



HPE6-A85^{Q&As}

Aruba Certified Campus Access Associate

Pass HP HPE6-A85 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/hpe6-a85.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

When performing live firmware upgrades on Aruba APs, which technology partitions all the APs based on RF neighborhood data minimizing the impact on clients?

- A. Aruba ClientMatch
- B. Aruba Ai insights
- C. Aruba AirMatch
- D. Aruba ESP

Correct Answer: C

Explanation: Aruba AirMatch is a feature that optimizes RF Radio Frequency. RF is any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an

electromagnetic field is created that then is able to propagate through space. performance and user experience by using machine learning algorithms and historical data to dynamically adjust AP power levels, channel assignments, and

channel width. AirMatch performs live firmware upgrades on Aruba APs by partitioning all the APs based on RFneighborhood data and minimizing the impact on clients. AirMatch uses a rolling upgrade process that upgrades one partition at a

time while ensuring that adjacent partitions are not upgraded simultaneously.

References:

https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdfhttps://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/arm/AirMatch.htm

QUESTION 2

What happens when the signal from an AP weakens by being absorbed as it moves through an object?

- A. APs will use bonded channels to decrease latency to clients
- B. Signal to Noise Ratio (SNR) increases
- C. Signal to Noise Ratio (SNR) decreases
- D. Aruba Central dynamically moves clients to neighboring APs

Correct Answer: C

Explanation: Signal to noise ratio (SNR) is a measure that compares the level of a desired signal to the level of background noise. SNR is defined as the ratio of signal power to the noise power, often expressed in decibels (dB). A high SNR means that the signal is clear and easy to detect or interpret, while a low SNR means that the signal is corrupted or obscured by noise and may be difficult to distinguish or recover¹. When the signal from an AP Access Point. AP is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. weakens by being absorbed as it moves through an object, such as a wall or a furniture, the signal power decreases. This reduces the SNR and affects the quality of the wireless connection. The noise power may also increase due to



interference from other sources, such as other APs or devices operating in the same frequency band². Therefore, the correct answer is that SNR decreases when the signal from an AP weakens by being absorbed as it moves through an object.

References: 1 https://en.wikipedia.org/wiki/Signal-to-noise_ratio 2 https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_%28SNR%29_and_Wireless_Signal_Strength

QUESTION 3

Which statement is correct when comparing 5 GHz and 6 GHz channels with identical channel widths?

- A. 5 GHz channels travel the same distances and provide different throughputs to clients compared to 6 GHz channels
- B. 5 GHz channels travel different distances and provide different throughputs to clients compared to 6 GHz channels
- C. 5 GHz channels travel the same distances and provide the same throughputs to clients compared to 6 GHz channels
- D. 5 GHz channels travel different distances and provide the same throughputs to clients compared to 6 GHz channels

Correct Answer: B

Explanation: The correct statement when comparing 5 GHz and 6 GHz channels with identical channel widths is that 5 GHz channels travel different distances and provide different throughputs to clients compared to 6 GHz channels. This

statement reflects the fact that higher frequency signals tend to have higher attenuation. Attenuation is a general term that refers to any reduction in signal strength during transmission over distance or through an object or medium. Higher

attenuation means that higher frequency signals have shorter range and lower throughput than lower frequency signals. Some facts about this statement are:

5 GHz channels have lower frequency than 6 GHz channels, which means they have lower attenuation than 6 GHz channels.

Lower attenuation means that 5 GHz channels can travel longer distances and provide higher throughputs to clients than 6 GHz channels with identical channel widths.

However, the difference in distance and throughput between 5 GHz and 6 GHz channels may not be significant in indoor environments where there are many obstacles and reflections that affect signal propagation. The advantage of using 6

GHz channels over 5 GHz channels is that they offer more spectrum availability, less interference, and more non-overlapping channels than 5 GHz channels.

The other options are not correct because:

5 GHz channels travel the same distances and provide different throughputs to clients compared to 6 GHz channels: This option is false because 5 GHz channels do not travel the same distances as 6 GHz channels due to higher attenuation

of higher frequency signals.

5 GHz channels travel the same distances and provide the same throughputs to clients compared to 6 GHz channels: This option is false because 5 GHz channels do not travel the same distances or provide the same throughputs as 6 GHz



channels due to higher attenuation of higher frequency signals. 5 GHz channels travel different distances and provide the same throughputs to clients compared to 6 GHz channels: This option is false because 5 GHz channels do not provide

the same throughputs as

6 GHz channels due to higher attenuation of higher frequency signals.

References: <https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e>

<https://www.wi-fi.org/file/wi-fi-alliance-spectrum-needs-study>

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-power-levels.html>

https://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert-wi-fi/prod_white_paper0900aecd807395a9.html

QUESTION 4

Which authentication does Aruba's Captive Portal use?

- A. Layer 3 authentication
- B. MAC authentication
- C. 802.1x authentication
- D. Layer 2 authentication

Correct Answer: A

Explanation: Aruba's Captive Portal uses Layer 3 authentication, which means that it intercepts the client's HTTP requests and redirects them to a web page where the client can enter their credentials. The credentials are then verified by a RADIUS server or a local database before granting network access.

References: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/captive-portal/captive-portal-auth.htm

QUESTION 5

A network technician has successfully connected to the employee SSID via 802.1X. Which RADIUS message should you look for to ensure a successful connection?

- A. Authorized
- B. Access-Accept
- C. Success
- D. Authenticated

Correct Answer: B

Explanation: The RADIUS message that you should look for to ensure a successful connection via 802.1X is Access-



Accept. This message indicates that the RADIUS server has authenticated and authorized the supplicant (the device that

wants to access the network) and has granted it access to the network resources. The Access-Accept message may also contain additional attributes such as VLAN ID, session timeout, or filter ID that specify how the authenticator (the device

that controls access to the network, such as a switch) should treat the supplicant's traffic. The other options are not RADIUS messages because:

Authorized: This is not a RADIUS message, but a state that indicates that a port on an authenticator is allowed to pass traffic from a supplicant after successful authentication and authorization.

Success: This is not a RADIUS message, but a status that indicates that an EAP Extensible Authentication Protocol (EAP) is an authentication framework that provides support for multiple authentication methods, such as passwords,

certificates, tokens, or biometrics. EAP is used in wireless networks and point-to-point connections to provide secure authentication between a supplicant (a device that wants to access the network) and an authentication server (a device that

verifies the credentials of the supplicant). exchange has completed successfully between a supplicant and an authentication server. Authenticated: This is not a RADIUS message, but a state that indicates that a port on an authenticator has

received an EAP-Success message from an authentication server after successful authentication of a supplicant.

References: <https://en.wikipedia.org/wiki/RADIUS#Access-Accept>

<https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html>

https://en.wikipedia.org/wiki/IEEE_802.1X#Port-based_network_access_control

https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_exchange

[HPE6-A85 Practice Test](#)

[HPE6-A85 Exam Questions](#)

[HPE6-A85 Braindumps](#)