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.leads4pass.com/hpe6-a85.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Match each AAA service with its correct definition (Matches may be used more than once or not at all)

Select and Place:

Correct Answer:

QUESTION 2

Which device configuration group types can a user define in Aruba Central during group creation? (Select two.)

A. Security group

B. Template group

C. Default group

D. Ul group

E. ESP group

Correct Answer: BC

Explanation: Aruba Central allows you to create device configuration groups that define common settings for devices within each group. You can create different types of groupsdepending on your network requirements and management

preferences. Two types of groups that you can define in Aruba Central during group creation are:

Template group: A template group allows you to create configuration templates using variables and expressions that can be applied to multiple devices or device groups. Template groups provide flexibility and scalability for managing

large-

scale deployments with similar configurations.

Default group: A default group is automatically created when you add devices to Aruba Central for the first time. The default group contains basic configuration settings that are applied to all devices that are not assigned to any other group.

You can modify or delete the default group as needed.

References: https://www.arubanetworks.com/techdocs/Central/latest/content/nms/device- groups.htm

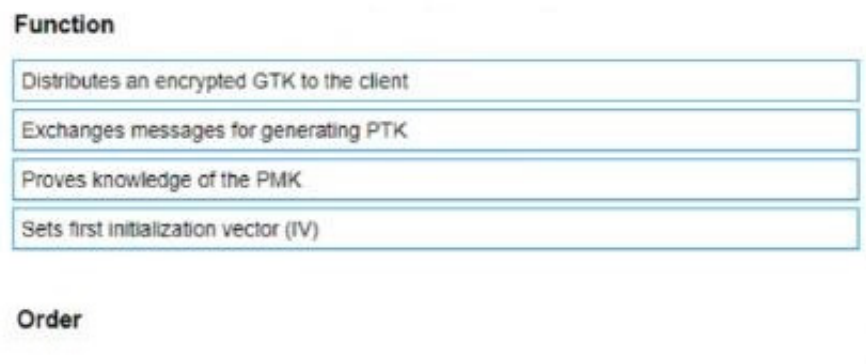
https://www.arubanetworks.com/techdocs/Central/latest/content/nms/template- groups.htm

https://www.arubanetworks.com/techdocs/Central/latest/content/nms/default- group.htm

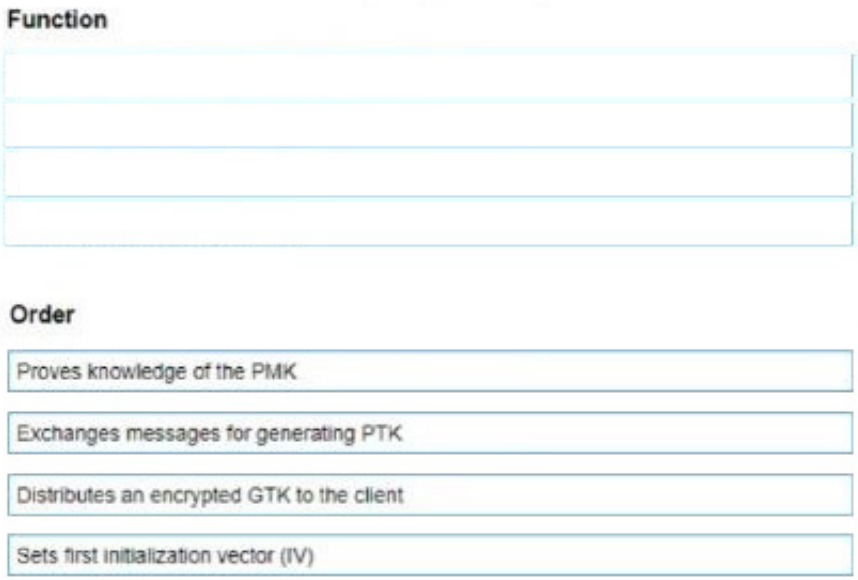
QUESTION 3

List the WPA 4-Way Handshake functions in the correct order.

Select and Place:



Correct Answer:



QUESTION 4

When measuring signal strength, dBm is commonly used and 0 dBm corresponds to 1 mW power.

What does -20 dBm correspond to?

A. .-1 mW

B. .01 mw

C. 10 mW

D. 1mW

Correct Answer: B

Explanation: dBm is a unit of power that measures the ratio of a given power level to 1 mW. The formula to convert dBm to mW is: P(mW) = 1mW * 10^(P(dBm)/10). Therefore, - 20 dBm corresponds to 0.01 mW, as follows: P(mW) = 1mW * 10^(-20/10) = 0.01 mW

References:https://www.rapidtables.com/convert/power/dBm_to_mW.html

QUESTION 5

When using the OSPF dynamic routing protocol on an Aruba CX switch, what must match on the neighboring devices to exchange routes?

A. Hello timers

B. DR configuration

C. ECMP method

D. BDR configuration

Correct Answer: A

Explanation: OSPF Open Shortest Path First. OSPF is a link-state routing protocol that uses a hierarchical structure to create a routing topology for IP networks. OSPF routers exchange routing information with their neighbors using Hello packets, which are sent periodically on each interface. To establish an adjacency Adjacency is a relationship formed between selected neighboring routers for the purpose of exchanging routing information., OSPF routers must agree on several parameters, including Hello timers, which specify how often Hello packets are sent on an interface. If the Hello timers do not match between neighboring routers, they will not form an adjacency and will not exchange routes. References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/osfp/osfp.htm

QUESTION 6

What is the correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1?

A. ip-route 10.2.10.0/24 172.16.1.1

B. ip route 10.2.10.0.255.255.255.0 172.16.1.1 description aruba

C. ip route 10.2.10.0/24.172.16.11

D. ip route-static 10.2 10.0.255.255.255.0 172.16.1.1

Correct Answer: A

Explanation: The correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1 is ip-route 10.2.10.0/24 172.16.1.1 . This command specifies the destination network address (10.2.10.0) and prefix length (/24) and the next-hop address (172.16.1 .1) for reaching that network from the switch. The other commands are either incorrect syntax or incorrect parameters for adding a static route.

References: https://www.arubanetworks.com/techdocs/AOS- CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm

QUESTION 7

What does the status of "ALFOE" mean when checking LACP with "show lacp interfaces\\'"?

A. The interface on the local switch is configured as static-LAG

B. LACP is not configured on the peer side

C. LACP is in a synchronizing process

D. LACP is working fine with no problems

Correct Answer: D

Explanation: The status of "ALFOE" means that LACP Link Aggregation Control Protocol (LACP) is a network protocol that provides dynamic negotiation of link aggregation between two devices. LACP allows multiple physical links to be

combined into a single logical link for increased bandwidth, redundancy, and load balancing. LACP is defined in IEEE 802.3ad standard. is working fine with no problems when checking LACP with "show lacp interfaces". The status of "ALFOE" is an acronym that stands for:

A: Active - The interface is actively sending LACP packets to negotiate link aggregation with the peer device.

L: Link Up - The interface has physical connectivity with the peer device.

F: Aggregatable - The interface can be aggregated with other interfaces into a single logical link.

O: Synchronized - The interface has successfully negotiated link aggregation parameters with the peer device and can transmit or receive traffic on the logical link.

E: Collecting/Distributing - The interface is collecting incoming traffic from the peer device and distributing outgoing traffic to the peer device on the logical link.

The other options are not correct because:

The interface on the local switch is configured as static-LAG: This option is false because static-LAG does not use LACP to negotiate link aggregation. Static-LAG requires manual configuration of link aggregation parameters on both devices

and does not have any status indicators.

LACP is not configured on the peer side: This option is false because if LACP is not configured on the peer side, the status of the interface would be "ALF? instead of "ALFOE". This means that the interface would not be synchronized or

collecting/distributing with the peer device.

LACP is in a synchronizing process: This option is false because if LACP is in a synchronizing process, the status of the interface would be "ALF-O" instead of "ALFOE". This means that the interface would not be collecting/distributing with

the peer device.

References: https://www.arubanetworks.com/techdocs/AOS- CX_10_08/NOSCG/Content/cx-noscg/lag/lag-overview.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/lag/lag-lacp.htm https:// www.arubanetworks.com/techdocs/AOS- CX_10_08/NOSCG/Content/cx-noscg/lag/lag-lacp-status.htm

---

QUESTION 8

What does WPA3-Personal use as the source to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network?

A. Session-specific information (MACs and nonces)

B. Opportunistic Wireless Encryption (OWE)

C. Simultaneous Authentication of Equals (SAE)

D. Key Encryption Key (KEK)

Correct Answer: A

Explanation: The source that WPA3-Personal uses to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network is session-specific information (MACs and nonces). WPA3-Personal uses

Simultaneous Authentication of Equals (SAE) to replace PSK authentication in WPA2-Personal. SAE is a secure key establishment protocol that uses a Diffie-Hellman key exchange to derive a shared secret between two parties without

revealing it to an eavesdropper. SAE involves the following steps:

The station and the access point exchange Commit messages that contain their MAC addresses and random numbers called nonces.

The station and the access point use their own passwords and the received MAC addresses and nonces to calculate a shared secret called SAE Password Element (PE).

The station and the access point use their own PE and the received MAC addresses and nonces to calculate a shared secret called SAE Key Seed (KS). The station and the access point use their own KS and the received MAC addresses

and nonces to calculate a shared secret called SAE Key Confirmation Key (KCK).

The station and the access point use their own KCK and the received MAC addresses and nonces to calculate a confirmation value called SAE Confirm. The station and the access point exchange Confirm messages that contain their SAE

Confirm values.

The station and the access point verify that the received SAE Confirm values match their own calculated values. If they match, the authentication is successful and the station and the access point have established a shared secret called SAE

PMK.

The SAE PMK is different for each session because it depends on the MAC addresses and nonces that are exchanged in each authentication process. The SAE PMK is used as an input for the 4-way handshake that generates the Pairwise

Temporal Key (PTK) for encrypting data frames.

The other options are not sources that WPA3-Personal uses to generate a different PMK each time a station connects to the wireless network because:

Opportunistic Wireless Encryption (OWE): OWE is a feature that provides encryption for open networks without requiring authentication or passwords. OWE uses a similar key establishment protocol as SAE, but it does not generate a PMK.

Instead, it generates a Pairwise Secret (PS) that is used as an input for the 4-way handshake that generates the PTK.

Simultaneous Authentication of Equals (SAE): SAE is not a source, but a protocol that uses session-specific information as a source to generate a different PMK each time a station connects to the wireless network. Key Encryption Key (KEK): KEK is not a source, but an output of the 4-way handshake that generates the PTK. KEK is used to encrypt group keys that are distributed by the access point.

References: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e https://www.wi-fi.org/file/wi- fi-alliance-unlicensed-spectrum-in-the-us https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access- points/wpa3-dep-guide-og.html https://info.support.huawei.com/info- finder/encyclopedia/en/WPA3.html https://rp.os3.nl/2019-2020/p99/presentation.pdf

QUESTION 9

What are two advantages of a UXI? (Select two.)

A. A UXI can be used without any internet connection

B. A UXI helps to calculate the best WiFi channels in a remote location

C. A UXI behaves like a client/user

D. A UXI measures the Wi-Fi coverage of all APs in the given location.

E. A UXI can check different applications, such as HTTP VOIP or Office 365.

Correct Answer: CE

Explanation: A UXI (User Experience Insight) is a device that simulates user behavior and tests network performance from the user perspective. It can check different applications, such as HTTP, VOIP, or Office 365, and measure metrics

such as latency, jitter, packet loss, and throughput.

References:https://www.arubanetworks.com/products/networking/user-experience-insight/

QUESTION 10

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 thenetwork) 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