HPE6-A90 Dumps

Shared by Horne on 10-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the distinction between L3 routed and L3 NATed SSIDs?

Options:

A- Routed translates to AP tunnel IP and avoids route advertisement; NATed preserves client source IP and requires route redistribution.
B- Routed preserves client source IP and requires route advertisement; NATed translates to AP tunnel IP and reduces route distribution needs.
C- Routed balances clients evenly across VPNCs; NATed assigns clients based on route weight from the orchestrator.
D- Routed uses corporate DHCP and L2 simulation; NATed uses corporate DHCP and L3 routing to the data center.

Answer:

B

Explanation:

Technical explanation

In a Layer 3 routed Microbranch design, client source addresses remain visible end-to-end and the enterprise must advertise or otherwise route the local client subnet toward return traffic. In an L3 NATed design, the AP translates outbound sessions to a tunnel or uplink address, reducing the need to distribute a route for every branch WLAN subnet. NAT simplifies routing but can limit source-IP visibility and inbound connection behavior. Choose the mode based on enterprise identity, application reachability and route-scale requirements rather than treating both modes as equivalent forwarding. In a routed Microbranch subnet, the VPN concentrator or upstream network needs a return route toward the branch client pool. With NAT, outside services instead see the AP translated address, reducing route advertisement needs but obscuring individual client addressing.

Option A reverses source translation and route-advertisement behavior. Option C concerns gateway-client balancing, not Microbranch routing modes, and D incorrectly assumes corporate DHCP/L2 simulation is intrinsic to both L3 modes. The deciding factor is whether upstream networks see the client subnet or an AP-translated address.

Official HPE references | Layer 3 Microbranch - Validated Solution Guide * Configuring VLANs - Microbranch | Study-guide topic: Introduction to AOS-10

Question 2

Question Type: MultipleChoice

Which three AP series are supported by AOS-10? (Choose three.)

Options:

A- 2xx series
B- 3xx series
C- 4xx series
D- 5xx series
E- 7xx series

Answer:

B, D, E

Explanation:

Technical explanation

The series shorthand is a quick screening question rather than a migration compatibility matrix. Supported AOS-10 hardware spans selected 3xx, 5xx, and 7xx families. A serial-number inventory should be matched with HPE's model-level support table and software release before scheduling AOS-10 adoption. Some older 3xx hardware has minimum or final supported releases; family membership does not override the exact SKU restrictions.

The options name broad hardware families rather than exact SKUs. The 2xx generation is outside the supported AOS-10 set, and ''4xx series'' is not included in the referenced supported-series choices. A 3xx selection still demands model-level and release-level validation.

Official HPE references | Supported Access Point Platforms for AOS-10 * AOS-10 Cloud Services | Study-guide topic: Introduction to AOS-10

Question 3

Question Type: MultipleChoice

Which category of information is included in telemetry sent from AOS-10 access points to HPE

Aruba Networking Central?

Options:

A- DHCP lease records issued to wireless clients
B- User authentication secrets exchanged during association
C- Routing table entries learned from upstream devices
D- Operational and radio metrics reported by the access point

Answer:

D

Explanation:

Technical explanation

AOS-10 APs send operating state, radio channel and transmit-power parameters, RF noise/retry indicators, client counts and related performance telemetry to Central. Analytics services aggregate these measurements for RF optimization, health scoring, anomaly detection and troubleshooting. Authentication secrets are not normal monitoring telemetry, and AP reporting is not a replacement for extracting arbitrary upstream router tables. When connectivity to Central is disrupted, APs can continue their currently applied forwarding and RF plans, although cloud-dependent optimizations may be delayed. A useful operational validation is to compare AP-reported RF counters and connectivity status before and after a known interference or availability event. The resulting time-series permits trend diagnosis without copying authentication credentials into the management platform.

DHCP lease information and learned routes can exist elsewhere in the topology but are not the defining AOS-10 AP telemetry category. Secret authentication material is not a routine performance-telemetry feed. Radios report operational metrics used in health and RF decisions.

Official HPE references | AOS-10 Cloud Services * Roaming and the Key Management Service | Study-guide topic: Introduction to AOS-10

Question 4

Question Type: MultipleChoice

Which capability is enabled by a firewall's Deep Packet Inspection (DPI) behavior?

Options:

A- Assigning IP addresses based on DHCP option fields and relay behavior
B- Selecting RF channels based on airtime utilization and interference levels
C- Performing SSL inspections looking for known threat vectors
D- Enforcing policy based on recognized applications and traffic categories

Answer:

D

Explanation:

Technical explanation

DPI identifies traffic according to application signatures and behavioral characteristics beyond traditional IP-address, port and protocol matches. That classification enables role-based rules and QoS decisions for applications such as collaboration, streaming or file sharing, even when services reuse common transport ports. DPI should not be equated with universal SSL interception; decryption requires separate, explicit capabilities and trust arrangements. Nor does it perform DHCP address allocation or Wi-Fi channel selection, which belong to different network subsystems.

DHCP relaying and RF channel selection are separate functions. Decrypting arbitrary SSL traffic is not implied by DPI; that would require additional TLS-interception capabilities and trust. DPI is useful because recognized application identities can be inputs to traffic policy.

Official HPE references | Application Visibility * AOS-10 Cloud Services | Study-guide topic: Introduction to AOS-10

Question 5

Question Type: MultipleChoice

How are roles, policies, and rules structured in the firewall model?

Options:

A- Roles reference rules, and rules contain ordered policies.
B- Policies reference rules, and rules inherit their role membership.
C- Policies reference roles, and roles contain ordered rule sets.
D- Roles reference policies, and policies contain ordered rules.

Answer:

D

Explanation:

Technical explanation

A user role is the attachment point for one or more firewall policies, and every policy consists of an ordered sequence of match/action rules. Match criteria can involve source/destination objects, protocols, ports and application identification; outcomes can include allow, deny, redirect or additional traffic treatment. Evaluation order matters because broader permissions placed before a specific restriction can defeat the intended access boundary. Verify the role assigned by AAA and whether the enforcement location is the AP, switch or gateway before assessing effective security behavior. Consider a role named GUEST: it references an internet-access policy, whose first rule denies RFC1918 management networks and later rules allow required services. Changing the policy changes the role's effective forwarding behavior.

Rules do not contain nested policies; roles do not reference loose rules independently of policy organization. Nor do policies ''inherit'' role membership in the reverse direction. Roles bind policy objects, and each policy evaluates an ordered sequence of matching rules.

Official HPE references | Configuring VLAN Settings for WLAN SSID in Tunnel and Mixed Mode * AOS-10 Cloud Services | Study-guide topic: Introduction to AOS-10

Question 6

Question Type: MultipleChoice

How does the control-plane model of AOS-10 access points differ from Instant AP deployments?

Options:

A- AOS-10 access points elect a conductor to coordinate RF and authentication services.
B- AOS-10 access points operate independently and rely on HPE Aruba Networking Central for control functions.
C- AOS-10 access points forward telemetry exclusively to peer access points.
D- AOS-10 access points manage roaming decisions through a local controller.

Answer:

B

Explanation:

Technical explanation

Instant AP groups traditionally use a local elected virtual conductor or equivalent cluster coordination model. AOS-10 APs do not select a local AP conductor for these centralized functions; configuration, RF planning, neighbor coordination and key-management services are orchestrated by Central. This does not imply that an AP is helpless during a cloud outage: existing datapath and configuration continue to operate within documented survivability limits. Some new coordination operations may be deferred until Central connectivity returns, whereas previously synchronized roaming information may remain available.

An elected AP conductor is the Instant model being contrasted, not the AOS-10 architecture. Peer-only telemetry and local controller-based roaming do not describe Central's cloud-supported services; individual APs maintain their datapaths while Central provides relevant shared services.

Official HPE references | AOS-10 Cloud Services * Roaming and the Key Management Service | Study-guide topic: Introduction to AOS-10

Question 7

Question Type: MultipleChoice

What are the benefits of gateway clustering in AOS-10?

Options:

A- RF channel planning, transmit power calibration, band steering, and airtime fairness
B- Seamless roaming, hitless failover, client state synchronization, and load balancing
C- DHCP snooping, dynamic ARP inspection, port security, and storm control tuning
D- Spanning tree suppression, MAC table merging, link aggregation, and stack monitoring

Answer:

B

Explanation:

Technical explanation

Gateway clustering couples high-availability datapath behavior with user state synchronization, load distribution and WLAN mobility support. Client traffic can be anchored and balanced across available gateways, and the cluster can preserve service through supported node failures or controlled software upgrades. Confirm that enough cluster capacity remains when a member is lost and that every gateway has consistent roles and tunnel reachability. RF channel planning belongs to AirMatch; DHCP snooping and spanning-tree are separate switching/security mechanisms rather than principal gateway-cluster benefits. A cluster maintains user-to-gateway mappings and shares relevant state across peers, improving failure recovery and distributing load. A design without valid cluster connectivity cannot provide that continuity simply because two gateways are online.

RF power/channel algorithms belong to radio management, and DHCP snooping or ARP inspection belong to switch security. Spanning tree and stack monitoring are Layer 2 infrastructure functions. Cluster value is the coordinated client state and traffic continuity between gateway peers.

Official HPE references | Configuring VLAN Settings for WLAN SSID in Tunnel and Mixed Mode * AOS-10 Cloud Services | Study-guide topic: Introduction to AOS-10

To Get Premium Files for HPE6-A90 Visit
https://www.p2pexams.com/products/hpe6-a90

For More Free Questions Visit
https://www.p2pexams.com/hp/pdf/hpe6-a90

