



Free Questions for HPE7-A01

Shared by Berry on 16-10-2023

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)



Question 1

Question Type: MultipleChoice

What is a primary benefit of BSS coloring?

Options:

- A- BSS color tags improve performance by allowing clients on the same channel to share airtime.
- B- BSS color tags are applied to client devices and can reduce the threshold for interference
- C- BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference
- D- BSS color tags improve security by identifying rogue APs and removing them from the network.

Answer:

C

Explanation:

BSS coloring is a mechanism that helps identify the BSS Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients on the same channel and differentiate them from other BSS on the same channel. Each BSS is assigned a color code, which is a 6-bit value that is carried in the PHY header of the Wi-Fi frames. By using BSS coloring, the APs and clients can reduce the threshold for interference detection and avoid unnecessary backoff or retransmissions when they detect frames from other BSS with different colors. This can improve the spectral efficiency and throughput of the network. The other options are incorrect because they do not describe the primary benefit of BSS coloring.

Question 2

Question Type: OrderList

List the firewall rule derivation flow in the correct order

Firewall Role	Order
Authentication default role	
Initial role assigned	
Server derived role	
User derived role	

⏪ ⏩
⏴ ⏵

Answer:

Server derived role User derived role Authentication default role Initiation role assigned

Question 3

Question Type: DragDrop

Match the solution components of NetConductor (Options may be used more than once or not at all.)

Client Insights	Cloud Auth		Built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots
The Fabric Wizard	Policy Manager		Defines user and device groups and creates the associated access enforcement rules for the physical network
			Enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores
			Simplifies the creation of the overlays using an intuitive, graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways

Answer:

See the Answer in the Premium Version!

Question 4

Question Type: MultipleChoice

You are troubleshooting an issue with a pair of Aruba CX 8360 switches configured with VSX. Each switch has multiple VRFs. You need to find the IP address of a particular client device with a known MAC address. You run the "show arp" command on the primary switch in the pair but do not find a matching entry for the client MAC address.

The client device is connected to an Aruba CX 6100 switch by VSX LAG.

Which action can be used to find the IP address successfully?

A)

Run the following command on the CX 6100 switch:

```
show mac-address-table
```

B)

Run the following command on the VSX primary switch:

```
show arp all-vrfs
```

C)

Run the following command on the VSX primary switch:

```
show mac-address-table
```

D)

Run the following command on the CX 6100 switch:

```
show arp all-vrfs
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

B

Explanation:

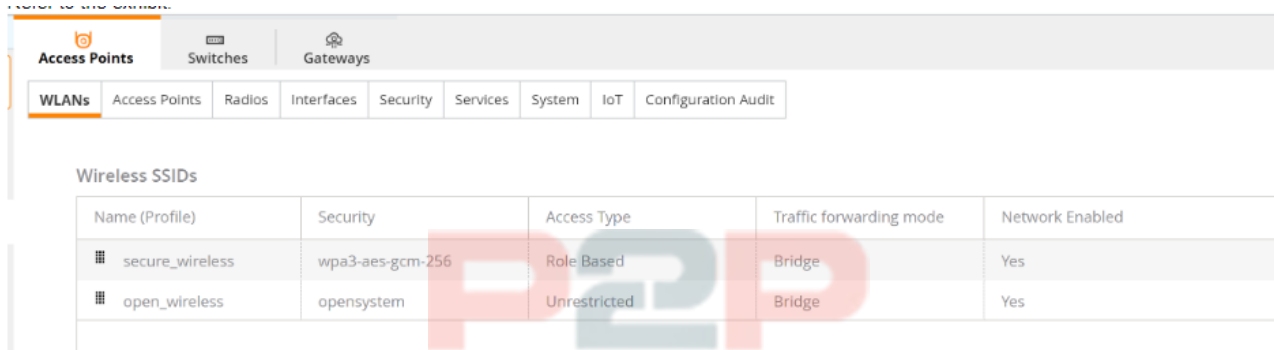
The show arp command displays the ARP table for a specific VRF or all VRFs on the switch. The ARP table contains the IP address to MAC address mappings for hosts that are directly connected to the switch or reachable through a gateway. If the client device is connected to another switch by VSX LAG, the ARP entry for the client device will not be present on the primary switch unless it has communicated with it recently. Therefore, to find the IP address of the client device, the administrator should run the show arp command on the secondary switch in the VSX pair, specifying the VRF name that contains the client device's subnet. Reference:

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

Question 5

Question Type: MultipleChoice

Refer to Exhibit:



The screenshot shows the Aruba Central configuration interface. The top navigation bar includes 'Access Points', 'Switches', and 'Gateways'. Below this, a sub-navigation bar highlights 'WLANs' and includes links for 'Access Points', 'Radios', 'Interfaces', 'Security', 'Services', 'System', 'IoT', and 'Configuration Audit'. The main content area is titled 'Wireless SSIDs' and contains a table with the following data:

Name (Profile)	Security	Access Type	Traffic forwarding mode	Network Enabled
secure_wireless	wpa3-aes-gcm-256	Role Based	Bridge	Yes
open_wireless	opensystem	Unrestricted	Bridge	Yes

A company has deployed 200 AP-635 access points. To take advantage of the 6 GHz band, the administrator has attempted to configure a new WPA3-OWE SSID in Central but is not working as expected.

What would be the correct action to fix the issue?

Options:

- A- Change the SSID to WPA3-Enterprise (CNSA).
- B- Change the SSID to WPA3-Personal.
- C- Change the SSID to WPA3-Enhanced Open.
- D- Change the SSID to WPA3-Enterprise (CCM).

Answer:

C

Explanation:

The correct action to fix the issue is C. Change the SSID to WPA3-Enhanced Open.

WPA3-OWE is not a valid SSID type in Central. OWE stands for Opportunistic Wireless Encryption, and it is a feature that provides encryption for open networks without requiring authentication. OWE is also known as Enhanced Open, and it is one of the options for WPA3 SSIDs in Central¹.

According to the Aruba document [Configuring WLAN Settings for an SSID Profile](#), one of the steps to configure a WPA3 SSID is:

Select the Security Level from the drop-down list. The following options are available:

WPA3-Personal: This option uses Simultaneous Authentication of Equals (SAE) to provide stronger password-based authentication and key exchange than WPA2-Personal.

WPA3-Enterprise: This option uses 192-bit cryptographic strength for authentication and encryption, as defined by the Commercial National Security Algorithm (CNSA) suite.

WPA3-Enterprise (CCM): This option uses 128-bit cryptographic strength for authentication and encryption, as defined by the Counter with CBC-MAC (CCM) mode.

WPA3-Enhanced Open: This option uses Opportunistic Wireless Encryption (OWE) to provide encryption for open networks without requiring authentication.

The other options are incorrect because:

A) WPA3-Enterprise (CNSA) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company's use case.

B) WPA3-Personal is a valid SSID type, but it requires a passphrase to join the network, which may not be suitable for the company's use case.

D) WPA3-Enterprise (CCM) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company's use case.



To Get Premium Files for HPE7-A01 Visit

<https://www.p2pexams.com/products/hpe7-a01>

For More Free Questions Visit

<https://www.p2pexams.com/hp/pdf/hpe7-a01>

20%
DISCOUNT

P2P
exams