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

What is a weakness introduced into the WLAN environment when WPA2-Personal is used for security?

A. It uses X 509 certificates generated by a Certification Authority

B. The Pairwise Temporal Key (PTK) is specific to each session

C. The Pairwise Master Key (PMK) is shared by ail users

D. It does not use the WPA 4-Way Handshake

Correct Answer: C

Explanation: The weakness introduced into WLAN environment when WPA2-Personal is used for security is that PMK Pairwise Master Key (PMK) is a key that is derived from PSK Pre-shared Key (PSK) is a key that is shared between two parties before communication begins , which are both fixed. This means that all users who know PSK can generate PMK without any authentication process. This also means that if PSK or PMK are compromised by an attacker, they can be used to decrypt all traffic encrypted with PTK Pairwise Temporal Key (PTK) is a key that is derived from PMK, ANonce AuthenticatorNonce (ANonce) is a random number generated by an authenticator (a device that controls access to network resources, such as an AP), SNonce Supplicant Nonce (SNonce) is a random number generated by supplicant (a device that wants to access network resources, such as an STA), AA Authenticator Address (AA) is MAC address of authenticator, SA Supplicant Address (SA) is MAC address of supplicant using Pseudo-Random Function (PRF). PTK consists of four subkeys: KCK Key Confirmation Key (KCK) is used for message integrity check, KEK Key Encryption Key (KEK) is used for encryption key distribution, TK Temporal Key (TK) is used for data encryption, MIC Message Integrity Code (MIC) key. . The other options are not weaknesses because: It uses X 509 certificates generated by a Certification Authority: This option is false because WPA2-Personal does not use X 509 certificates or Certification Authority for authentication. X 509 certificates and Certification Authority are used in WPA2- Enterprise mode, which uses 802.1X and 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). for user authentication with a RADIUS server Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service . The Pairwise Temporal Key (PTK) is specific to each session: This option is false because PTK being specific to each session is not a weakness but a strength of WPA2-Personal. PTK being specific to each session means that it changes periodically during communication based on time or number of packets transmitted. This prevents replay attacks and increases security of data encryption. It does not use the WPA 4-Way Handshake: This option is false because WPA2- Personal does use the WPA 4-Way Handshake for key negotiation. The WPA 4- Way Handshake is a process that allows the station and the access point to exchange ANonce and SNonce and derive PTK from PMK. The WPA 4-Way Handshake also allows the station and the access point to verify each other\\'s PMK and confirm the installation of PTK.

References: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management https://www.cwnp.com/wp- content/uploads/pdf/WPA2.pdf

QUESTION 2

What is the ideal Aruba access switch for a cost-effective connection to 200-380 clients, printers and APs per distribution rack?

A. Aruba CX 6400

B. Aruba CX 6200

C. Aruba CX 6300

D. Aruba CX 6000

Correct Answer: B

The ideal Aruba access switch for a cost-effective connection to 200-380 clients, printers and APs per distribution rack is the Aruba CX 6200. This switch series is a cloud- manageable, stackable access switch series that is ideal for enterprise

branch offices and campus networks, as well as SMBs. The CX 6200 series offers the following benefits:

Enterprise-class connectivity: The CX 6200 series supports ACLs, robust QoS, and common protocols such as static and Access OSPF routing. Power and speed for users and IoT: The CX 6200 series provides built-in 1/10GbE uplinks and

30W to 60W of Class 4 to Class 6 PoE for powering devices such as APs and cameras.

Scalable growth made simple: The CX 6200 series supports Aruba Virtual Switching Framework (VSF) that allows you to quickly grow your network to eight members in a single stack using high-performance built-in 10G SFP ports.

Management flexibility: The CX 6200 series supports a choice of management, including cloud-based and on-prem Central, CLI, switch Web GUI and programmability with AOS-CX operating system, and REST APIs.

The other options are not ideal because:

Aruba CX 6400: This switch series is a high-availability modular switch series that is ideal for versatile edge access to data center deployments. It offers more performance, scalability, and modularity than the CX 6200 series, but it is also

more expensive and complex to deploy and manage. It may not be cost-effective for connecting 200-380 clients per distribution rack. Aruba CX 6300: This switch series is a layer 3 stackable access and aggregation switch series that offers

Smart Rate and High Power PoE. It offers more features and performance than the CX 6200 series, but it is also more expensive and may not be necessary for connecting 200-380 clients per distribution rack. Aruba CX 6000: This switch

series is a layer 2 access switch series that offers PoE. It offers less features and performance than the CX 6200 series, and it does not support VSF stacking or routing protocols. It may not be sufficient for connecting 200-380 clients per

distribution rack.

References: https://www.arubanetworks.com/products/switches/access/

https://www.arubanetworks.com/products/switches/access/6200-series/

https://www.arubanetworks.com/products/switches/access/6400-series/

https://www.arubanetworks.com/products/switches/access/6300-series/

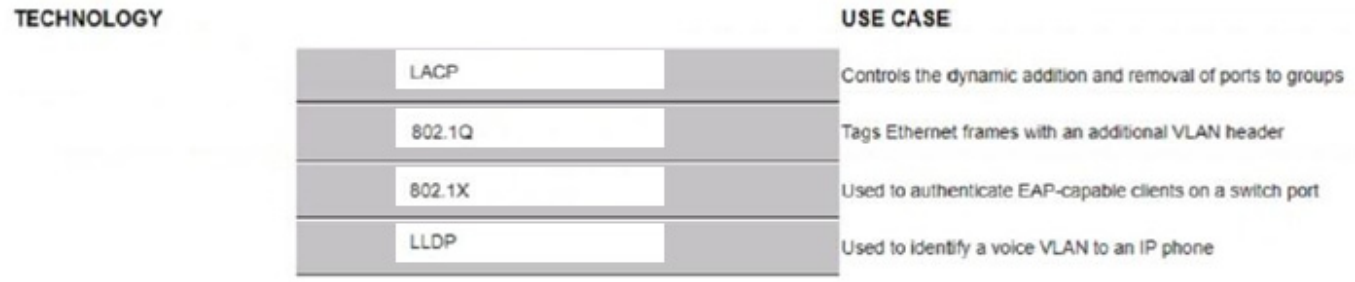
https://www.arubanetworks.com/products/switches/access/6000-series/

QUESTION 3

Match the switching technology with the appropriate use case.

Select and Place:

Correct Answer:



QUESTION 4

You need to configure wireless access for several classes of loT devices, some of which operate only with 802 11b. Each class must have a unique PSK and will require a different security policy applied as a role There will be 15-20 different classes of devices and performance should be optimized

Which option fulfills these requirements\\'\\'

A. Single SSID with MPSK for each loT class using 5 GHz and 6 GHz bands

B. Single SSID with MPSK for each loT class using 2.4GHz and 5 GHz bands

C. Individual SSIDs with unique PSK for each loT class, using 5GHz and 6 GHz bands

D. Individual SSIDs with unique PSK for each loT class, using 2.4GHZ and 5GHz band

Correct Answer: D

Explanation: The option that fulfills the requirements is to create individual SSIDs with unique PSK for each loT class, using 2.4 GHz and 5 GHz band. This option provides the following benefits:

Each loT class has a unique PSK that can be used to apply a different security policy as a role. This enhances the security and flexibility of the WLAN network. Individual SSIDs allow for better isolation and management of different loT

classes. This improves the performance and scalability of the WLAN network. Using both 2.4 GHz and 5 GHz bands

allows for backward compatibility with IoT devices that operate only with 802.11b, which uses the 2.4 GHz band1. It also

allows for higher throughput and less interference for IoT devices that support 802.11a, 802.11g, 802.11n, or 802.11ac, which use the 5 GHz band2. The other options do not fulfill the requirements because:

Single SSID with MPSK for each IoT class using 5 GHz and 6 GHz bands: This option does not support IoT devices that operate only with 802.11b, which uses the 2.4 GHz band1. It also does not optimize the performance of the WLAN

network, as a single SSID may cause co-channel interference and congestion among different IoT classes.

Single SSID with MPSK for each IoT class using 2.4 GHz and 5 GHz bands: This option does not optimize the performance of the WLAN network, as a single SSID may cause co-channel interference and congestion among different IoT

classes. Individual SSIDs with unique PSK for each IoT class, using 5 GHz and 6 GHz bands: This option does not support IoT devices that operate only with 802.11b, which uses the 2.4 GHz band1.

References: 1 https://en.wikipedia.org/wiki/IEEE_802.11b-1999 2 https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553

QUESTION 5

You need to drop excessive broadcast traffic on ingress to an ArubaOS-CX switch What is the best technology to use for this task?

A. Rate limiting

B. DWRR queuing

C. QoS shaping

D. Strict queuing

Correct Answer: A

Explanation: The best technology to use for dropping excessive broadcast traffic on ingress to an ArubaOS-CX switch is rate limiting. Rate limiting is a feature that allows network administrators to control the amount of traffic that enters or leaves a port or a VLAN on a switch by setting bandwidth thresholds or limits. Rate limiting can be used to prevent network congestion, improve network performance, enforce service level agreements(SLAs), or mitigate denial-of-service (DoS) attacks. Rate limiting can be applied to broadcast traffic on ingress to an ArubaOS-CX switch by using the storm-control command in interface configuration mode. This command allows network administrators to specify the percentage of bandwidth or packets per second that can be used by broadcast traffic on an ingress port. If the broadcast traffic exceeds the specified threshold, the switch will drop the excess packets. The other options are not technologies for dropping excessive broadcast traffic on ingress because: DWRR queuing: DWRR stands for Deficit Weighted Round Robin, which is a queuing algorithm that assigns different weights or priorities to different traffic classes or queues on an egress port. DWRR ensures that each queue gets its fair share of bandwidth based on its weight while avoiding starvation of lower priority queues. DWRR does not drop excessive broadcast traffic on ingress, but rather schedules outgoing traffic on egress. QoS shaping: QoS stands for Quality of Service, which is a set of techniques that manage network resources and provide different levels of service to different types of traffic based on their requirements. QoS shaping is a technique that delays or buffers outgoing traffic on an egress port to match the available bandwidth or rate limit. QoS shaping does not drop excessive broadcast traffic on ingress, but rather smooths outgoing traffic on egress. Strict queuing: Strict queuing is another queuing algorithm that assigns different priorities to different traffic classes or queues on an egress port. Strict queuing ensures that higher priority queues are always served before lower priority queues regardless of their bandwidth requirements or weights. Strict queuing does not drop

excessive broadcast traffic on ingress, but rather schedules outgoing traffic on egress.

References: https://en.wikipedia.org/wiki/Rate_limiting https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/qos/storm-control.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/dwrr.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx- noscg/qos/shaping.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/strict.htm