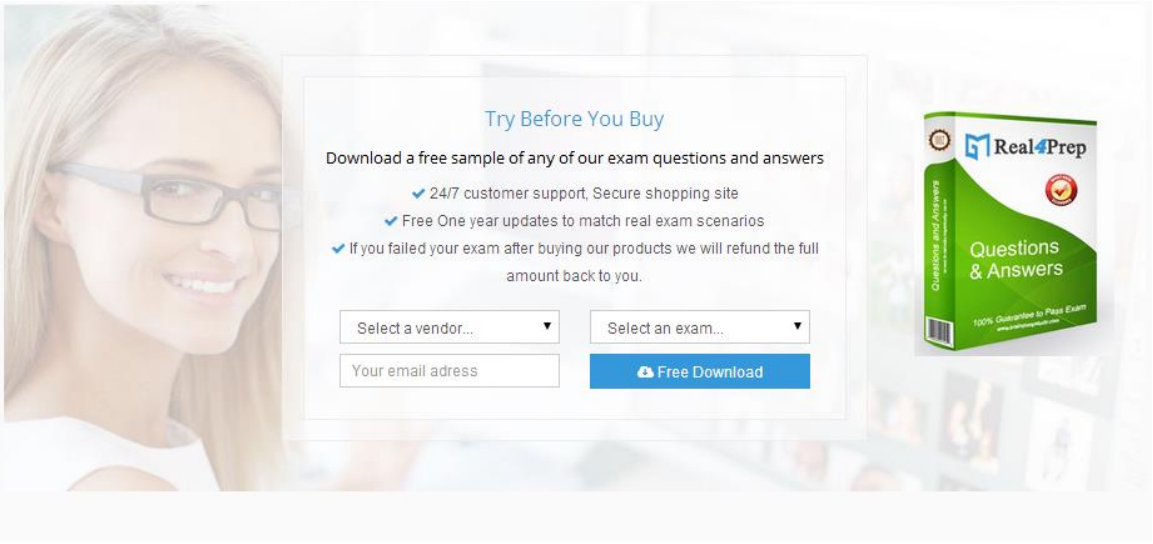
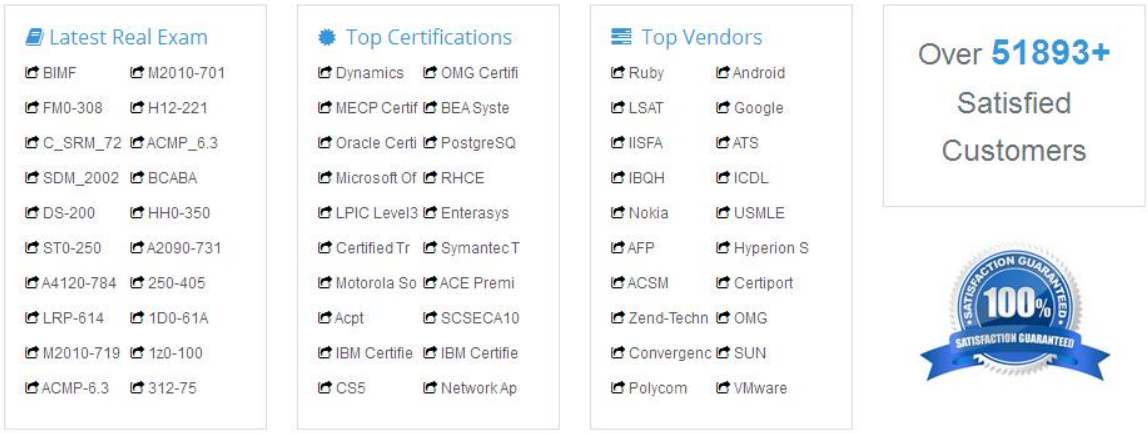
Real4Prep





http://www.real4prep.com

Latest Real Exam Prep Dumps for IT Exam Preparation

Exam : **HPE6-A47**

Title : Aruba Certified Design Professional Exam

Vendor : HP

Version : DEMO

NO.1 An architect proposes an Aruba wireless solution for a customer that uses Microsoft Skype for Business. What should be set up on the MCs, or MM, to ensure that wireless voice traffic is properly prioritized?

A. Firewall policies and SDN to mark voice

B. Broadcast suppression combined with AirGroup

C. Airtime Fairness set to fair-access

D. Voice-aware Layer 3 roaming

Answer: A

Explanation:

To ensure that wireless voice traffic is properly prioritized for Microsoft Skype for Business, the architect should set up firewall policies and SDN to mark voice on the MCs or MM. Firewall policies are used to classify and prioritize traffic based on the application, user role, device type, and location. SDN is used to integrate with the Skype for Business SDN API, which provides real-time information about voice and video sessions, such as source and destination IP addresses, ports, codecs, and quality metrics. By using firewall policies and SDN, the MCs or MM can dynamically mark voice traffic with the appropriate DSCP values and queue them in the highest priority queue on the wireless and wired network12.

The other options are not sufficient or relevant for ensuring wireless voice traffic prioritization for Skype for Business. Broadcast suppression combined with AirGroup is used to reduce the network overhead and improve the user experience for wireless devices that use multicast or broadcast protocols, such as Apple Bonjour or Microsoft UPnP3. Airtime Fairness set to fair-access is used to balance the airtime usage among clients with different capabilities and data rates, such as 802.11ac and 802.11n4. Voice-aware Layer 3 roaming is used to enable seamless handoff of voice sessions across different subnets without dropping the call5. While these features may enhance the overall wireless performance and reliability, they do not directly prioritize voice traffic for Skype for Business .

References:

Aruba Validated Reference Design: 802.11ac Networks

Aruba Validated Reference Design: Skype for Business

Aruba Validated Reference Design: AirGroup

Aruba Validated Reference Design: Adaptive Radio Management

Aruba Validated Reference Design: Voice over Wireless LAN

NO.2 The customer has an office environment with users who have laptops that can connect with wired or wireless.

Users also bring one or two of their own devices. An architect creates a proposal with Aruba AP-325s, 7210 Mobility Controllers (MCs), a Mobility Master (MM), and Aruba 2930M switches at the access layer to support the laptops and APs.

The architect plans to recommend 802.1X authentication without tunnelled node on Aruba 2930M switch ports that connect to laptops. What is one advantage of this form of authentication?

A. ensures that Aruba firewall policies apply to wired user traffic.

B. prevents users from connection attempts with more than three devices

C. enables user access control and ensures only authorized users connect.

D. provides a second layer of protection for wireless users at the internal perimeter

Answer: C

Explanation:
802.1X authentication without tunnelled node is a form of port-based network access control that uses the Extensible Authentication Protocol (EAP) to authenticate users and devices on a wired network. This form of authentication provides several benefits, such as:
It enables user access control and ensures only authorized users connect. This prevents unauthorized access to the network and its resources, and enhances security and compliance.
It allows dynamic assignment of VLANs and roles based on user identity and device type. This simplifies network management and improves user experience.
It supports multiple authentication methods, such as certificates, passwords, tokens, or biometrics. This provides flexibility and choice for users and administrators.
It integrates with Aruba ClearPass Policy Manager (CPPM) for centralized policy enforcement and visibility. This enables granular control and monitoring of wired user traffic and devices. References:
Aruba 2930M Switch Series - Data sheet)
Aruba ClearPass Policy Manager - Data sheet)
ArubaOS-Switch Wired Access with ClearPass - Configuration guide)

NO.3 An architect proposes the following Aruba solutions:
Two Virtual Mobility Masters (VMMs)
Six 7030 Mobility Controllers (MCs)
300 APs
In addition to any necessary AP, PEF, and RFP licenses, which license package should the architect propose?

A. six LIC-MM-VA-50

B. one LIC-MC-VA-250 and one LIC-MC-VA-50; one LIC-MM-VA-500

C. one LIC-MM-VA-500

D. one LIC-MC-VA-250 and one LIC-MC-VA-50; six LIC-MM-VA-500

Answer: C

Explanation:
The architect should propose one LIC-MM-VA-500 license package for the customer. This license package allows the customer to deploy up to two VMMs and manage up to 500 MCs and 10,000 APs. The customer does not need any additional licenses for the MCs or the APs, as they are included in the LIC-MM-VA-500 package. The other options are either insufficient or excessive for the customer's needs.
Option A is insufficient because six LIC-MM-VA-50 licenses only allow the customer to manage up to 300 MCs and 6,000 APs. The customer needs to manage 300 APs and six MCs, so this option does not meet the requirement.
Option B is excessive because one LIC-MC-VA-250 and one LIC-MC-VA-50 licenses allow the customer to deploy up to 300 MCs and 6,000 APs, which is more than what the customer needs.
Moreover, one LIC-MM-VA-500 license allows the customer to deploy up to two VMMs and manage up to 500 MCs and 10,000 APs, which is also more than what the customer needs. Therefore, this option is wasteful and unnecessary.
Option D is also excessive because one LIC-MC-VA-250 and one LIC-MC-VA-50 licenses allow the customer to deploy up to 300 MCs and 6,000 APs, which is more than whatthe customer needs.
Additionally, six LIC-MM-VA-500 licenses allow the customer to deploy up to 12 VMMs and manage up to 3,000 MCs and 60,000 APs, which is way more than what the customer needs. Therefore, this option is also wasteful and unnecessary.

References:
ArubaOS 8.5 Licensing Guide)
Aruba Mobility Master Data Sheet)
Aruba 7000 Series Mobility Controllers Data Sheet)

NO.4 What should an architect use as a guideline to determine when to define another VLAN for wireless devices?
A. the WLAN or SSID, with a different VLAN for each SSID
B. the AP deployment, with a different VLAN for each AP that is deployed
C. the number of devices, with a different VLAN for each 250 devices
D. the employee roles, with a different VLAN for each role or department
Answer: D
Explanation:
The guideline for defining another VLAN for wireless devices should be based on the employee roles, with a different VLAN for each role or department. This approach allows for better control and management of network resources. It also enhances security by segregating network traffic based on roles or departments. This is particularly useful in large organizations where different departments may have different network requirements and security levels12.
References:
Configuring VLANs - Aruba
TECH BRIEF SINGLE VLAN DESIGN FOR WIRELESS LAN - Aruba

NO.5 An architect has an Instant AP (IAP) cluster at a mid-sized branch office. The IAP cluster now needs to tunnel corporate traffic to a Mobility Controller (MC) at the main office. However, the branch office should remain functional even if the link to the main office fails. Users at the branch office require access to main office resources, but do not require multicast services.
What is the recommended DHCP mode?
A. Local
B. Centralized L2
C. Distributed L2
D. Distributed L3
Answer: A
Explanation:
In local mode, the IAP cluster at the branch office has a local subnet and the master IAP of the cluster acts as the DHCP server and gateway for clients. The local mode provides access to the corporate network using the inner IP of the IPsec tunnel. The local mode is recommended for this scenario because it allows the branch office to remain functional even if the link to the main office fails, as the clients can still obtain IP addresses and access local resources. The local mode also avoids the need for additional routing or switching configuration on the MC or the branch office network12.
References:
1: Understanding IAP-VPN Architecture - Aruba
2: IAP-VPN Forwarding Modes - Aruba

NO.6 A plan includes these security settings for the employee WLAN:
WPA2-Enterprise with AES encryption

802.1X with PEAP-MSCHAPv2
However, the customer wants to use certificates to authenticate user devices. Which change brings the plan in alignment with the customer requirements?
A. Use EAP-TLS instead of PEAP-MSCHAPv2
B. The TKIP encryption instead of AES.
C. Add WPA2-PSK as an alternative to WPA2-Enterprise.
D. Add Tunneled TLS (TTLS) as an alternative to PEAP-MSCHAPv2.
Answer: A
Explanation:
The customer wants to use certificates to authenticate user devices, which means that they need a strong and secure method of verifying the identity of the devices that connect to the employee WLAN. The best option for this is to use EAP-TLS instead of PEAP-MSCHAPv2. EAP-TLS stands for Extensible Authentication Protocol-Transport Layer Security, and it is a protocol that uses certificates on both the client and the server side to establish a mutual authentication and a secure channel for data exchange. EAP-TLS is considered the most secure EAP method, as it prevents common attacks such as dictionary attacks, man-in-the-middle attacks, and replay attacks.
The other options are not suitable for the customer requirements:
Option B is incorrect because TKIP encryption is weaker than AES encryption. TKIP stands for Temporal Key Integrity Protocol, and it is an older encryption method that was designed to replace WEP, which had serious security flaws. However, TKIP also has some vulnerabilities, and it is not recommended for modern WLANs. AES stands for Advanced Encryption Standard, and it is a newer and stronger encryption method that provides better security and performance for WLANs.
Option C is incorrect because WPA2-PSK is less secure than WPA2-Enterprise. WPA2-PSK stands for Wi-Fi Protected Access 2-Pre-Shared Key, and it is a security mode that uses a common passphrase or key to authenticate all devices that connect to the WLAN. However, this passphrase or key can be easily compromised or shared, and it does not provide individual authentication or encryption for each device.
WPA2-Enterprise stands for Wi-Fi Protected Access 2-Enterprise, and it is a security mode that uses a RADIUS server to authenticate each device individually and dynamically generate encryption keys for each session. WPA2-Enterprise provides better security and scalability for WLANs.
Option D is incorrect because TTLS does not use certificates to authenticate user devices. TTLS stands for Tunneled Transport Layer Security, and it is a protocol that uses certificates only on the server side to establish a secure tunnel for data exchange. The client side can use different methods to authenticate, such as passwords, tokens, or certificates. However, TTLS does not require certificates on the client side, and it is less secure than EAP-TLS.
References:
ArubaOS 8.5 User Guide)
ArubaOS 8.5 Security Guide)
Aruba Certified Design Professional Official Certification Study Guide (HPE6-A47))

NO.7 An architect plans 128 APs to support 12,800 devices in a very high density (VHD) design. The customer requires high availability, so the architect plans to recommend a pair of controllers. What is one reason to recommend 7210 controllers rather than 7205 controllers for this deployment?
A. the need for high speed 10 GbE ports
B. the need for clustering

C. the number of devise required
D. the number of APs required
Answer: D
Explanation:
The Aruba 7210 Mobility Controller is designed to support up to 512 APs and 16,384 simultaneous users. In contrast, the 7205 Mobility Controller supports up to 256 APs and 8,192 simultaneous users. Therefore, for a very high density (VHD) design with 128 APs supporting 12,800 devices, the 7210 controllers would be a better fit due to their higher capacity for APs and simultaneous users.
References:
Designing Aruba Solutions, Rev. 20.11, Module 4: Aruba Mobility Controller Design, page 4-16
7200 Series Controller Data Sheet, page 1