Aruba Certified Mobility Associate (ACMA) Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which role does a controller play in a wireless networking environment?

A. Managing network traffic

B. Enhancing encryption

C. Providing internet access

D. Offering firewall protection

2. Which of the following cannot be accomplished from the startup wizard?

A. VPN Configuration

B. AP Configuration

C. Network Setup

D. Security Settings

3. Where in the controller would we configure a wireless network to not use encryption?

A. Policy profile

B. SSID profile

C. Access Point profile

D. Global settings

4. What is essential for performance optimization in an access point?

A. Firmware Updates

B. Parallel Processing

C. Mesh Networking

D. Access Control Lists

5. Which one of the following file types cannot be imported to Visual RF Plan?

A. png

B. pdf

C. tiff

D. jpg

6. What is the primary difference between "Policy" and "Role" in Aruba's architecture?

- **A. Policies define device types, while roles determine traffic paths**
- **B. Policies dictate permissions based on roles, which define user or device identity**
- **C. Roles manage network segments, while policies enforce authentication measures**
- **D. Policies are user-based, and roles are device-based permissions**

7. What role does the “Unified Wireless” feature play in Aruba solutions?

- **A. It enhances wireless signal strength**
- **B. It integrates wired and wireless access into one seamless network**
- **C. It provides wireless fallback in wired networks**
- **D. It excludes wireless access from enterprise networks**

8. What is the primary purpose of dual-band access points in Aruba?

- **A. To enhance security protocols**
- **B. To provide connectivity for legacy devices**
- **C. To increase capacity and performance using 2.4 GHz and 5 GHz bands**
- **D. To simplify network management**

9. What is the purpose of Aruba’s ClearPass Policy Manager?

- **A. To monitor network bandwidth usage.**
- **B. To provide policy-based network access control and guest management.**
- **C. To manage firmware updates for devices.**
- **D. To automatically decrypt network traffic.**

10. What is the strongest encryption type mentioned in mobility solutions?

A. WEP

B. TKIP

C. DES

D. AES

Answers

1. A
2. A
3. B
4. A
5. C
6. B
7. B
8. C
9. B
10. D

Explanations

1. Which role does a controller play in a wireless networking environment?

A. Managing network traffic

B. Enhancing encryption

C. Providing internet access

D. Offering firewall protection

The role of a controller in a wireless networking environment primarily revolves around managing network traffic. A controller is responsible for centralizing the management of access points and coordinating their activities. This includes monitoring network performance, load balancing, and ensuring that devices are properly authenticated and connected to the network. By managing network traffic effectively, the controller can optimize the performance of the wireless network, minimize interference, and ensure efficient use of bandwidth across different access points and services. The other roles listed, such as enhancing encryption, providing internet access, and offering firewall protection, may be functions of different components within the network but are not directly tied to the primary responsibilities of a controller. While a controller can play a role in security by managing encryption settings or facilitating secure communication, its main focus is on traffic management and network efficiency.

2. Which of the following cannot be accomplished from the startup wizard?

A. VPN Configuration

B. AP Configuration

C. Network Setup

D. Security Settings

The startup wizard is designed to streamline initial configuration tasks for Aruba devices, making it user-friendly for administrators who may not be deeply familiar with the technical intricacies of the system. It typically covers essential aspects of setting up a network environment, including the basic configuration of access points (AP), network settings, and preliminary security feature activation. VPN configuration is generally more complex and involves specific settings that go beyond what the startup wizard can manage. VPNs require detailed information regarding tunneling protocols, authentication types, and other variables that need careful optimization depending on the organizational requirements and infrastructure specifics. This complexity is why the startup wizard does not accommodate VPN configuration. In contrast, AP configuration, network setup, and security settings are fundamental network services that can be simplified and included in the startup wizard. The objective of the wizard is to get the system up and running with essential configurations, which includes enabling access points, establishing basic network parameters, and implementing initial security measures.

3. Where in the controller would we configure a wireless network to not use encryption?

A. Policy profile

B. SSID profile

C. Access Point profile

D. Global settings

The configuration of a wireless network to either use or not use encryption is handled primarily within the SSID profile. The SSID (Service Set Identifier) profile contains settings that govern the characteristics of the wireless network, including security measures such as encryption protocols. When you want to configure a wireless network to operate without encryption, you specifically set this within the SSID profile. This profile allows you to define the type of security being implemented for the wireless clients that will connect to that particular SSID. By selecting "open" or no encryption as part of the SSID profile settings, you can enable access without requiring a security key, which is essential when deliberately allowing unencrypted access. In contrast, other profiles such as the policy profile focus on user roles and application policies, the access point profile pertains to configurations related to specific access points (like radio settings or VLAN assignments), and global settings affect the controller's overall configuration without directly managing individual SSIDs. Therefore, the SSID profile is the most direct and relevant section for specifying whether a wireless network should use encryption or not.

4. What is essential for performance optimization in an access point?

A. Firmware Updates

B. Parallel Processing

C. Mesh Networking

D. Access Control Lists

For performance optimization in an access point, firmware updates are crucial because they ensure that the device is running the latest software, which often includes enhancements and bug fixes that can improve functionality and performance. Updating firmware can resolve known issues that affect stability and efficiency, enhance security, and improve compatibility with new devices and technologies. Manufacturers frequently release updates to optimize the performance of their hardware, so staying current with these updates can help maintain the overall network performance and user experience. Other options, while useful in certain contexts, do not directly relate to the performance optimization of an access point. Parallel processing may enhance data handling in specific scenarios but is not a defining factor in how access points operate. Mesh networking provides extended coverage and reliability but concerns network topology rather than individual access point performance. Access control lists are important for security and managing access but do not directly contribute to performance optimization in the same way that firmware updates do.

5. Which one of the following file types cannot be imported to Visual RF Plan?

A. png

B. pdf

C. tiff

D. jpg

The ability to import files into Visual RF Plan is quite specific, and certain formats are supported while others are not. The correct answer indicates that TIFF files cannot be imported into Visual RF Plan. This is primarily due to the nature of the TIFF format, which is often used for high-quality images and doesn't typically align with the types of files needed for visualization and planning within the software. Visual RF Plan is designed to handle 2D and 3D mapping and typically prefers bitmap formats that are easier to handle for the kind of analysis and planning it performs, such as PNG and JPG, which are more prevalent for web use and imaging. Additionally, PDF files may also be supported as they can contain vector data and drawings useful for planning, while both PNG and JPG formats are efficient for images used in site planning and design processes. Understanding these distinctions helps in selecting the appropriate file types when preparing plans and layouts in visual RF applications.

6. What is the primary difference between "Policy" and "Role" in Aruba's architecture?

A. Policies define device types, while roles determine traffic paths

B. Policies dictate permissions based on roles, which define user or device identity

C. Roles manage network segments, while policies enforce authentication measures

D. Policies are user-based, and roles are device-based permissions

The primary difference between "Policy" and "Role" in Aruba's architecture lies in their respective functions regarding user access and permissions. Policies are designed to dictate permissions and access controls based on the roles assigned to users or devices. A role serves as a category that identifies a user or device within the network, while the policy specifies what that role can do once authenticated. This means that the policy enforces specific rules, such as what resources can be accessed, the types of actions that can be performed, and any restrictions that apply based on the role. This understanding is critical in network management since establishing clear roles helps in defining access policies that align with an organization's security protocols. It allows network administrators to quickly and efficiently manage permissions based on established roles, ensuring that users and devices have the appropriate level of access without compromising security.

7. What role does the “Unified Wireless” feature play in Aruba solutions?

A. It enhances wireless signal strength

B. It integrates wired and wireless access into one seamless network

C. It provides wireless fallback in wired networks

D. It excludes wireless access from enterprise networks

The "Unified Wireless" feature in Aruba solutions plays a crucial role in integrating wired and wireless access into one seamless network. This integration allows for consistent user experiences across various types of access, leading to improved network efficiency and management. With Unified Wireless, clients can connect to the network without worrying about the underlying infrastructure—whether they are connected wirelessly or through a wired connection, the network operates as a cohesive entity. This approach simplifies network administration and allows for better resource utilization, making it easier to manage security policies, Quality of Service (QoS), and traffic management within a single network framework. It essentially unifies the management of both types of connections, providing a holistic view of the network status, performance, and security. The other options focus on different aspects that are either too narrow or don't align with the main purpose of Unified Wireless. For instance, enhancing signal strength is typically addressed through hardware improvements like antennas and transmitters, and providing wireless fallback does not capture the full scope of integrating wired and wireless networks effectively. Additionally, excluding wireless access contradicts the very nature of what Unified Wireless aims to achieve, which is full integration rather than exclusion.

8. What is the primary purpose of dual-band access points in Aruba?

A. To enhance security protocols

B. To provide connectivity for legacy devices

C. To increase capacity and performance using 2.4 GHz and 5 GHz bands

D. To simplify network management

The primary purpose of dual-band access points in Aruba is to increase capacity and performance by utilizing both the 2.4 GHz and 5 GHz frequency bands. This dual-band capability allows for more efficient management of bandwidth, as the 2.4 GHz band offers wider coverage and better penetration through obstacles, while the 5 GHz band supports higher data rates and less interference due to its additional channels. By operating on both bands simultaneously, dual-band access points can accommodate a larger number of devices and distribute network traffic more effectively, leading to improved overall performance. This is especially important in environments where many users are connected to the network, as it helps to alleviate congestion and ensures a more reliable experience for all devices. This combination optimizes network efficiency and enhances user experience, which is critical in today's advanced wireless environments where multiple devices are simultaneously accessing the network. The other choices, while relevant to various network functionalities, do not directly address the fundamental role of dual-band access points in enhancing network capacity and performance through the use of multiple frequency bands.

9. What is the purpose of Aruba's ClearPass Policy Manager?

A. To monitor network bandwidth usage.

B. To provide policy-based network access control and guest management.

C. To manage firmware updates for devices.

D. To automatically decrypt network traffic.

The purpose of Aruba's ClearPass Policy Manager is to provide policy-based network access control and guest management. This tool enables organizations to establish and enforce security policies for users and devices attempting to connect to the network. It operates by authenticating users, which can include employees, guests, and IoT devices, ensuring that only authorized users gain access to the network according to predetermined policies. This capability helps maintain network security by defining who can access what, and under what conditions. Additionally, ClearPass offers guest management features that facilitate the onboarding process for visitors, allowing them to connect to the network easily while maintaining security protocols. Through role-based access controls, ClearPass can tailor network access permissions based on user roles, device types, or other criteria, effectively managing diverse user populations within an enterprise environment. While monitoring network bandwidth usage, managing firmware updates, and decrypting network traffic are important functions in network management and security, they do not encapsulate the primary function of the ClearPass Policy Manager, which is centered around access control and policy enforcement.

10. What is the strongest encryption type mentioned in mobility solutions?

A. WEP

B. TKIP

C. DES

D. AES

AES, or Advanced Encryption Standard, is recognized as the strongest encryption type among the options listed in mobility solutions. It was established by the U.S. National Institute of Standards and Technology (NIST) and has become the standard for securing data across various platforms and applications. The strength of AES lies in its design, which allows it to use key sizes of 128, 192, and 256 bits, making it significantly more secure than older encryption methods. AES is resistant to most forms of attack, including brute-force attacks, thanks to its robust key structure and encryption process. This level of security is essential in mobility solutions where data integrity and confidentiality are crucial. In contrast, WEP (Wired Equivalent Privacy) and TKIP (Temporal Key Integrity Protocol) are older encryption protocols that have well-documented vulnerabilities, making them less secure. DES (Data Encryption Standard) is also considered outdated, as it utilizes a shorter key length and has been largely replaced by AES due to its inherent weaknesses. Therefore, AES stands out as the most secure option, making it the preferred choice for modern mobility solutions.