue detection. Dedicated monitor allows you to suppress APs with deauth frames.

upvoted 1 times

🗨️ **tochno** 3 years, 2 months ago

C and D are correct.

A is incorrect - dedicated radio doesn't support SSID broadcasting and wireless client connections;

B is incorrect - background scanning doesn't do rogue AP suppression.

upvoted 1 times

When configuring a wireless network for dynamic VLAN allocation, which three IETF attributes must be supplied by the radius server? (Choose three.)

- A. 81 Tunnel-Private-Group-ID
- B. 65 Tunnel-Medium-Type
- C. 83 Tunnel-Preference
- D. 58 Egress-VLAN-Name
- E. 64 Tunnel-Type

Suggested Answer: ABE

The RADIUS user attributes used for the VLAN ID assignment are:

- ⇒ IETF 64 (Tunnel Type) Set this to VLAN.
- ⇒ IETF 65 (Tunnel Medium Type) Set this to 802
- ⇒ IETF 81 (Tunnel Private Group ID) Set this to VLAN ID.

Reference:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-vlan/71683-dynamicvlan-config.html>

Community vote distribution

ABE (100%)

🗨️ **Manuel2493** 4 months, 2 weeks ago

Selected Answer: ABE

Study Guide ABE are correct
upvoted 2 times

🗨️ **draven76** 1 year ago

Selected Answer: ABE

A, B, E is correct
upvoted 1 times

🗨️ **re_john** 1 year, 5 months ago

Selected Answer: ABE

A, B, E
upvoted 1 times

🗨️ **kinge2** 1 year, 5 months ago

81, 64 and 65 is the correct answer
upvoted 1 times

Which two phases are part of the process to plan a wireless design project? (Choose two.)

- A. Project information phase
- B. Hardware selection phase
- C. Site survey phase
- D. Installation phase

Suggested Answer: CD

Reference:

<https://www.sciencedirect.com/topics/computer-science/wireless-site-survey> <https://www.automation.com/en-us/articles/2015-2/wireless-device-network-planning-and-design>

Community vote distribution

AC (100%)

🗨️ 👤 **diaz9019** 5 months ago

Selected Answer: AC

A and C.

upvoted 2 times

🗨️ 👤 **re_john** 1 year, 5 months ago

Selected Answer: AC

A and C

upvoted 2 times

🗨️ 👤 **afons0** 1 year, 8 months ago

A and C are correct (Page 68 of Study Guide)

upvoted 3 times

🗨️ 👤 **tochno** 1 year, 8 months ago

Installation is not a part of design project.

You need to make site survey and select appropriate hardware during design project, so I would say that B and C are correct.

upvoted 1 times

🗨️ 👤 **tochno** 1 year, 8 months ago

I was wrong, correct answers are A and C.

Study guide

upvoted 3 times

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.)

- A. Control channels
- B. Security channels
- C. FortLink channels
- D. Data channels

Suggested Answer: AD

The control channel for managing traffic, which is always encrypted by DTLS. | The data channel for carrying client data packets.



Reference:

[https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ac61f4d3-ce67-11e9-8977-00505692583a/FortiWiFi_and_FortiAP-](https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ac61f4d3-ce67-11e9-8977-00505692583a/FortiWiFi_and_FortiAP-6.2-)

6.2-
Cookbook.pdf

Community vote distribution



AD (100%)

  **p3dr01n** 7 months, 1 week ago

Selected Answer: AD

A D is OK



upvoted 1 times

  **re_john** 1 year, 5 months ago

Selected Answer: AD

A and D

upvoted 1 times

  **kinge2** 1 year, 5 months ago

UDP port 5246 - control channel and UDP port 5247 - Data channel

upvoted 2 times

Part of the location service registration process is to link FortiAPs in FortiPresence.

Which two management services can configure the discovered AP registration information from the FortiPresence cloud? (Choose two.)

- A. AP Manager
- B. FortiAP Cloud
- C. FortiSwitch
- D. FortiGate

Suggested Answer: *BD*

FortiGate, FortiCloud wireless access points (send visitor data in the form of station reports directly to FortiPresence)

Reference:

<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/df877622-c976-11e9-8977-00505692583a/FortiPresence-v4.3-release-notes.pdf>

Community vote distribution

BD (100%)

evilCorpBot7494 8 months, 3 weeks ago

Selected Answer: BD

Answers are B and D. A third correct answer would be FortiWLC.

According to Study guide page 87:

"FortiPresence Cloud - Location Services Configuration

AP can be linked through:

- FortiAP Cloud
- Fortigate
- FortiWLC"

upvoted 1 times

Manuel2493 1 year, 10 months ago

Study Guide P85

BD Are correct

upvoted 3 times

re_john 2 years, 11 months ago

Selected Answer: BD

B and D

upvoted 1 times

kinge2 2 years, 11 months ago

B and D is correct

upvoted 1 times

Which two configurations are compatible for Wireless Single Sign-On (WSSO)? (Choose two.)

- A. A VAP configured for captive portal authentication
- B. A VAP configured for WPA2 or 3 Enterprise
- C. A VAP configured to authenticate locally on FortiGate
- D. A VAP configured to authenticate using a radius server

Suggested Answer: BD

In the SSID choose WPA2-Enterprise authentication.

WSSO is RADIUS-based authentication that passes the user's user group memberships to the FortiGate.

Reference:

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/b92a67f9-73a6-11ea-9384-00505692583a/FortiWiFi_and_FortiAP-6.4.2-Configuration_Guide.pdf

Community vote distribution

BD (100%)

 **tochno** Highly Voted 1 year, 8 months ago

Correct answers are C and D.

In SSID configuration you configure security mode as WPA2/3 enterprise, but after that select authentication lo Local or RADIUS server.
upvoted 5 times

 **Robin997** Most Recent 5 months, 3 weeks ago


Selected Answer: BD

B & D are ok
upvoted 1 times

 **p3dr01n** 7 months ago


Selected Answer: BD

B,D are OK
upvoted 1 times


 **re_john** 1 year, 5 months ago

Selected Answer: BD

B and D
upvoted 1 times

 **kinge2** 1 year, 5 months ago

B and D are correct
upvoted 1 times

 **hrolrh** 1 year, 6 months ago

B D are correct, WSSO dynamically maps remote RADUS users. To use RADIUS, wpa2 wpa3 enterprise mode is needed
upvoted 1 times

Where in the controller interface can you find a wireless client's upstream and downstream link rates?

- A. On the AP CLI, using the cw_diag ksta command
- B. On the controller CLI, using the diag wireless-controller wlac -d sta command
- C. On the AP CLI, using the cw_diag -d sta command
- D. On the controller CLI, using the WiFi Client monitor

Suggested Answer: B

Community vote distribution

A (100%)

🗨️ **Johnny92** 7 months, 1 week ago

Question asks "Controller interface". A is from the AP interface. B is correct.,
upvoted 1 times

🗨️ **Yorkylad** 1 year, 6 months ago

Correct is A (Page 270 of study guide) cw_diag ksta. The key information that is not available anywhere else is the downstream (AP to Client) AND upstream linkrate
upvoted 2 times

🗨️ **p3dr01n** 1 year, 7 months ago

Selected Answer: A

Page 270 of study guide
upvoted 2 times

🗨️ **draven76** 2 years ago

Selected Answer: A

Right answer: A (page 270 of the study guide). afons0 is right.
upvoted 4 times

🗨️ **adiaz_** 2 years, 1 month ago

La A es la correcta
upvoted 1 times

🗨️ **kinge2** 2 years, 5 months ago

A is correct
upvoted 3 times

🗨️ **afons0** 2 years, 8 months ago

Correct is A (Pag 270 of study guide)
upvoted 4 times



Which administrative access method must be enabled on a FortiGate interface to allow APs to connect and function?

- A. Security Fabric
- B. SSH
- C. HTTPS
- D. FortiTelemetry

Suggested Answer: A



Reference:

<https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/788897/configuring-the-root-fortigate-and-downstream-fortigates>

  **adiaz_** 7 months, 1 week ago



A is the correct

upvoted 2 times

  **re_john** 11 months, 2 weeks ago

You must enable Security Fabric connection access on the interface to use CAPWAP.

upvoted 2 times

  **kinge2** 11 months, 3 weeks ago

A is correct

upvoted 3 times

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?

- A. Enable Locate WiFi clients when not connected in the relevant AP profiles.
- B. Enable Monitor channel utilization on the relevant AP profiles.
- C. Ensure that all allowed channels are enabled for the AP radios.
- D. Enable Radio resource provisioning on the relevant AP profiles.

Suggested Answer: *D*

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.

Reference:

<https://docs.fortinet.com/document/fortigate/6.4.0/new-features/228374/add-arrp-profile-for-wireless-controller-6-4-2>

  **kinge2** 5 months, 3 weeks ago

D is correct

upvoted 2 times

Which two roles does FortiPresence analytics assist in generating presence reports? (Choose two.)

- A. Gathering details about on site visitors
- B. Predicting the number of guest users visiting on-site
- C. Comparing current data with historical records
- D. Reporting potential threats by guests on site

Suggested Answer: AB

Reference:

<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/457ebad4-2437-11e9-b20a-f8bc1258b856/FortiPresence-v2.0-getting-started.pdf>

Community vote distribution

AC (100%)

🗉 **Manuel2493** 4 months, 2 weeks ago

Selected Answer: AC

SG P84 A&C Are correct

upvoted 1 times

🗉 **Yorkylad** 6 months, 3 weeks ago

Selected Answer: AC

Correct answers A & C. (Pg84 Study guide)

upvoted 2 times

🗉 **Yorkylad** 6 months, 3 weeks ago

Correct answers A & C. (Pg84 Study guide)

upvoted 1 times

🗉 **p3dr01n** 7 months ago

Selected Answer: AC

Page 84 of study guide

upvoted 1 times

🗉 **kinge2** 1 year, 5 months ago

A and C is correct

upvoted 1 times

🗉 **afons0** 1 year, 8 months ago

Correct is A and C (Pag 84 of study guide)

upvoted 4 times

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

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

Suggested Answer: A

FortiPlanner will look familiar to anyone who has used architectural or home design software.

Reference:

<http://en.hackdig.com/?7883.htm>

Community vote distribution

B (100%)

🗨️ **Yorkylad** 6 months, 3 weeks ago

Selected Answer: B

Answer B is correct

upvoted 1 times

🗨️ **re_j0hn** 1 year, 5 months ago

Predictive design model

upvoted 2 times

🗨️ **kinge2** 1 year, 5 months ago

B is correct

upvoted 1 times

🗨️ **afons0** 1 year, 8 months ago

Correct is B (Pag 72 of study guide)

upvoted 4 times