HP ACP - Campus Access HPE7-A01 Practice Questions

Shared by Dunn on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network Traffic originating from 10.2.250.0/24 should use a new default route to 10.1.1.253. Other non-default routes for this subnet should not be affected by this change.

What are two parts of the solution for these requirements? (Select two.)

A)

```
pbr-action-list def_route_test
    default-nexthop 10.1.1.253/24
```

B)

```
class ip test_subnet
    10 match any 10.2.250.0/24 any
policy def_route_test_policy
    10 class ip test_subnet action pbr def_route_test
interface vlan 100
    ip address 10.2.250.0/24
    apply policy pbr_test routed in
```

C)

```
class ip test_subnet
    10 match any 10.2.250.0 255.255.255.0 any
policy def_route_test_policy
    10 class ip ip_test_subnet action pbr def_route_test
interface vlan 100
    ip address 10.2.250.0/24
    apply policy pbr_test routed out
```

D)

```
pbr-action-list def_route_test
    default-nexthop 10.1.1.253
    interface null
```

E)

```
pbr-action-list def_route_test
    nexthop 10.1.1.253
    interface null
```

Options:

A- Option A
B- Option B
C- Option C
D- Option D
E- Option E

Answer:

C, E

Explanation:

Two parts of the solution for these requirements are Option C and Option E.

Option C is a part of the solution because it defines a policy-based routing action list named route_test, which specifies the next hop IP address as 10.1.1.253 for the matching traffic. This is the new default route that the user wants to use for the subnet 10.2.250.0/24. The interface null parameter indicates that the traffic will be routed to the next hop without using a specific interface1.

Option E is a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 250, which has an IP address of 10.2.250.1/24. This is the subnet that the user wants to test the new default route for. The apply policy command enables policy-based routing on the interface and associates it with the action list2.

Option A is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify the next hop IP address as 10.1.1.253, which is the new default route that the user wants to use. Instead, it specifies a next hop IP address of 10.1.1.254, which is different from the requirement.

Option B is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify any next hop IP address at all, which is necessary for policy-based routing to work. Instead, it specifies an interface null parameter without any IP address, which is invalid.

Option D is not a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 200, which has an IP address of 10.2.200.1/24. This is not the subnet that the user wants to test the new default route for, but a different subnet that should not be affected by this change.

Question 2

Question Type: MultipleChoice

What is an Aruba-recommended best practice for hardening that only applies to Aruba CX 6300 series switches with dedicated management ports?

Options:

A- Implement a control plane ACL to limit access to approved IPs and/or subnets
B- Manually enable Enhanced Security Mode from a console session.
C- Disable all management services on the default VRF.
D- Create a dedicated management VRF, and assign the management port to it.

Answer:

D

Explanation:

This is an Aruba-recommended best practice for hardening that only applies to Aruba CX 6300 series switches with dedicated management ports. A dedicated management port is a physical port that is used exclusively for out-of-band management access to the switch. A dedicated management VRF is a virtual routing and forwarding instance that isolates the management traffic from other traffic on the switch. By creating a dedicated management VRF and assigning the management port to it, the administrator can enhance the security and performance of the management access to the switch. The other options are incorrect because they either do not apply to switches with dedicated management ports or do not follow Aruba-recommended best practices. Reference: https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

Question 3

Question Type: MultipleChoice

A customer is using Aruba Cloud Guest, but visitors keep complaining that the captive portal page keeps coming up after devices go to sleep Which solution should be enabled to deal with this issue?

Options:

A- MAC Caching under the splash page
B- MAC Caching under the user-role

C- Wireless Caching under the splash page
D- MAC Caching under the WLAN

Answer:

A

Explanation:

MAC Caching is a feature that allows a guest user to bypass the captive portal page after the first authentication based on their MAC address1MAC Caching can be enabled under the splash page settings in Aruba Cloud Guest2MAC Caching can improve the user experience and reduce the network overhead by eliminating the need for repeated authentication.

Question 4

Question Type: MultipleChoice

The customer needs a network hardware refresh to replace an aging Aruba 5406R core switch pair using spanning tree configuration with Aruba CX 8360-32YC switches What is the benefit of VSX clustering with the new solution?

Options:

A- stacked data-plane
B- faster MSTP converge processing
C- dual Aruba AP LAN port connectivity for PoE redundancy
D- dual control plane provides better resiliency

Answer:

D

Explanation:

VSX clustering is a feature that allows two Aruba CX switches to operate as a single logical device, providing high availability, scalability, and simplified management. VSX clustering has several benefits over spanning tree configuration, such as:

Dual control plane provides better resiliency. Unlike stacking, where switches share a single control plane, VSX switches have independent control planes that synchronize their states over

an inter-switch link (ISL). This means that if one switch fails or reboots, the other switch can continue to operate without affecting traffic flows or network services.

Active-active forwarding provides better performance. Unlike spanning tree, where some links are blocked to prevent loops, VSX switches use all available links for forwarding traffic, providing load balancing and increased bandwidth utilization.

Multichassis LAG provides better redundancy. Unlike single-chassis LAG, where all member ports belong to one switch, VSX switches can form multichassis LAGs with downstream or upstream devices, where member ports are distributed across both switches. This provides link redundancy and seamless failover in case of switch or port failure.

Question 5

Question Type: MultipleChoice

You need to drop excessive broadcast traffic on an ingress port or an ArubaOS-CX switch. What is the best feature to use for this task?

Options:

A- DWRR queuing
B- Strict queuing
C- Rate limiting
D- QoS shaping

Answer:

C

Explanation:

According to the Aruba Documentation Portal1, the ArubaOS-CX switch supports various features to control the ingress traffic on specific ports, such as rate limiting, QoS shaping, and access control. These features can help reduce the impact of excessive broadcast traffic on the network performance and availability.

This is because rate limiting is a feature that allows you to limit the inbound or outbound traffic on a port based on a percentage of the port capacity or a fixed amount of bytes per second.Rate limiting can help prevent broadcast storms by reducing the amount of broadcast packets that enter or leave a port

https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-access-c

ontrol.htm2:
https://community.arubanetworks.com/blogs/esupport1/2021/02/08/broadcast-storm-containment-in-aruba-pvos-switches3:
https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8160_ssw_mcg/content/ch05.html

Question 6

Question Type: MultipleChoice

You are setting up a customer's 150 headless loT devices that do not support 802.1 X. What should you use?

Options:

A- Multiple Pre-Shared Keys (MPSK) Local
B- Multiple Pre-Shared Keys (MPSK) with WPA3-AES
C- HPE Aruba Networking ClearPass profiling with MAC-AUTH
D- HPE Aruba Networking ClearPass profiling with WPA-PSK

Answer:

A

Question 7

Question Type: MultipleChoice

You are building a configuration in Central that will be used for a standardized network design for small sites for your company, you want to use GUI configuration for gateways and Aps, while template configuration for switches. You need to align with Aruba best practices.

Which set of actions will satisfy these requirements?

Options:

A- Create one group in Central for switches a second group for APs. and a third group for gateways Create a unique site for each location, and assign devices to the appropriate site.
B- Create one group in Central for switches and a second group for APs and gateways. Create a unique site for each location, and assign devices to the appropriate site.

C- Create a single group in Central. Create a unique site for each location, and assign devices to the appropriate site.
D- Create a single group in Central. Create a unique site for each type of device, and assign devices to the appropriate site.

Answer:

C

Explanation:

This is because option C shows how to create a single group in Central with different configuration methods defined for each device type. For example, you can create a group with the name Group1, and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (Group1). If a device type in the group is marked for template-based configuration method, the group name is prefixed with TG (TG Group1).You can use Group1 as the group ID for workflows such as user management, monitoring, reports, and audit trail2.

https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/abt-groups.htm2: https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/groups.htm