DUMPSBOSS.

Aruba Certified Campus Access Associate Exam

HP HPE6-A85

Version Demo

Total Demo Questions: 12

Total Premium Questions: 122

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Networking Fundamentals	32
Topic 2, Aruba Products and Solutions	12
Topic 3, Wired Network Configuration	25
Topic 4, Wireless Network Configuration	18
Topic 5, Network Security	20
Topic 6, Troubleshooting	15
Total	122

QUESTION NO: 1

Which commands are used to set a default route to 10.4.5.1 on an Aruba CX switch when In-band management using an SVI is being used?

A. iP default-gateway 10.4.5.1

B. ip route 0 0 0.070 10.4 5.1 vrf mgmt

C. ip route 0.0.0.0/0 10.4.5.1

D. default-gateway 10.4.5.1

ANSWER: C

Explanation:

`ip route 0.0.0.0/0 10.4.5.1` is the correct ArubaOS-CX global-configuration command for installing an IPv4 default static route when management connectivity is in-band through an SVI. The `0.0.0.0/0` prefix represents the IPv4 default route, which matches destinations for which the switch has no more-specific route in its routing table. The next-hop value, `10.4.5.1`, identifies the Layer 3 neighbor to which traffic for those otherwise unknown destinations is sent. Because the switch is managed through an SVI, this route belongs in the routing context used by that in-band interface, normally the default VRF unless the SVI has explicitly been assigned to another VRF. This provides the switch with return-path reachability to remote management stations and services beyond its directly connected VLANs. ArubaOS-CX documents default-route configuration using the `ip route` command and the default destination prefix of `0.0.0.0/0`. See the ArubaOS-CX Default route documentation and its VRF overview.

QUESTION NO: 2

What describes Clearpass OnGuard? (Select two.)

A. OnGuard assigns a unique identity to each device.

B. It is used for the self-registration of guest devices.

C. OnGuard is an agent running on client systems.

D. OnGuard performs posture checks on client systems.

E. It is an intuitive portal for users to securely configure their devices.

ANSWER: C D

Explanation:

ClearPass OnGuard is an endpoint health-validation capability within Aruba ClearPass Policy Manager. “OnGuard is an agent, running on client systems” is correct because OnGuard uses an installed persistent agent or a temporary web-based agent to collect endpoint posture information. This endpoint-side component evaluates the device locally and sends relevant health information to ClearPass for use in access-control decisions.

“OnGuard is doing posture checks on client systems” is also correct because its central purpose is to assess whether a device satisfies an organization’s defined security requirements before or while it receives network access. Typical posture data can include operating-system status, antivirus and antispyware state, firewall status, patch level, disk encryption, and the presence or absence of specified applications or processes. ClearPass can use the resulting posture state in policy evaluation, such as allowing compliant endpoints normal access or placing endpoints that need remediation into a restricted role or network segment. This supports continuous enforcement of endpoint-security requirements across wired and wireless access environments. Aruba’s ClearPass documentation describes OnGuard as the framework for endpoint posture assessment and remediation: ClearPass OnGuard Overview. Additional product context is available at Aruba ClearPass.

QUESTION NO: 3

What are two characteristics of Wi-Fi 6 OFDMA and Target Wake Time (TWT)? (Select two.)

A. OFDMA divides a channel into resource units for simultaneous client transmissions.

B. TWT can schedule when a client wakes to send or receive traffic.

C. OFDMA requires every client to use an 80 MHz channel.

D. TWT permanently disables client roaming between access points.

E. Wi-Fi 6 features require WPA3-Personal security.

ANSWER: A B

Explanation:

OFDMA divides a channel into resource units for simultaneous client transmissions and **TWT can schedule when a client wakes to send or receive traffic** are correct. OFDMA improves efficiency when many clients have relatively small amounts of data to transmit by allowing the AP to allocate portions of a channel to multiple clients. TWT allows compatible clients and the AP to agree on scheduled wake periods, which can reduce unnecessary radio activity and conserve battery power.

Neither feature eliminates the need for RF planning or guarantees that all legacy clients receive Wi-Fi 6 capabilities. WPA3 is a security certification and is not a requirement for OFDMA operation.

QUESTION NO: 4

A wireless client reports an RSSI of -67 dBm and the AP reports a noise floor of -90 dBm on the client radio.

What is the client signal-to-noise ratio?

A. 13 dB

B. 23 dB

C. 67 dB

D. 90 dB

ANSWER: B

Explanation:

23 dB is correct. Signal-to-noise ratio is calculated by subtracting the noise-floor value from the received signal value: -67 dBm - (-90 dBm) = 23 dB. The negative dBm values represent received power levels, while the resulting SNR is expressed as a positive dB difference.

An RSSI of -67 dBm alone does not determine client quality. The noise floor must also be considered because a higher noise level reduces the usable difference between the wanted signal and background RF energy.

QUESTION NO: 5

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

ANSWER: C

Explanation:

Signal to Noise Ratio (SNR) decreases because absorption attenuates the Wi-Fi signal as radio-frequency energy passes through materials such as walls, furniture, glass, or building structures. The received signal level at the client is therefore lower than it would be in an unobstructed path. SNR represents the difference between the received desired signal and the ambient noise floor, expressed in dB. When attenuation lowers the desired signal while the noise floor remains substantially unchanged, that difference becomes smaller, producing a lower SNR.

A lower SNR reduces the reliability and usable capacity of a wireless connection. Clients may need to use more robust, lower-rate modulation and coding schemes, retransmissions can increase, and roaming or application performance may be affected if coverage becomes insufficient. Aruba wireless design practice therefore includes accounting for expected attenuation from building materials during predictive planning and validating both coverage and signal quality during an onsite survey. AP placement and transmit-power design should provide adequate SNR at the intended client locations, rather than relying only on a detectable signal level. Aruba's campus WLAN design guidance discusses RF design and validation considerations at Aruba Validated Solution Guide: WLAN Design. Aruba Central monitoring documentation is available at Aruba Central AP Monitoring.

QUESTION NO: 6

You are in a meeting with a customer where you are asked to explain how the network redundancy feature VRRP works. What is the correct statement for this feature?

A. VRRP uses BPDUs for messaging

B. VRRP uses multicast for messaging

C. VRRP uses unicast for messaging

D. VRRP uses broadcast for messaging

ANSWER: B

Explanation:

VRRP uses multicast for messaging. Virtual Router Redundancy Protocol provides default-gateway resilience by allowing multiple routers to represent one virtual router, identified by a shared virtual IP address and virtual MAC address. One participating router is elected the Master and is responsible for forwarding traffic sent to the virtual gateway. The Master periodically sends VRRP Advertisements so the Backup routers can monitor its availability. If those advertisements stop arriving within the applicable timeout, an eligible Backup router takes over the Master role, maintaining gateway availability for connected hosts without requiring hosts to change their configured default gateway. For IPv4 VRRP, these protocol advertisements are sent to the link-local multicast address 224.0.0.18, using IP protocol number 112. The multicast scope keeps the redundancy control traffic on the local network segment where the VRRP peers participate. This multicast advertisement mechanism is defined by the VRRP standard and is fundamental to the master-election and failover behavior described in Aruba networking implementations. See RFC 5798: Virtual Router Redundancy Protocol and Aruba's AOS-CX VRRP overview.

QUESTION NO: 7

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.

ANSWER: C E

Explanation:

A UXI sensor behaves like a real client/user because it connects to the wired or wireless network and continuously performs synthetic tests from the endpoint perspective. This gives operations teams visibility into the actual experience a user would encounter rather than only infrastructure-side statistics. The sensor's testing can identify where in the service path an issue is affecting the user experience, including the network, DNS, DHCP, authentication, or an upstream application/service dependency.

A UXI can check different applications, such as HTTP, VOIP, or Office 365, because UXI runs active application and network tests to validate availability and performance. Its application-focused monitoring helps establish whether critical services are reachable and whether quality metrics affecting interactive use are within acceptable bounds. Aruba describes UXI as an always-on user-experience monitoring solution that uses purpose-built sensors to provide end-to-end visibility across Wi-Fi, wired, and application environments. This client-like, application-aware approach allows IT staff to detect and troubleshoot experience degradation proactively, including at remote or unattended sites. See Aruba's User Experience Insight product page and UXI data sheet.

QUESTION NO: 8

A company uses ClearPass to apply different access privileges to employees, contractors, and unmanaged devices after authentication.

Which two ClearPass policy components are required to make an authorization decision and return the appropriate access enforcement? (Select two.)

A. A role-mapping policy

B. An enforcement policy

C. An authentication source only

D. An audit record

E. A guest self-registration portal

ANSWER: A B

Explanation:

A role-mapping policy and **an enforcement policy** are correct. ClearPass uses role mapping to evaluate authentication and endpoint attributes and assign roles, such as employee, contractor, or noncompliant device. The enforcement policy then evaluates those roles and returns the appropriate enforcement profile, such as a VLAN, downloadable role, or access-control result.

An authentication source validates credentials or retrieves identity attributes, but it does not itself decide the final access enforcement. An audit record and a guest portal can support operations or guest workflows, but neither replaces role mapping and enforcement policy processing.

QUESTION NO: 9 - (SIMULATION)

Please match the use case to the appropriate authentication technology

ANSWER: See the explanation for the answer

Explanation:

Correct matching:

Add certificates to Android devices with the Aruba Onboard application for wireless authentication → ClearPass Policy Manager

Authenticate users on corporate-owned Chromebook devices using 802.1X and context gathered from the network devices they log into → Cloud Authentication and Policy
Provide unbound MPSKs managed by Aruba Central to end users and client devices → Cloud Authentication and Policy
Validate that devices exist in an MDM database before authenticating BYOD users against corporate Active Directory with certificates → ClearPass Policy Manager

Reasoning: ClearPass Policy Manager provides the advanced NAC, Onboard certificate provisioning, Active Directory integration, and MDM/device-posture validation capabilities. Cloud Authentication and Policy is Aruba Central's cloud-managed authentication service and supports cloud-managed 802.1X policy workflows and MPSK delivery/management.

QUESTION NO: 10

A wireless client is moving through a large office and must roam efficiently between Aruba APs. The WLAN uses standards-based roaming assistance features.

Which two statements correctly describe 802.11k and 802.11v? (Select two.)

A. 802.11k can provide neighbor information to a client

B. 802.11v can suggest a BSS transition target to a client

C. 802.11k forces a client to reassociate immediately

D. 802.11v replaces 802.1X authentication with a pre-shared key

E. 802.11r provides the AP channel plan for all nearby APs

ANSWER: A B

Explanation:

802.11k can provide neighbor information to a client and **802.11v can suggest a BSS transition target to a client**. Neighbor reports from 802.11k can help a client identify candidate APs without extensive scanning. With 802.11v, the WLAN can send BSS transition management requests that recommend an appropriate AP for the client.

The client still makes the final roaming decision. 802.11r is the standard associated with Fast BSS Transition and can reduce the authentication delay during a roam, but it is not the feature that supplies neighbor reports or transition recommendations.

QUESTION NO: 11 - (SIMULATION)

What is the correct order of the TCP 3-Way Handshake sequence?

ANSWER: See the explanation for the answer

Explanation:

The correct TCP 3-way handshake order is:

In short: `SYN → SYN/ACK → ACK → established`.

QUESTION NO: 12

An Aruba CX access switch has a two-member LACP LAG to the distribution layer. Each member link operates at 10 Gb/s. A server connected to the access switch transfers a single large TCP flow to a server at the distribution layer, but the transfer never exceeds approximately 10 Gb/s.

What is the most likely explanation?

A. The server must use a static route toward the distribution switch.

B. LACP load balancing keeps a single flow on one physical member link.

C. The LAG must use passive mode on both switches.

D. The switch must disable spanning tree on the LAG.

ANSWER: B

Explanation:

LACP load balancing keeps a single flow on one physical member link is correct. A LAG provides aggregate bandwidth across multiple flows, but the switch uses a hashing algorithm to select one member link for an individual traffic flow. This prevents frames within the same flow from arriving out of order. Therefore, one TCP flow normally uses only one 10-Gb/s member, while multiple flows with different hash values can be distributed across both LAG members.

Adding a second LAG member increases the aggregate capacity available to multiple conversations; it does not combine both links into a 20-Gb/s path for one ordinary TCP session.