DUMPSARENA

Aruba Certified Mobility Associate Exam

HP HPE6-A70

Version Demo

Total Demo Questions: 18

Total Premium Questions: 181

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, WLAN Fundamentals	19
Topic 2, WLAN Design	14
Topic 3, WLAN Security	59
Topic 4, WLAN Configuration	56
Topic 5, WLAN Monitoring and Troubleshooting	33
Total	181

QUESTION NO: 1

Refer to the exhibits.

Exhibit 1

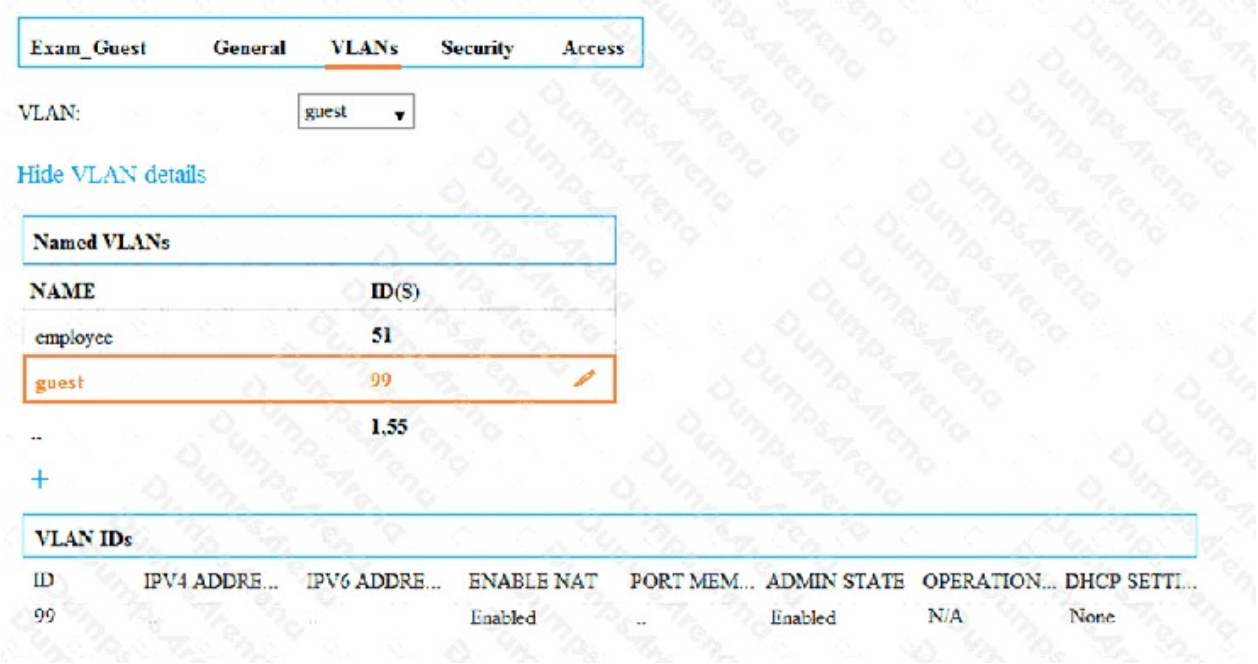
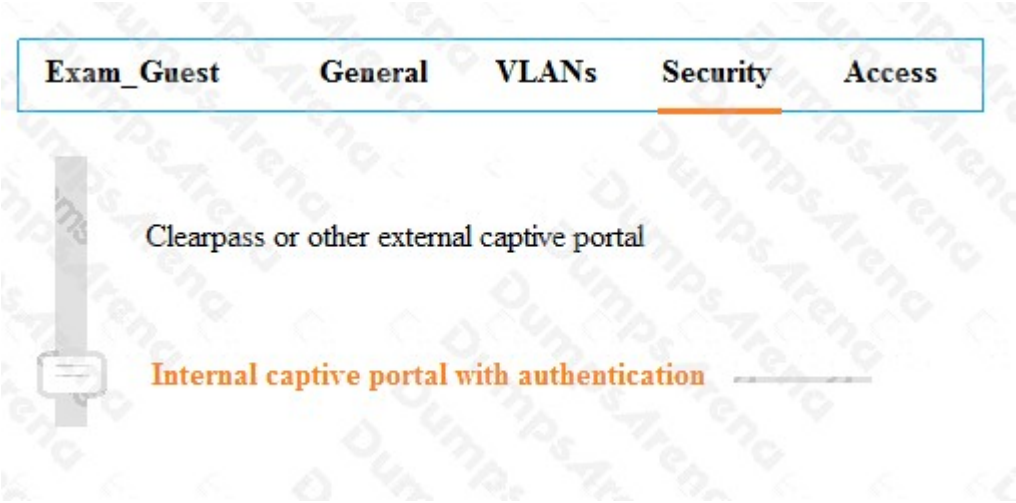


Exhibit 2



A network administrator configures a guest WLAN on an Aruba Mobility Master (MM)-based solution. The exhibits show some of the settings for this WLAN.

Which settings must the administrator configure on each Mobility Controller (MC) at the device level for this configuration to function properly?

A. an IPsec preshared key

B. CPSec certificates

C. a portal page

D. VLAN 99 IP settings

ANSWER: D

Explanation:

VLAN 99 IP settings must be configured locally on every Mobility Controller that can terminate clients for this guest WLAN. The WLAN configuration can be centrally defined and inherited from the Mobility Master hierarchy, including the virtual AP, SSID, AAA settings, and VLAN assignment. However, each controller that forwards guest-client traffic needs the local Layer 3 configuration required to provide services for the assigned client VLAN. This includes the VLAN interface addressing appropriate to that controller and deployment, enabling the controller to route, relay, or otherwise handle traffic for clients placed into VLAN 99.

In an ArubaOS 8 managed deployment, configuration is often applied at a group or folder level, while settings that depend on an individual controller's local connectivity and addressing must be configured at the device level. Because a guest user can associate to an AP terminated on any participating controller, the VLAN's IP configuration must exist on each such controller; configuring it only centrally does not supply device-specific interface addressing. Aruba's documentation describes VLAN interfaces as controller network configuration and distinguishes hierarchy-based configuration from local controller requirements. See the ArubaOS 8.4 User Guide and ArubaOS VLAN configuration documentation.

QUESTION NO: 2

A company has an Aruba Mobility Master (MM)-based solution. Where can network administrators look to monitor the health status of all controllers, APs, and clients?

A. the top banner

B. the MM Maintenance pages

C. the Performance dashboard

D. the Potential Issues dashboard

ANSWER: A

Explanation:

the top banner is correct because it provides an at-a-glance, global health view for the Mobility Master-managed deployment. In the ArubaOS WebUI, the top banner presents summarized status indicators and counts for managed controllers, access points, and clients. An administrator can use these indicators to quickly identify whether the managed infrastructure is operating normally or whether an element requires attention, then drill into the associated information as needed. This makes the banner appropriate for monitoring the collective health status of all these device and client categories from the Mobility Master context, rather than examining an individual device's operational details. Aruba documents the Mobility Master WebUI dashboard and its monitoring functions in the ArubaOS User Guide; see the ArubaOS 8.4 WebUI Help and the ArubaOS Dashboard documentation. The top banner therefore serves as the immediate, centralized health-status indicator for controllers, APs, and connected clients in an MM-based solution.

QUESTION NO: 3

A company has a Mobility Master (MM) solution that manages Mobility Controllers (MCs) in several groups. The company has several WebCC licenses and wants to reserve these licenses for MCs in the Sunnyvale group only.

How can a network administrator achieve this goal?

A. Associate the MAC addresses for the Sunnyvale MCs with the licenses when they are generated.

B. Make sure to be at the Managed Network > Sunnyvale level in the MM Interface when the licenses are installed.

C. Install the licenses on the MM, and allocate them to a dedicated local pool for the Sunnyvale group.

D. Install the licenses directly on the MCs in the Sunnyvale group, and activate the licneses locally.

ANSWER: C

Explanation:

Install the licenses on the MM, and allocate them to a dedicated local pool for the Sunnyvale group. ArubaOS licensing in a Mobility Master–managed deployment is centrally administered through the Mobility Master. Licenses installed on the Mobility Master are placed into a global licensing pool by default, from which managed devices can consume entitlements. To reserve a defined number of Web Content Classification (WebCC) licenses for a particular managed-device group, the administrator creates a local license pool at the applicable group level and allocates the required licenses to that pool. The Sunnyvale group's Mobility Controllers can then draw WebCC capacity from their assigned local pool, ensuring that controllers in other groups cannot consume the licenses reserved for Sunnyvale. This hierarchy-based pool allocation supports centralized license administration while allowing license capacity to be controlled according to organizational or site boundaries. The pool must be configured at the Sunnyvale group level, or at an appropriate parent level whose scope includes only the intended controllers. Aruba's licensing documentation describes the Mobility Master license pool model and the use of local pools for assigning entitlements to managed-device groups. See ArubaOS 8.4 Licensing documentation and ArubaOS 8.4 license pool configuration documentation.

QUESTION NO: 4

Refer to the exhibit.



The exhibit shows output from a Mobility Master (MM) dashboard. What is a valid reason for the administrator to click the akamai square under applications?

A. to see the break down for only the roles, destinations, WLANs, and devices that use this

application

B. to download a report about the usage of this application over time

C. to create filter rules in order to control wireless user access to this application

D. to set up bandwidth rule in order to control wireless user access to this application

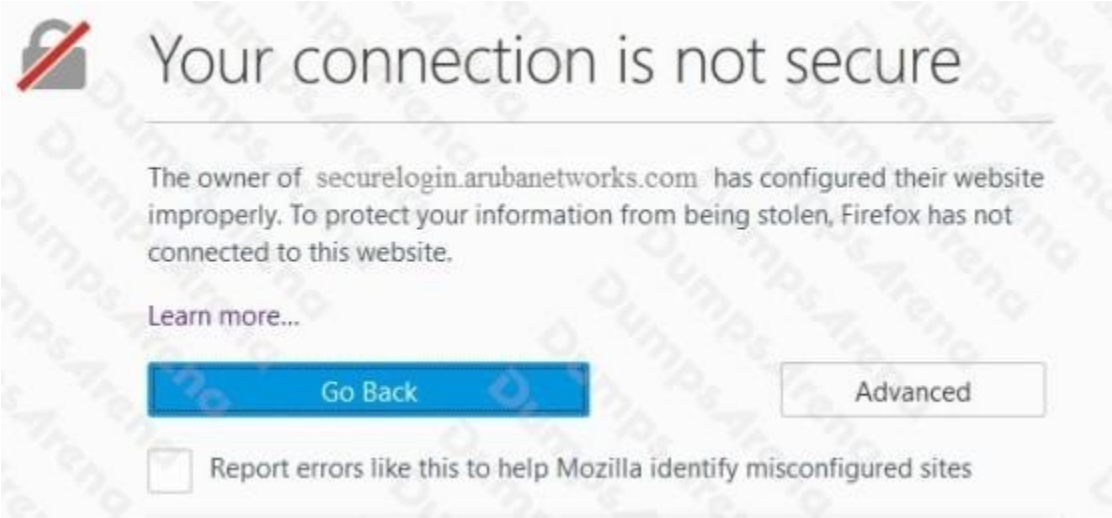
ANSWER: A

Explanation:

Clicking the *akamai* application square is valid because the Mobility Master Dashboard supports application-level drill-down. The Applications widget summarizes application traffic detected by AppRF, and selecting an application opens more focused monitoring information for that application. This lets an administrator identify the roles associated with the traffic, the destinations contacted, the WLANs on which it is seen, and the devices generating or using it. That context is useful for investigating where an application is being consumed and which parts of the wireless environment are involved, without manually constructing separate monitoring queries. ArubaOS dashboard monitoring is designed to move from a summarized widget view to detailed, filtered information about the selected traffic category or application. AppRF provides the application-awareness and classification data that makes this drill-down possible. Aruba documents Dashboard monitoring and its contextual views in the ArubaOS 8.4 Dashboard documentation; application classification and visibility are described in the ArubaOS AppRF documentation.

QUESTION NO: 5

Refer to the exhibit.



A company has a Mobility Master (MM)-based solution with a guest WLAN. During the captive portal redirection, users who access a non-HTTPS Website see the error shown in the exhibit.

How can a network administrator prevent this error?

A. Enable automatic CPSec certificate deployment.

B. Replace the default Mobility Master certificate with a certificate that has the correct hostname.

C. Replace the default server certificate for mobility controllers with a certificate signed by a trusted CA.

D. Reconfigure the guest WLAN to use EAP methods that rely on passwords rather than certificates.

ANSWER: C

Explanation:

Replace the default server certificate for mobility controllers with a certificate signed by a trusted CA. Captive portal operation commonly intercepts an unauthenticated client's HTTP request and redirects the client to an HTTPS login page hosted by the mobility controller. The browser validates the certificate presented by that HTTPS portal before it displays the login page. Aruba's default controller certificate is self-signed, so client operating systems and browsers do not inherently trust its issuer. That lack of trust produces the browser security warning shown during the redirect, even though the user originally browsed to a non-HTTPS site.

Installing a server certificate issued by a public certificate authority, or by an enterprise CA that is trusted by every guest client, establishes a valid certificate chain and prevents the trust warning. The certificate should include the portal DNS name used by clients in its subject alternative name and must be installed on every mobility controller that can terminate guest captive-portal sessions. Aruba documents captive portal redirection and certificate management in the ArubaOS 8.4 Captive Portal documentation and the ArubaOS certificate-management overview.

QUESTION NO: 6

A company uses controller-based Aruba APs with tunneled forwarding. A wireless client sends traffic to an internal server.

Where is the client traffic normally forwarded after it reaches the AP?

A. through a tunnel to the Mobility Controller (MC)

B. directly to the RADIUS server

C. directly onto the local wired VLAN at the AP

D. through the Mobility Master (MM)

ANSWER: A

Explanation:

It is forwarded **through a tunnel to the Mobility Controller (MC)**. In tunneled forwarding mode, the AP encapsulates client traffic and sends it through its secure AP-to-controller tunnel. The controller decapsulates the traffic, applies the relevant role and firewall policies, and forwards it toward the destination network.

In contrast, bridge forwarding places client traffic onto the local wired network at the AP. The RADIUS server performs authentication and authorization functions, while the Mobility Master provides centralized management and does not normally forward client traffic. See the ArubaOS 8.4 documentation.

QUESTION NO: 7

Refer to the exhibit.



A network administrator adds a global rule in the area shown in the exhibit. Where does the global rule take effect?

A. It immediately applies only to the guest role, as part of the final policy applied to the role. Administrators cannot apply the rule to other roles.

B. It immediately applies to the guest role and other roles, as part of the first policy applied to the role.

C. It immediately applies to the guest role and other roles, as part of the final policy applied to the role.

D. It immediately applies only to the guest role and other roles, as part of the first policy applied to the role. Administrators can choose to apply the rule to other roles.

ANSWER: B

Explanation:

It immediately applies to the guest role and other roles, as part of the first policy applied to the role. In ArubaOS, a global access-control rule is not limited to the role from which it is created. It is incorporated into the policy processing for every user role, including the guest role, so that the administrator can enforce a common requirement consistently across the controller. The global-rule designation also determines its evaluation position: global rules are processed before the role-specific rules configured for an individual user role. This makes global rules appropriate for controls that must be evaluated uniformly before any role-level policy logic, such as broad security restrictions or common traffic-handling requirements. The rule becomes effective as part of the controller's policy configuration and does not need to be individually copied into each role. Aruba's ArubaOS documentation describes user-role access rules and their policy evaluation behavior in the ArubaOS Firewall Policies documentation. Additional ArubaOS 8.4 configuration guidance is available through the ArubaOS 8.4 Web Help.

QUESTION NO: 8

Which Mobility Master (MM) dashboard should an administrator access to view a list of rogue and interfering APs?

A. Potential issues

B. Security

C. Performance

D. Network

ANSWER: B

Explanation:

The **Security** dashboard is correct because ArubaOS presents wireless threat and intrusion-detection information there, including detected rogue access points and interfering access points. A rogue AP is an access point detected by Aruba radios that is not classified as authorized within the managed environment, while an interfering AP represents an access point or radio source that can affect WLAN operation without necessarily being connected to the organization's wired network. The Security dashboard gives an administrator an operational view of these security-relevant detections and provides access to the associated lists and details needed for investigation, classification, and response. This makes it the appropriate Mobility Master dashboard when the task is to review rogue and interfering AP activity rather than general device status or client-performance metrics. Aruba's dashboard documentation describes the Security dashboard's role in displaying security information and threat-related data, and the ArubaOS user documentation covers rogue-AP detection and management concepts. See the ArubaOS 8.4 Dashboard documentation and the ArubaOS 8.4 Rogue AP Detection documentation.

QUESTION NO: 9

Refer to the exhibits.

Exhibit 1

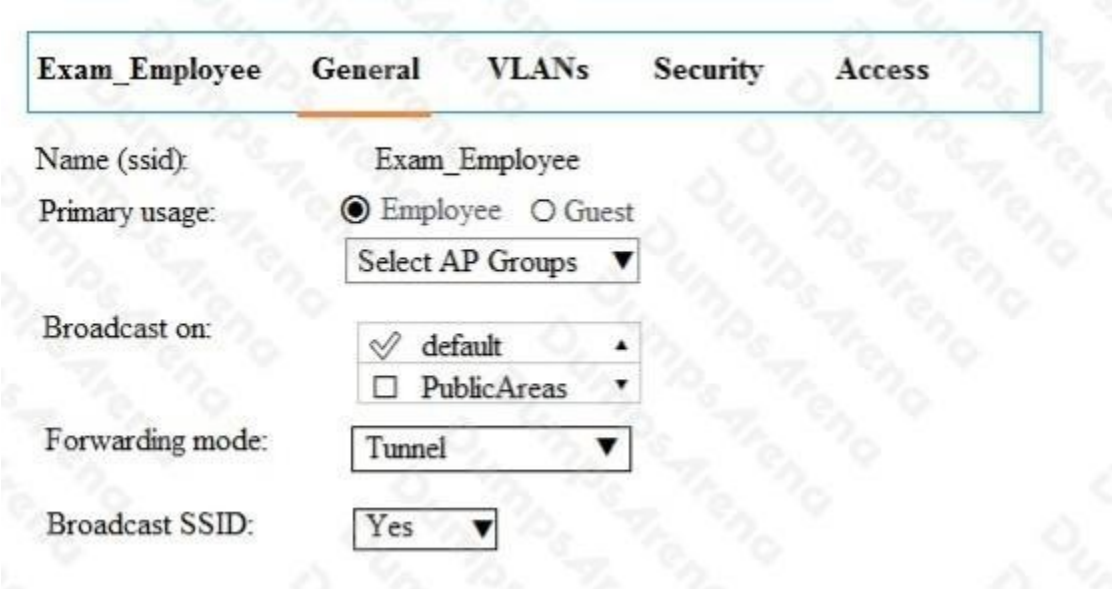
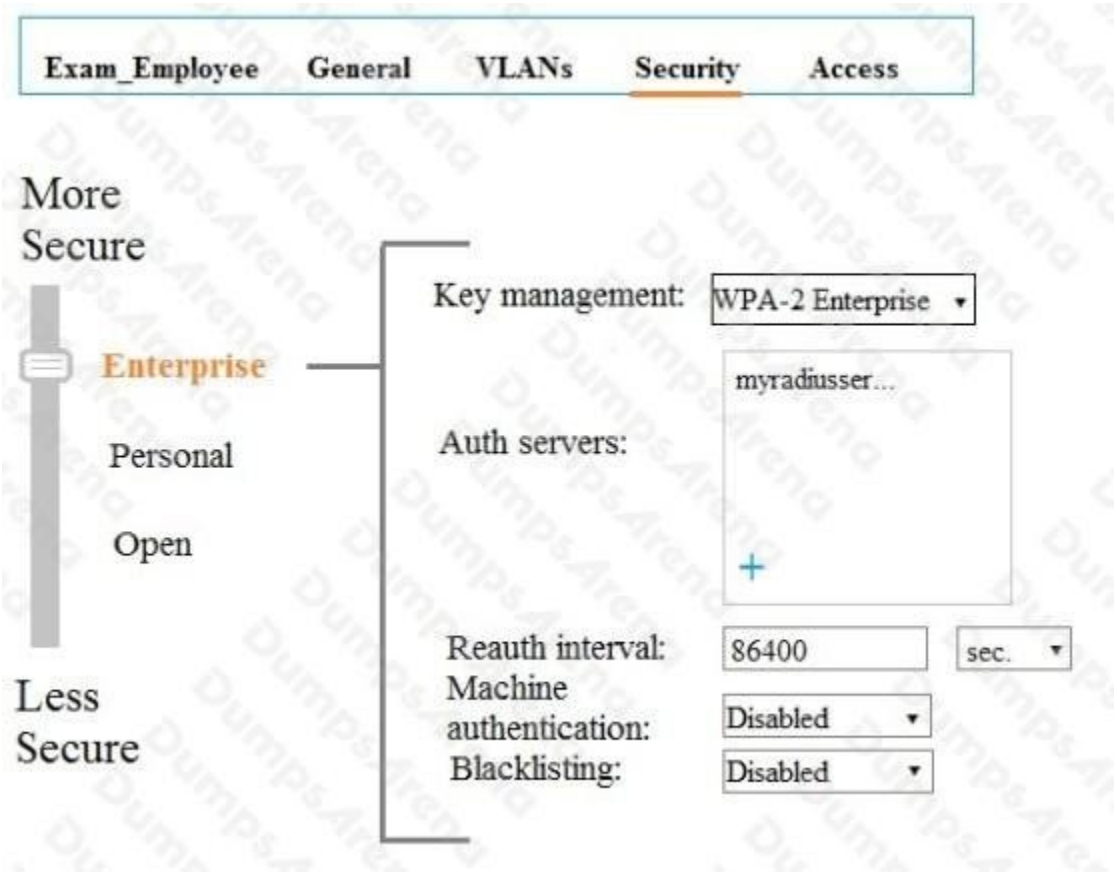


Exhibit 2



Network administrators use the Aruba Mobility Master (MM) wizard to create a WLAN and do not manually alter any of the profiles for that WLAN. The exhibits show some of the settings for the WLAN. Some wireless users cannot successfully connect to the WLAN. Network administrators attempt to connect on their own machines with a test account, and the connection is successful. They attempt to connect with the same account on user clients, and the connection fails.

Which issue could prevent authentication from completing correctly?

A. The user clients have unauthorized MAC addresses, so the RADIUS server rejects the authentication even though the username and password are correct.

B. The user clients do not trust the RADIUS server certificate and are configured not to prompt users to trust new certificates.

C. Some access points (APs) are not configured as clients on the RADIUS server, so user clients connected to them cannot authenticate.

D. The RADIUS server has reached the maximum number of RADIUS clients that it can support, so it rejects new wireless clients.

ANSWER: B

Explanation:

The user clients do not trust the RADIUS server certificate and are configured not to prompt users to trust new certificates. This behavior is consistent with an enterprise WLAN using 802.1X/EAP authentication: the wireless client must validate the certificate presented by the authentication server before it can safely establish the protected EAP exchange and submit credentials. Certificate validation depends on the endpoint configuration, including whether the issuing root certificate is trusted, whether the server name matches, and whether the client is permitted to display a trust prompt. Therefore, the same test account can authenticate successfully on an administrator's machine that already trusts the issuing certificate authority, while failing on user devices that do not have the required trust chain and cannot ask the user to accept a new certificate. The WLAN created by the Mobility Master wizard can correctly forward authentication to RADIUS; the failure occurs on affected client devices during EAP server-certificate validation, before username and password validity can resolve the connection. Administrators should deploy the appropriate trusted root and intermediate CA certificates and configure the wireless supplicant to validate the intended RADIUS server identity. See Microsoft's EAP network access documentation and Aruba's 802.1X authentication documentation.

QUESTION NO: 10

A company has a Mobility Master (MM)-based solution. A network administrator wants to monitor data transfer speed ranges of all currently connected clients.

Which dashboard page in the MM interface should the administrator visit?

A. Security

B. Performance

C. Traffic Analysis

D. Network

ANSWER: B

Explanation:

Performance is the appropriate dashboard page because it provides client-performance visibility, including the distribution of associated clients by wireless data-rate ranges. This lets an administrator quickly see how many currently connected clients are operating at different transmit/receive rate levels, which is the needed high-level view for assessing client connection speeds across the managed environment. The dashboard is intended to summarize operational performance indicators rather than require an administrator to inspect each client individually. Data-rate distribution is useful for identifying a broad population of clients operating at unexpectedly low rates and for determining whether further RF, coverage, capability, or client-specific investigation is warranted. In an Mobility Master deployment, the dashboard aggregates monitoring information from managed devices so that the administrator can review the overall client-performance state from the centralized interface. Aruba's ArubaOS documentation describes the dashboard's performance monitoring views and client-related statistics in the ArubaOS Dashboard documentation. The complete ArubaOS 8.4 web-help collection is also available from the ArubaOS 8.4 documentation home page.

QUESTION NO: 11

Which class of controller is more appropriate in a branch installation with up to 64 APs?

A. 7008

B. 7030

C. 7205

D. 7210

ANSWER: B

Explanation:

7030 is the appropriate controller for a branch deployment supporting up to 64 access points. Aruba's 7000 Series branch controllers were designed for small and medium branch environments, where local controller services are needed without deploying a higher-capacity campus controller. Within that family, the 7030 provides the access-point scale needed for this requirement while retaining a branch-oriented form factor and feature set. It can terminate AP tunnels and provide the centralized ArubaOS services required for WLAN operation, such as AP management, client connectivity, policy enforcement, and security services. Selecting a platform whose supported AP capacity aligns with the expected maximum is an important sizing practice: it provides sufficient headroom for the stated branch requirement without unnecessarily using a controller class intended for larger campus aggregation. Aruba documentation identifies the 7000 Series as its branch-controller family and provides the platform specifications used to match controller models to AP scale. See the Aruba 7000 Series data sheet and Aruba's Gateways and Controllers product information.

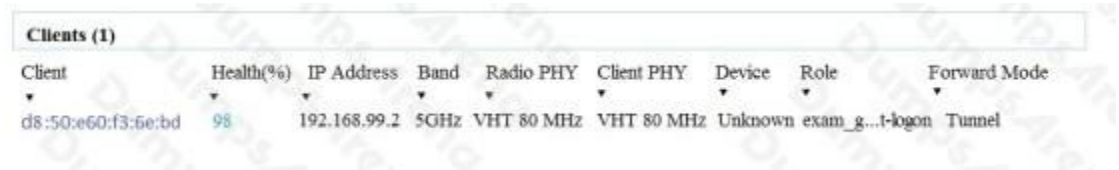
QUESTION NO: 12

Refer to the exhibits.

Exhibit 1



Exhibit 2



A company has a Mobility Master (MM)-based solution with a guest WLAN. Users can connect to the WLAN, but they receive the error shown browser rather than see login page.

Exhibit 2 shows the status for one of the guest clients.

What is one issue that could cause the errors described?

A. The firewall blocks DHCP traffic between the guest clients and the DHCP server.

B. The DHCP pool for guests does not assign users a DNS server address.

C. The MM and Mobility Controllers (MCs) have invalid certificates.

D. The Captive Portal is not enabled for the role to which these clients are assigned.

ANSWER: B

Explanation:

The DHCP pool for guests does not assign users a DNS server address. A guest client can successfully associate to the WLAN and receive an IP address, subnet mask, and default gateway while still being unable to resolve website names if DHCP option 6 does not provide usable DNS-server addresses. Captive-portal detection normally begins when the client browser or operating system attempts to reach an Internet hostname. The controller can intercept the resulting HTTP request and redirect the unauthenticated client to the guest login page. Without DNS resolution, however, the client cannot translate that hostname into an IP address and therefore does not generate the web request that the captive portal needs to redirect. The browser instead displays a name-resolution or site-reachability error rather than the portal page. This also aligns with a client status that shows successful WLAN connectivity and addressing but an unsuccessful guest browsing experience. Aruba's captive-portal workflow depends on clients having valid network services, including DHCP-provided addressing and DNS reachability, before they can reliably be redirected and authenticate. See Aruba's Captive Portal documentation and the IETF definition of DHCP DNS-server option 6 in RFC 2132.

QUESTION NO: 13

A network administrator examines a list of 2.4GHz clients with low performance in the Mobility Master (MM) dashboard. Which property for a client should pose a concern as a potential performance issue?

A. Radio PHY of HT 20MHz

B. Max speed of 72Mbps

C. Goodput data rate of 12 Mbps

D. Usage of 10 MB

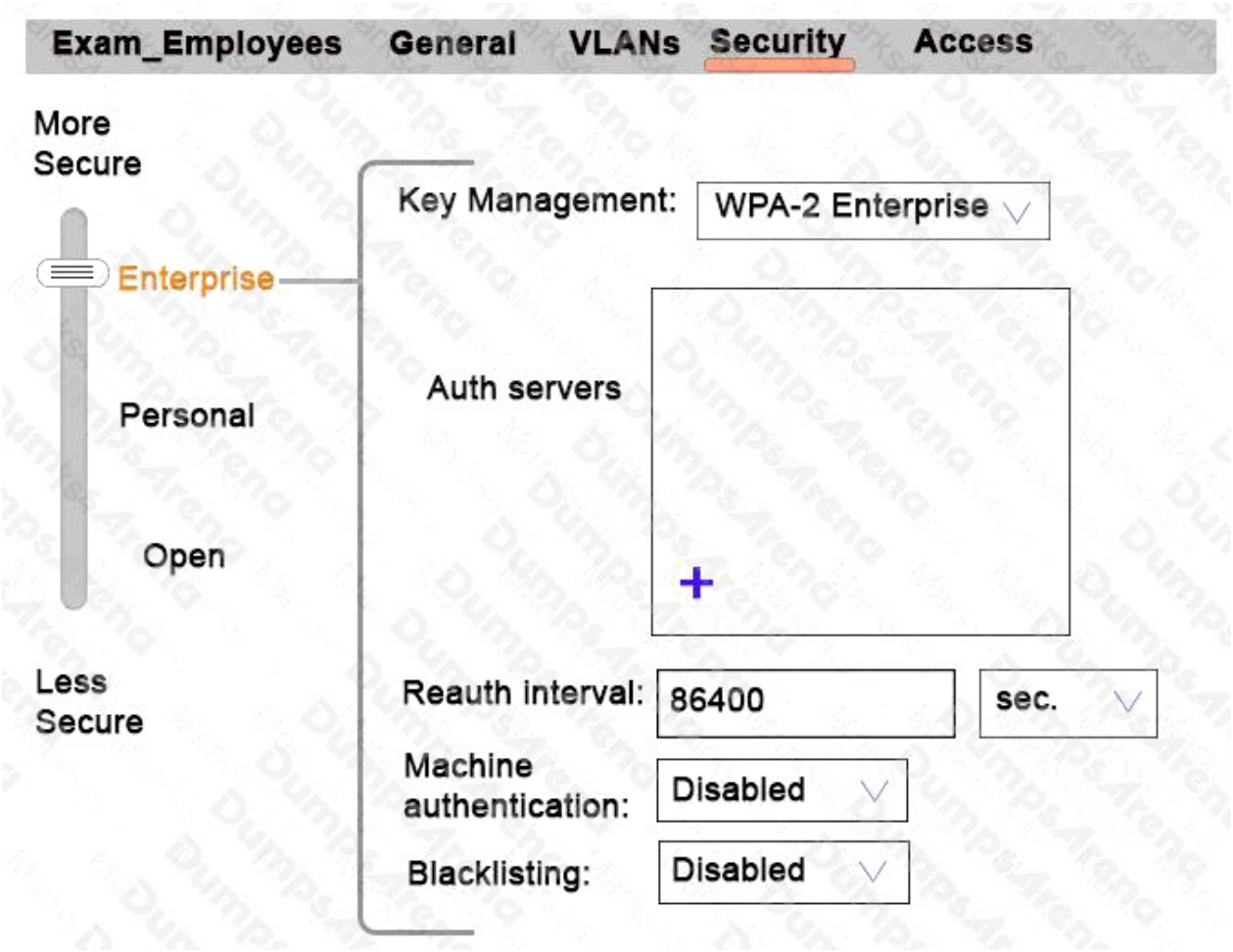
ANSWER: C

Explanation:

Goodput data rate of 12 Mbps should be investigated because goodput represents the rate at which useful payload data is successfully delivered, rather than merely the PHY rate negotiated by the radio. A 12 Mbps goodput value for a client identified as low-performing indicates that the client is achieving limited effective throughput. This can result from RF conditions such as weak signal or interference, retransmissions, contention on the 2.4 GHz channel, or a client that is transmitting and receiving at low effective rates. In a Mobility Master deployment, the client monitoring and dashboard views are intended to help administrators correlate client experience with live radio and traffic statistics. Goodput is especially useful for this purpose because it reflects the usable data rate experienced after wireless overhead and unsuccessful transmissions affect performance. The administrator should use the client details, AP radio information, and RF statistics to determine whether the low goodput is persistent and whether remediation such as improving coverage, reducing interference, or moving capable clients to 5 GHz is appropriate. ArubaOS monitoring documentation is available in the ArubaOS 8.4 Web Help, and Aruba's documentation portal provides the associated technical documentation.

QUESTION NO: 14

Refer to the exhibit.



Network administrators need to set up a WLAN that uses WPA2 encryption and authenticates users with a preshared key (PSK) that is the same for all users. Administrators do not see where they should specify the option for the preshared key.

What should the administrators do?

A. Click Personal in the slide bar.

B. Click the + icon in the Authentication server section

C. Return to the first page in the wizard and select the guest option

D. Configure an L3 authentication profile after the WLAN wizard is complete

ANSWER: A

Explanation:

Click Personal in the slide bar. This selection changes the WLAN security configuration from an enterprise authentication model to a personal security model. Personal WLAN security is intended for deployments in which all clients use a common pre-shared secret, rather than supplying individual credentials to an authentication server. After Personal is selected, the wizard presents the fields needed to configure a WPA2-Personal security method and enter the shared passphrase used by wireless clients.

In Aruba WLAN configuration, WPA2 can be paired with different authentication approaches. WPA2-Personal uses a shared PSK and is appropriate where a common password is required. The controller derives the encryption keys used for the protected wireless connection from that passphrase during client association. Selecting the Personal category is therefore the required wizard step to expose the PSK setting and complete the requested WLAN configuration.

Aruba's WLAN configuration documentation describes configuring WLAN security profiles and selecting the appropriate authentication method: ArubaOS 8.4 Unified WLAN Configuration. Aruba's security guidance also distinguishes personal pre-shared-key authentication from enterprise authentication: ArubaOS 8.4 Security.

QUESTION NO: 15

An Aruba Mobility Master (MM)-based solution has a WLAN that uses WPA2-Enterprise security. A test login on a wireless client fails.

How can a network administrator determine whether the RADIUS server rejected the credentials or another issue occurred?

A. View Technical Support information for the MM.

B. Ping the IP address configured as the RADIUS server.

C. Use the MM AAA Server Test Diagnostic tool.

D. Use the tools in the MM Dashboard > Security window.

ANSWER: C

Explanation:

Use the MM AAA Server Test Diagnostic tool. This diagnostic sends an authentication test to the configured external RADIUS server using the selected server configuration and supplied test credentials. Its result directly indicates the RADIUS transaction outcome, enabling the administrator to distinguish an explicit RADIUS Access-Reject response—which means the server received the request and rejected the authentication—from conditions such as server unreachability, timeout, shared-secret mismatch, or another communication or configuration failure. This makes it an appropriate first validation step when a WPA2-Enterprise client cannot log in, because it tests the AAA path independently of the wireless client's association and 802.1X exchange. The ArubaOS WebUI provides AAA server diagnostic capabilities for testing configured authentication servers, while the ArubaOS command reference documents the associated AAA and server-testing functions. After confirming the diagnostic result, the administrator can focus either on the RADIUS account or policy data when an explicit reject is returned, or on connectivity and AAA configuration when no valid server response is obtained. See the ArubaOS 8.4 Web Help and the ArubaOS 8.4 Command-Line Interface Reference Guide.

QUESTION NO: 16

A company has two Mobility Controllers (MCs) that serve different buildings. Wireless users must retain their IP addresses when they roam between APs controlled by different MCs.

Which configuration is required on the MCs?

A. Place the MCs in the same mobility domain.

B. Assign the MCs to the same AP group.

C. Configure the same LMS IP address on both MCs.

D. Enable AirMatch on both MCs.

ANSWER: A

Explanation:

Place the MCs in the same mobility domain. A mobility domain establishes the relationship between Aruba controllers that is required to support inter-controller mobility. When controllers participate in the same mobility domain, ArubaOS can maintain client mobility state and support Layer 3 roaming between them.

This enables a client to retain its original IP address while moving to an AP controlled by another MC, provided that the overall mobility and VLAN design supports the roam. Aruba describes controller mobility configuration in the ArubaOS mobility documentation.

QUESTION NO: 17

Which task can an Aruba Spectrum Monitor (SM) perform?

A. Analyze wireless traffic patterns at the application level.

B. Optimize RF through the AP channel and transmit power plans.

C. Analyze RF signals to determine the cause of non-802.11 interference.

D. Help to detect rogue APs in the environment.

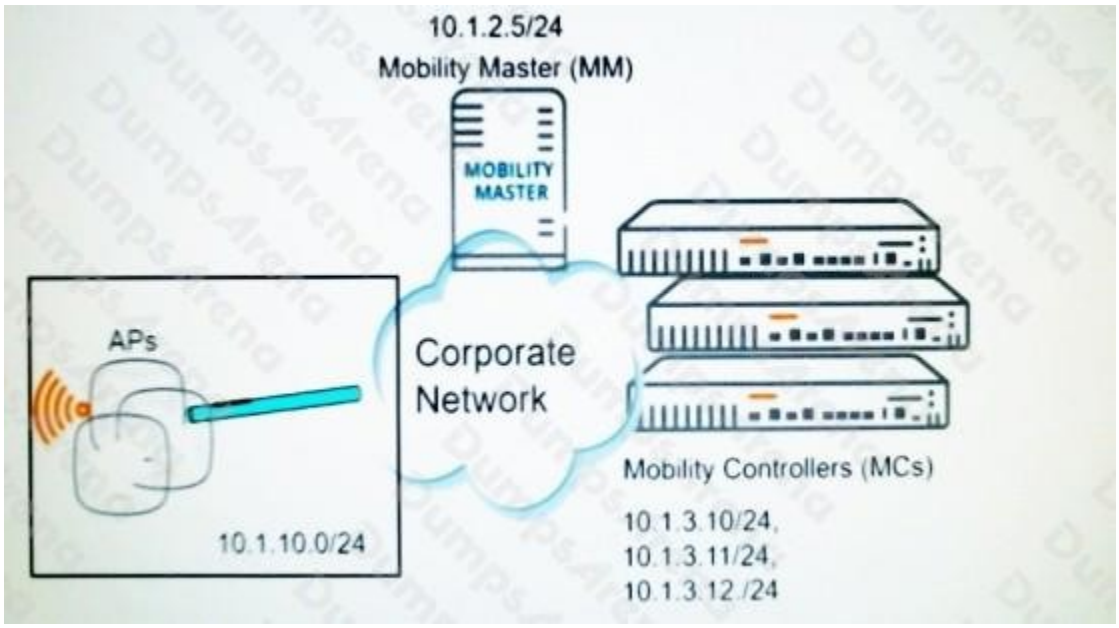
ANSWER: C

Explanation:

Analyze RF signals to determine the cause of non-802.11 interference. An Aruba Spectrum Monitor is a radio operating in spectrum-monitor mode that dedicates its time to observing RF energy rather than serving wireless clients. It collects spectrum data and identifies interference sources that occupy the wireless bands but do not use Wi-Fi protocols. This capability helps administrators investigate RF conditions that can degrade WLAN performance, such as microwave ovens, Bluetooth devices, cordless phones, wireless cameras, and other noise-generating equipment. The monitor reports characteristics including the interference type, frequency or channel range, signal strength, and duty cycle, enabling an administrator to correlate the RF activity with connectivity or performance symptoms and locate the likely source. ArubaOS uses spectrum analysis to classify recognized non-Wi-Fi interferers and present actionable RF information through its management and monitoring interfaces. This is specifically a spectrum-analysis function: it examines the underlying radio-frequency environment to establish whether non-802.11 energy is affecting the WLAN. Aruba documents spectrum monitoring and interference detection in its ArubaOS monitoring guidance and spectrum-analysis documentation: ArubaOS 8.4 Spectrum Analysis and ArubaOS 8.4 Monitoring.

QUESTION NO: 18

Refer to the exhibit.



What is a valid way to help the APs discover devices that can control them?

A. Set up an Aruba Central subscription, and ensure that APs can reach the Internet.

B. Enable CPSec, and ensure the Mobility Master (MM) and Mobility Controllers (MCs) trust the Aruba certificates installed on the APs at the factory.

C. Specify the Mobility Master (MM) IP address in DHCP option 43 on the network DHCP server.

D. Map the Mobility Controller (MC) IP addresses to the aruba-master name on the network DNS server.

ANSWER: D

Explanation:

Mapping the Mobility Controller (MC) IP addresses to the `aruba-master` name on the network DNS server is a valid controller-discovery method for Aruba access points. During its startup and discovery process, an AP can perform a DNS lookup for the well-known hostname `aruba-master`. When DNS returns the address of a reachable managed device, the AP can send its discovery request to that controller and proceed with the normal adoption and provisioning workflow. This method is particularly useful because it centralizes the discovery configuration in DNS: APs do not need individually configured controller addresses, and the DNS record can be updated if controller addressing changes. In an ArubaOS 8 deployment, APs are ultimately terminated and managed by Mobility Controllers, while the Mobility Master provides centralized management and configuration orchestration rather than serving as the AP's direct control-plane termination point. Aruba documents DNS resolution of `aruba-master` as one of the supported AP discovery mechanisms. See the ArubaOS AP discovery guidance at ArubaOS 8.4 AP Discovery and the ArubaOS user guide library at ArubaOS 8.4 Web Help.