PassQueen
a.k.a dumpsqueen.com

Aruba Certified Mobility Professional 6.4

Aruba ACMP_6.4

Version Demo

Total Demo Questions: 19

Total Premium Questions: 193

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Planning and Design	23
Topic 2, Implementation and Configuration	131
Topic 3, Troubleshooting	21
Topic 4, Analysis and Optimization	18
Total	193

QUESTION NO: 1

Which components are part of an 802.1X authentication exchange? (Choose three)

A. Supplicant

B. Authenticator

C. Authentication server

D. DHCP server

E. Default gateway

ANSWER: A B C

Explanation:

The **supplicant**, **authenticator**, and **authentication server** are the principal components of an 802.1X deployment. The wireless client acts as the supplicant and provides the user or device credentials. The AP/controller acts as the authenticator, controlling access to the network while relaying EAP authentication messages. The RADIUS server acts as the authentication server and validates the credentials.

A DHCP server can provide IP addressing after access is authorized, but it is not an 802.1X authentication component. ArubaOS supports 802.1X authentication through its AAA and RADIUS integration. See the ArubaOS 6.4 AAA documentation.

QUESTION NO: 2

Which are benefits of deploying wireless clients in the 5 GHz band? (Choose three)

A. More non-overlapping channels

B. Less exposure to common non-Wi-Fi interference sources

C. Support for 802.11a/n/ac operation

D. Greater signal penetration through walls than 2.4 GHz

E. Support for all legacy 802.11b clients

ANSWER: A B C

Explanation:

The 5 GHz band provides **more non-overlapping channels** than the 2.4 GHz band, allowing a higher-density AP deployment with more effective channel reuse. It also has **less exposure to common non-Wi-Fi interference sources**, such as Bluetooth devices, microwave ovens, and many consumer devices that operate in 2.4 GHz. In addition, the 5 GHz band supports **802.11a/n/ac operation**, enabling modern clients to use higher-capacity PHY capabilities where supported.

QUESTION NO: 3

A university, has 2 departments. Department 1 has its own mobility domain with one controller. Department 2 has multiple controllers configured in a second domain. The university is planning on offering a new application and needs users to be able to roam between both mobility domains.

What is the best way to accomplish this?

A. The 2 existing domains should be left as they are. A 3rd mobility domain should then be created and all 3 controllers need to be added to it

B. Merge the controllers into the same mobility domain

C. The IP subnets of all controllers need to be configured to match

D. This cannot be accomplished

E. Create a new domain between a department 1 controller and one of the department 2 controllers

ANSWER: B

Explanation:

Merge the controllers into the same mobility domain. In ArubaOS, a mobility domain is the administrative grouping of controllers that coordinate client mobility services. Controllers in the same domain exchange the information needed to maintain a wireless client's session as that client moves between access points managed by different controllers. Bringing the Department 1 controller and all Department 2 controllers into one common mobility domain therefore establishes the required inter-controller roaming relationship for users of the new application. This design also provides a consistent scope for mobility-related configuration and client state sharing, rather than attempting to layer a separate domain over existing independent domains. ArubaOS documentation describes the mobility domain as the set of controllers participating in coordinated mobility services and explains that controllers must be configured as members of the domain to support this behavior. Before making the change, the university should plan the unified domain configuration carefully, including controller reachability, role assignments, and consistency of relevant WLAN and AAA settings, so roaming clients receive the intended service throughout both departments. See Aruba's Mobility Domains overview and the ArubaOS mobility-domain configuration guidance.

QUESTION NO: 4

The Aruba Policy Enforcement Firewall (PEF) module supports source network address translation (src-nat).

Which is a use of this statement in an Aruba configuration?

A. provide a single source IP address for users in a role

B. redirect Captive Portal HTTP sessions

C. redirect Access Points to another Aruba controller

D. provide IP addresses to clients

E. redirects clients to Aruba Firewall

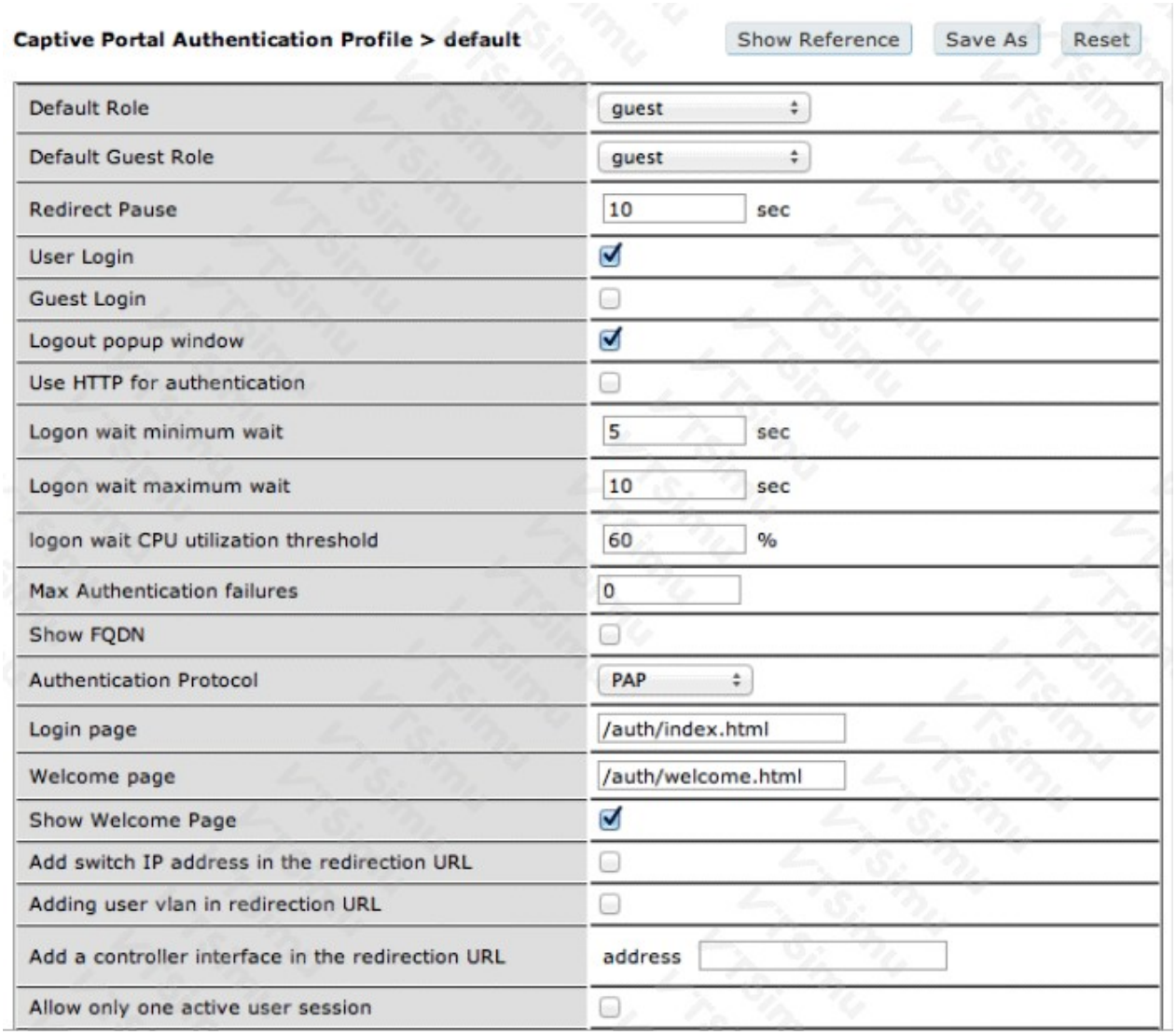
ANSWER: A

Explanation:

The correct use is **provide a single source IP address for users in a role**. In an ArubaOS firewall policy, the `src-nat` action performs source network address translation on traffic that matches the policy rule. The controller replaces the client's original source address with the address specified in the rule before forwarding the traffic. Consequently, multiple clients assigned to the relevant user role can appear to an upstream network, server, or Internet destination as traffic originating from one common source address.

This is useful when a role needs controlled or simplified outbound addressing, such as allowing role-based traffic through an upstream firewall that permits a known source IP address, or hiding individual client addresses from an external destination. Because the action is attached to a firewall policy, the translation can be applied selectively according to the client role and the traffic criteria defined by the policy. Aruba documents source NAT as a Policy Enforcement Firewall action that translates the source address of matching packets; see the ArubaOS 6.4 Network Address Translation documentation and the ArubaOS 6.4 firewall policy documentation.

QUESTION NO: 5



A user logged in with the Captive Portal settings shown in the above screen capture.

What does the user need to do to logout?

A. wait 30 minutes then logout

B. wait 60 minutes then logout

C. click Logout on the browser screen

D. he cannot logout

E. wait 10 seconds for redirect

ANSWER: C

Explanation:

click Logout on the browser screen is correct. The Captive Portal configuration shown provides a browser-based logout mechanism, so the authenticated user ends the session by selecting the Logout control presented in the captive-portal browser page or logout pop-up. This action sends a logout request to the Aruba controller, which removes the client's authenticated session and associated role/state. The user does not need to wait for an authentication timeout, an idle timeout, or a redirect timer before initiating this action. Captive Portal is designed to support explicit user session termination when the logout page or logout pop-up functionality is enabled; it is separate from timers that may eventually expire a session automatically. Aruba's ArubaOS Captive Portal documentation describes captive-portal authentication and the associated login/logout behavior, including configuration of logout pages and pop-up windows. See the ArubaOS 6.4 Captive Portal overview and the ArubaOS 6.4 Captive Portal configuration documentation.

QUESTION NO: 6

How does the ARM Band Steering feature encourage 5GHz capable clients to move/connect to the 5GHz radios of Aruba APs?

A. ARM suppresses the probe responses on the 2.4 ghz radio?

B. ARM utilizes third party software on the wireless clients

C. Current Wi-Fi chipset firmware supports this by default

D. It's not possible the move clients to 5GHz radios when they can see both 2.4 and 5GHz APs

E. ARM disables the 2.4Ghz radio for the specified client

ANSWER: A

Explanation:

“ARM suppresses the probe responses on the 2.4 ghz radio?” is correct. Aruba Adaptive Radio Management (ARM) band steering is designed to influence dual-band, 5 GHz-capable clients to associate on the less-congested 5 GHz band. When a client sends probe requests, the AP can selectively withhold 2.4 GHz probe responses for an interval while continuing to respond on 5 GHz. This makes the 5 GHz BSSID more attractive during the client’s network-selection process, encouraging the client to discover and join the 5 GHz radio instead of immediately associating at 2.4 GHz.

This behavior is an association-time steering technique: it works with normal Wi-Fi client discovery and does not require a special client-side application. It is intended to improve RF efficiency by moving capable clients away from the typically more congested 2.4 GHz spectrum, leaving that band available for clients that genuinely need it. The client still makes the final association decision, and ARM’s steering behavior is therefore an encouragement mechanism rather than a forced migration. Aruba documents band steering as an ARM capability for directing dual-band clients toward 5 GHz operation; see the ArubaOS 6.4 ARM documentation and Aruba’s ARM overview.

QUESTION NO: 7

Refer to the following configuration segment for this item.

ip access-list session anewone

user network 172.16.1.0 255.255.255.0 any permit

user host 172.16.1.1 any deny

user any any permit

An administrator wants users to have access to all destinations except 172.16.1.1. Based on the above Aruba Mobility Controller configuration segment, which statements best describe this policy? (Choose two)

A. The rule user host 172.16.1.1 any deny is redundant because of the implicit deny all at the end.

B. The rule user network 172.16.1.0 255.255.255.0 any permit is redundant.

C. The two rules user network 172.16.1.0 255.255.255.0 any permit and user host 172.16.1.1 any deny need to be re-sequenced.

D. The last statement user any any permit is not required

E. The last statement should be any any any deny

ANSWER: B C

Explanation:

Session ACL entries on an Aruba Mobility Controller are evaluated in their configured order, with the first matching entry determining the action. The rule *user network 172.16.1.0 255.255.255.0 any permit* permits traffic to every host in that subnet, including 172.16.1.1. Because it appears before the host-specific deny, traffic for 172.16.1.1 matches the broader network permit first. To preserve both entries while implementing the intended exception, the host-specific deny must precede the subnet-wide permit.

The subnet-wide permit is also redundant in this particular ACL because *user any any permit* subsequently permits user traffic to every destination. After a host-specific deny for 172.16.1.1 is placed before that general permit, all other destinations—including the remainder of 172.16.1.0/24—are already permitted by the final rule. Aruba's firewall policy documentation describes session-policy rules as ordered rules and explains that policy evaluation uses the first applicable match. See the ArubaOS firewall policy documentation and the ArubaOS session ACL documentation.

QUESTION NO: 8

What are the types of user derivation rules that can be applied to a user?(Choose two)

A. SSID

B. MAC

C. VLAN

D. Role

E. AP

ANSWER: C D

Explanation:

VLAN and **Role** are the applicable user-derivation rule types in ArubaOS. A VLAN-based derivation rule uses the VLAN associated with a client session as the condition for assigning the appropriate user role. This is useful where network segmentation itself identifies the class of access required, such as assigning different policies to users placed into employee, guest, or device VLANs.

A role-based derivation rule uses a user's current role as the condition for deriving another role. This supports policy refinement and role transitions, allowing ArubaOS to apply the role that contains the firewall rules, bandwidth controls, captive-portal settings, and access permissions appropriate for the session. In both cases, the result of derivation is a user role, which is ArubaOS's central mechanism for enforcing per-user access policy after authentication and during session handling.

Aruba's ArubaOS 6.4 documentation describes role assignment and derivation as part of the AAA and user-role framework; see the ArubaOS 6.4 Role Derivation documentation and the ArubaOS 6.4 Authentication documentation.

QUESTION NO: 9

Fast Failover has been implemented between Local 1 and Local 2 separated by Routers. During testing Local1 was disabled and all Campus APs backed up to Local 2 flawlessly. But the RAPs did not, they all failed.

What could be the cause?

A. RAPs should be configured in their own AP-groups

B. A VPN IP Pool must be configured on Local 2

C. The RAP whitelist must be ported over to Local 2

D. IPSec must be enabled on Local 2

E. RAPs are not supported by Fast Failover

ANSWER: E

Explanation:

RAPs are not supported by Fast Failover is correct. In ArubaOS 6.4, Fast Failover is a campus AP high-availability mechanism. It enables a campus AP to maintain its primary controller relationship while preparing a backup controller path, which substantially reduces the interruption when the primary local controller becomes unavailable. This behavior accounts for the successful, rapid recovery of the campus APs when Local 1 was disabled.

A Remote Access Point operates differently because its controller relationship is established across an IPsec tunnel from an untrusted or remote network. The RAP's tunnel establishment, authentication, and controller-recovery behavior do not participate in the campus AP Fast Failover mechanism. Consequently, a design can show successful Fast Failover for campus APs while RAPs do not fail over through that feature. Remote AP resiliency must therefore be designed and validated using the RAP-supported controller redundancy and tunnel-reconnection behavior applicable to the ArubaOS release.

Aruba's ArubaOS 6.4 documentation describes controller redundancy and AP high-availability behavior in the ArubaOS 6.4 Web Help. Aruba's documentation library is also available through the Aruba Technical Documentation portal.

QUESTION NO: 10

Which match condition can be used by a server derivation rule?(Choose two)

A. greater than

B. less than

C. inverse of

D. contains

E. equals

ANSWER: D E

Explanation:

contains and **equals** are valid match conditions for an ArubaOS server derivation rule. Server derivation rules inspect an attribute returned by an authentication server, such as a RADIUS attribute, and use the configured condition to determine whether the rule matches. A successful match can derive a user role, VLAN, or other value used by the controller's authorization process.

The **equals** condition is appropriate when the returned attribute must exactly match a specified value. For example, an administrator can match a particular group or role value returned by RADIUS and derive the corresponding Aruba user role. The **contains** condition is useful when the desired value may be embedded within a longer returned attribute string, allowing the controller to identify a relevant substring and apply the configured derivation action.

These conditions support common identity-store and RADIUS integration designs, where authorization decisions depend on values sent in authentication responses. Aruba documents server derivation rules as part of its authentication and user-role assignment workflow; see the ArubaOS 6.4 Server Derivation Rules documentation and the ArubaOS 6.4 Authentication documentation.

QUESTION NO: 11

An administrator wants to assign a VLAN to a user based upon the authentication process using Vendor Specific Attributes (VSA). Where are Aruba Vendor Specific Attribute (VSA) values provisioned?

A. controller

B. client

C. RADIUS server

D. Internal user database

E. Option 60 of DHCP reply

ANSWER: C

Explanation:

RADIUS server is correct because Aruba Vendor-Specific Attributes are RADIUS attributes that the authentication server includes in its Access-Accept response after validating a user. The administrator provisions the applicable Aruba VSA values in the user's account, group, role, or authorization policy on the RADIUS service. When the Aruba controller receives the Access-Accept, it reads the returned attributes and applies the associated authorization outcome, such as assigning the user to a particular VLAN.

This design separates authentication and authorization policy from the network-access device. The controller acts as the RADIUS client and enforcement point: it sends the authentication request, receives the reply, and enforces the VLAN or role information delivered in that reply. The RADIUS server is therefore the location where the attribute-value policy is defined and maintained. Aruba documents the use of RADIUS attributes, including Aruba-specific attributes, as part of AAA and user authorization processing. See the ArubaOS AAA documentation and the RADIUS protocol specification (RFC 2865).

QUESTION NO: 12

An administrator is setting up a factory default controller. No new AP groups were created. When adding a WLAN SSID in the Campus WLAN wizard what AP group is available?

A. The air-monitors AP group

B. The logon AP group

C. The default AP group

D. The initial AP group

E. The Spectrum AP group

ANSWER: C

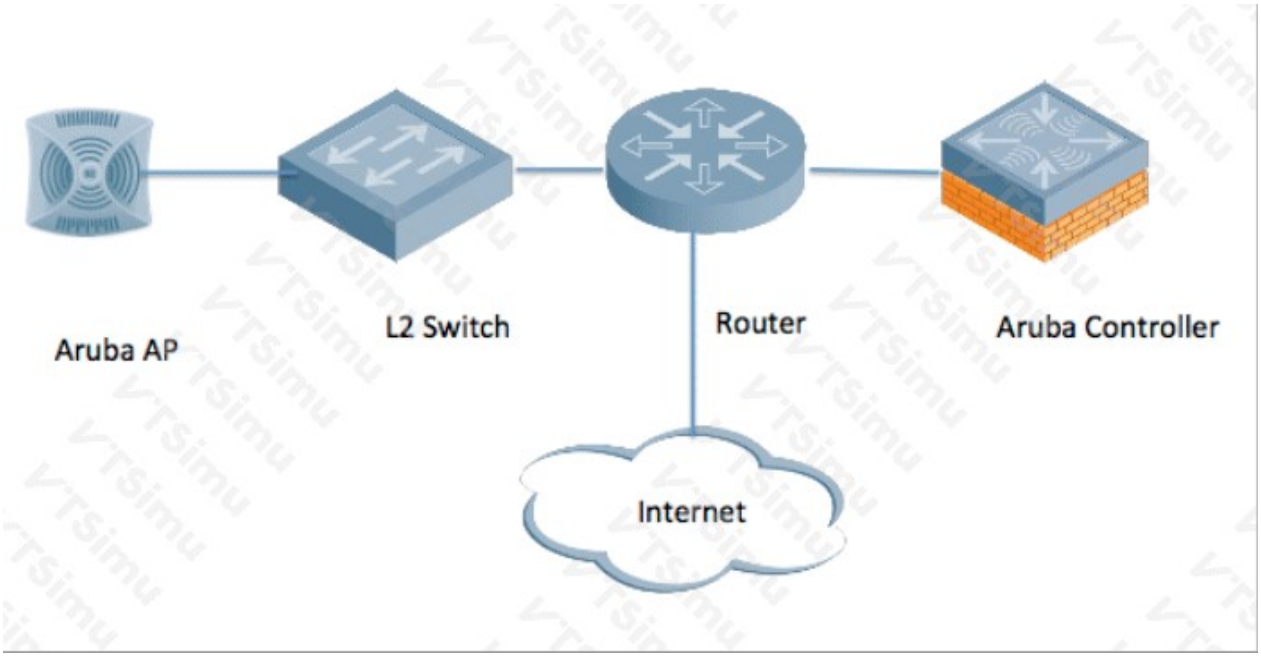
Explanation:

The default AP group is correct because ArubaOS provides a built-in AP group named *default* on a controller's initial configuration. AP groups are used to apply configuration profiles, including virtual AP/WLAN settings, to access points assigned to that group. On a factory-default controller where the administrator has not created any additional AP groups, the built-in default group is therefore the available group to which the Campus WLAN wizard can apply the new SSID configuration.

This behavior makes initial WLAN deployment straightforward: APs that have not been explicitly assigned to a custom AP group use the default AP-group configuration. The wizard can associate the WLAN's virtual AP profile with that existing group, allowing the SSID to be advertised by APs using the default group. Once custom AP groups are created, an administrator can use them to scope different SSIDs, radio settings, and policies to selected AP populations, but their absence does not remove the controller's built-in default group.

Aruba's ArubaOS documentation describes AP groups as the mechanism for organizing AP-specific configuration and notes the default AP group used for APs without another group assignment. See the ArubaOS 6.4 AP group configuration documentation and the ArubaOS 6.4 virtual AP documentation.

QUESTION NO: 13



Referring to the diagram provided for this question, in which locations must you define the new data VLANs for wireless client traffic? (Choose two)

A. in all L2 switches where an Aruba AP is physically connected

B. in all APs and the L2 switches to which they are connected

C. in the Aruba controller and the router it's connected to in an L2 deployment

D. in the routers and switches where the APs are physically connected

E. only on the Aruba controller in an L3 deployment

ANSWER: C E

Explanation:

In an L2 deployment, the Aruba controller terminates the wireless user traffic and places it into the configured user VLAN. The router directly connected to the controller must also have the corresponding VLAN defined so that it can provide the Layer 3 gateway and route traffic for that client subnet. Therefore, the VLAN must be configured in both the Aruba controller and the directly connected router for the L2 topology shown.

In an L3 deployment, APs can be separated from the controller by routed infrastructure while maintaining their control and data tunnels to the controller. Wireless client traffic remains tunneled to the controller, where the user role and VLAN assignment are applied. As a result, the new wireless data VLAN is defined on the Aruba controller; it does not need to be extended as a Layer 2 VLAN through the routed AP access network. This separation is a core advantage of Aruba's tunneled WLAN architecture: AP transport networks do not need to carry every client VLAN. Aruba describes controller-based tunneled forwarding and VLAN assignment in its ArubaOS VLAN configuration documentation and VLAN overview.

QUESTION NO: 14

An Aruba Controller is configured with VLAN 1,5, 200, and 4095. All VLANs have IP addresses assigned. Which is the default management VLAN on the Aruba controller?

A. VLAN 5

B. VLAN 1

C. VLAN 200

D. None, it must be defined

E. VLAN 4095

ANSWER: B

Explanation:

VLAN 1 is the default management VLAN on an Aruba controller. In the default ArubaOS configuration, the controller's management IP addressing is associated with VLAN 1 unless an administrator explicitly configures a different VLAN for management connectivity. The presence of IP addresses on other configured VLANs does not automatically designate any of them as the management VLAN; those addresses may support routed user traffic, controller services, or other administrative designs. VLAN 1 therefore remains the expected answer when the question asks for the default management VLAN and provides no statement that the management VLAN has been changed.

This default behavior matters during initial deployment and troubleshooting. Administrators commonly use an interface placed in VLAN 1 to reach the controller for initial web, SSH, or console-assisted configuration, then may move management access to a dedicated management VLAN as part of production network design. Aruba's controller setup guidance identifies VLAN 1 as the default VLAN used for initial controller management configuration. See Aruba's ArubaOS controller setup documentation and the ArubaOS VLAN configuration documentation.

QUESTION NO: 15

Which netdestination aliases are built into the controller? (Choose three)

A. logon

B. any

C. user

D. guest

E. localip

ANSWER: B C E

Explanation:

The controller includes the built-in netdestination aliases **any**, **user**, and **localip**. These predefined aliases can be used directly in ArubaOS firewall policy rules, avoiding the need to define equivalent address objects manually. The **any** alias represents all IP destinations, making it appropriate when a rule is intended to apply regardless of the destination address. The **user** alias represents the IP address space assigned to wireless users; it is useful in policies that need to identify traffic directed toward client devices. The **localip** alias identifies addresses local to the controller itself, which is important when creating rules for traffic destined to controller services or management interfaces. ArubaOS treats these as system-provided netdestination aliases, so they are available for policy construction without additional configuration. The ArubaOS policy documentation describes netdestinations and their use as address-based policy objects, including the predefined aliases supplied by the controller. See the ArubaOS 6.4 Network Destinations documentation and the ArubaOS 6.4 Access Control documentation.

QUESTION NO: 16

The permanent licenses on the controller will be deleted with the use of which command?

A. delete license

B. write erase

C. Licenses cannot be deleted once activated

D. write erase all

E. reboot delete all

ANSWER: D

Explanation:

`write erase all` is the correct command because it performs the full erase operation on an ArubaOS controller, including the permanent license information stored on the device. This is more extensive than clearing only the running or startup configuration: it returns the controller to a substantially unprovisioned state and removes licensing data along with the configuration data that must be cleared during a complete reset or decommissioning procedure. In ArubaOS 6.4 operational practice, administrators should use this command only when they intentionally need to wipe the controller, such as before repurposing hardware, because the resulting state requires the controller to be configured and licensed again as appropriate. Aruba's ArubaOS documentation describes licensing as controller-resident information and documents controller reset and erase operations as administrative maintenance tasks. Review the ArubaOS licensing documentation before performing the operation and ensure that any required license keys or entitlement records are available for later restoration. See the ArubaOS 6.4 licensing documentation and the ArubaOS 6.4 configuration-management documentation.

QUESTION NO: 17

An administrator configures a DHCP helper address on a controller VLAN interface.

What is the purpose of this configuration?

A. Relay DHCP requests to a remote DHCP server

B. Assign static IP addresses to APs

C. Translate user source addresses with NAT

D. Redirect users to captive portal

E. Synchronize controller time with an NTP server

ANSWER: A

Explanation:

A DHCP helper address enables the controller to **relay DHCP requests to a DHCP server on another IP network**. DHCP client requests are initially broadcasts and normally cannot cross a Layer-3 boundary. The controller receives the request on the client VLAN and forwards it as a unicast DHCP relay message to the configured DHCP server.

This configuration is commonly used when the DHCP server is centralized rather than located in every client VLAN. The DHCP server uses the relay information to select an address scope appropriate for the requesting VLAN. ArubaOS VLAN and DHCP-relay configuration are described in the ArubaOS 6.4 VLAN documentation.

QUESTION NO: 18

Which AP operating modes can be assigned through an AP system profile? (Choose three)

A. AP mode

B. AM mode

C. Spectrum mode

D. Captive portal mode

E. Firewall mode

ANSWER: A B C

Explanation:

AP mode, **AM mode**, and **Spectrum mode** are valid ArubaOS AP operating modes. AP mode allows the device to provide normal client access. AM mode configures the AP as an air monitor for RF monitoring and wireless intrusion detection functions rather than client access. Spectrum mode configures the AP to perform spectrum-analysis functions.

An AP operating mode is distinct from settings such as forwarding mode or a user role, which are configured in virtual AP, AAA, and policy profiles. ArubaOS documentation describes AP system-profile settings and AP operating modes in the ArubaOS 6.4 User Guide.

QUESTION NO: 19

Which settings can be configured as part of an ArubaOS user role? (Choose three)

A. Session ACL

B. Bandwidth contract

C. VLAN assignment

D. AP radio channel

E. Controller software image

ANSWER: A B C

Explanation:

A user role is the ArubaOS policy construct applied to an active client session. A role can include a **session ACL** to control permitted and denied traffic, a **bandwidth contract** to regulate traffic rates, and a **VLAN assignment** to place users into an appropriate network segment. The controller applies these role settings after authentication and role derivation determine the effective role for the user.