

HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam



NEW QUESTION 1

How is Multicast Transmission Optimization implemented in an HPE Aruba wireless network?

- A. "The optimal rate for sending multicast frames is based on the highest broadcast rate across all associated clients
- B. When this option is enabled the minimum default rate for multicast traffic is set to 12 Mbps for 5 GHz
- C. The optimal rate for sending multicast frames is based on the lowest broadcast rate across all associated clients.
- D. The optimal rate for sending multicast frames is based on the lowest unicast rate across all associated clients.

Answer: D

Explanation:

multicast transmission optimization is a feature that allows the IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients¹. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5.0 GHz is 6 Mbps. This option is disabled by default¹.

NEW QUESTION 2

What is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches?

- A. Switch authentication and local forwarding of the voice traffic
- B. Switch authentication and user-based tunneling of the voice traffic.
- C. Central authentication and port-based tunneling of the voice traffic.
- D. Controller authentication and port-based tunneling of all traffic

Answer: A

Explanation:

This is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches. Dynamic segmentation is a feature that allows AOS-CX switches to tunnel user traffic to a controller or another switch based on user roles and policies. For voice traffic, it is recommended to use switch authentication and local forwarding, which means the voice devices are authenticated by the switch and their traffic is forwarded locally without tunneling. This reduces latency and jitter for voice traffic and improves voice quality. The other options are incorrect because they either use central authentication or tunneling, which are not optimal for voice traffic. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html>
https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

NEW QUESTION 3

Your customer is having issues with Wi-Fi 6 clients staying connected to poor-performing APs when a higher throughput APs are closer. Which technology should you implement?

- A. Clearpass
- B. ClientMatch
- C. Airmatch
- D. ARM

Answer: B

Explanation:

Wi-Fi 6 is an industry certification for products that support the new wireless standard 802.11ax, also known as ??high-efficiency wireless??. Wi-Fi 6 offers increased capacities, improved resource utilization and higher throughput speeds than previous standards.

Option B: ClientMatch

This is because option B shows how to use ClientMatch to optimize the wireless performance of Wi-Fi 6 clients on a UniFi network. ClientMatch is a feature that uses machine learning to analyze the traffic patterns of each client and assign them to the best available AP based on their location, device type, and network conditions².

Therefore, option B is the best technology to implement for your customer??s issue.

1: <https://help.ui.com/hc/en-us/articles/221029967-UniFi-Network-Optimizing-Wireless-Connectivity> 2: <https://help.ui.com/hc/en-us/articles/360012947634-UniFi-Network-Optimizing-Wireless-Speeds>

NEW QUESTION 4

A customer wants to provide wired security as close to the source as possible The wired security must meet the following requirements:

- allow ping from the IT management VLAN to the user VLAN
- deny ping sourcing from the user VLAN to the IT management VLAN

The customer is using Aruba CX 6300s

What is the correct way to implement these requirements?

- A. Apply an outbound ACL on the user VLAN allowing temp echo-reply traffic toward the IT management VLAN
- B. Apply an inbound ACL on the user VLAN allowing icmp echo-reply traffic toward the IT management VLAN
- C. Apply an inbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN
- D. Apply an outbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN

Answer: C

Explanation:

An inbound ACL is applied to traffic entering a port or VLAN. An outbound ACL is applied to traffic leaving a port or VLAN⁴. To deny ping sourcing from the user VLAN to the IT management VLAN, an inbound ACL on the user VLAN should be used to filter icmp echo traffic toward the IT management VLAN. Icmp echo-reply traffic is not needed to be allowed because it is already permitted by default⁵. References: 4

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html 5

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-0C3A9D0F-6E5B-4E1A-AF3C-8D8B2F9C1A7B.html

NEW QUESTION 5

A client is connecting to 802.1X SSID that has been configured in tunnel mode with the default AP-group settings. After receiving Access-Accept from the RADIUS server, the Aruba Gateway will send Access-Accept to the AP through which tunnel?

- A. IPsec tunnel
- B. Split tunnel
- C. GRE tunnel
- D. PAR tunnel

Answer: C

Explanation:

According to the Aruba Documentation Portal¹, 802.1X is a standard for port- based network access control that uses a RADIUS server to authenticate and authorize wireless clients. 802.1X can be configured in different modes, such as bridge mode, tunnel mode, or split tunnel mode.

Option C: GRE tunnel

This is because option C shows how to configure an SSID in tunnel mode with the default AP-group settings on an Aruba switch. In tunnel mode, all client traffic from the access points is tunneled back to the controller and the controller would in turn put the client traffic onto the network². The GRE protocol is used to encapsulate and decapsulate the traffic between the access points and the controller³.

Therefore, option C is correct.

1: <https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html> 2:

<https://community.arubanetworks.com/discussion/bridge-and-tunnel-mode> 3: <https://www.twingate.com/blog/ipsec-tunnel-mode>

NEW QUESTION 6

A customer has a site with 200 AP-515 access points 75AP-565 access points installed.

The customer is rolling out new mobile phones with Wi-Fi-calling. 802.1X is in use for authentication

What should be enabled to ensure the best roaming experience?

- A. 802.1X
- B. 802. 11r
- C. 802.11W
- D. 802 .11h

Answer: A

Explanation:

<https://www.howtogeek.com/794724/what-is-wi-fi-calling/> 2:

<https://www.networkcomputing.com/networking/your-network-optimized-wifi-calling> 3: https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm

Wi-Fi calling is a feature that allows you to make or receive voice calls over Wi-Fi instead of cellular network. Wi-Fi calling can provide better voice quality and reliability in areas with poor or no cellular coverage.

NEW QUESTION 7

Which feature allows the device to remain operational when a remote link failure occurs between a Gateway cluster and a RADIUS server that is either in the cloud or a datacenter?

- A. MAC caching
- B. MAC Authentication
- C. Authentication survivability
- D. Opportunistic key caching

Answer: C

Explanation:

Authentication survivability is a feature that allows the device to remain operational when a remote link failure occurs between a Gateway cluster and a RADIUS server that is either in the cloud or a datacenter. Authentication survivability enables the Gateway cluster to cache successful authentication requests from the RADIUS server and use them to authenticate clients when the RADIUS server is unreachable. Authentication survivability also allows clients to use MAC caching or MAC authentication bypass (MAB) methods to access the network when the RADIUS server is down. References:

https://www.arubanetworks.com/assets/tg/TG_AuthSurvivability.pdf

NEW QUESTION 8

In an ArubaOS 10 architecture using an AP and a gateway, what happens when a client attempts to join the network and the WLAN is configured with OWE?

- A. Authentication information is not exchanged
- B. The Gateway will not respond.
- C. No encryption is applied.
- D. RADIUS protocol is utilized.

Answer: A

Explanation:

This is the correct statement about what happens when a client attempts to join the network and the WLAN is configured with OWE (Opportunistic Wireless Encryption). OWE is a standard that provides encryption for open networks without requiring any authentication or credentials from the client or the network. OWE uses a Diffie-Hellman key exchange mechanism to establish a secure session between the client and the AP without exchanging any authentication information. The other options are incorrect because they either describe scenarios that require authentication or encryption methods that are not used by OWE. References:

https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

NEW QUESTION 9

What is used to retrieve data stored in a Management Information Base (MIS)?

- A. SNMPv3

- B. DSCP
- C. TLV
- D. CDP

Answer: A

Explanation:

The correct answer is A. SNMPv3.

SNMPv3 is a protocol that is used to retrieve data stored in a Management Information Base (MIB), which is a database of managed objects in a network.

SNMPv3 provides security and access control features that are not available in earlier versions of SNMP. SNMPv3 can also use encryption to protect the data from unauthorized access or modification.

According to the Aruba Certified Professional – Campus Access document¹, one of the skills that this certification validates is:

? Implement and Analyze the output from common network monitoring tools

The document also mentions that the candidate should have a distinguished understanding of different protocols across vendors, which implies that they should be familiar with SNMPv3 and how it can be used to access MIB data.

NEW QUESTION 10

Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements. After the configuration was complete, it was noted that a user assigned with the auditors role did not have the appropriate level of access on the switch.

The user was not allowed to perform firmware upgrades and a privilege level of 15 was not assigned to their role. Which default management role should have been assigned for the user?

- A. sysadmin
- B. sysops
- C. administrators
- D. config

Answer: B

Explanation:

The correct answer is B. sysops.

The sysops user role is a predefined role that allows users to perform system operations on the switch, such as backup, restore, upgrade, or reboot. The sysops user role also has access to the PUT and POST methods for REST API, which can be used to modify the switch configuration. The sysops user role has a privilege level of 15, which is the highest level of access on the switch¹.

The other options are incorrect because:

? A. sysadmin: The sysadmin user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The sysadmin user role does not have access to the REST API methods, and cannot perform firmware upgrades¹.

? C. administrators: The administrators user role is a predefined role that has full access to all switch configuration information and all REST API methods. This role is more than what the Director of Security requires¹.

? D. config: The config user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The config user role does not have access to the REST API methods, and cannot perform firmware upgrades¹.

NEW QUESTION 10

Your customer is having connectivity issues with a newly-deployed Microbranch group The access points in this group are online in Aruba Central, but no VPN tunnels are forming.

What is the most likely cause of this issue?

- A. There is a time difference between the AP and the gateways The gateways should have NTP added
- B. The SSL certificate on the gateway used to encrypt the connection has not been added to the APs trust list
- C. There may be a firewall blocking GRE tunneling between the AP and the gateway
- D. The gateway group is running in automatic cluster mode and should be in manual cluster mode

Answer: C

Explanation:

This is the most likely cause of the issue where the access points in a Microbranch group are online in Aruba Central, but no VPN tunnels are forming. A

Microbranch group is a group that contains both APs and Gateways and allows them to form VPN tunnels for secure communication. The VPN tunnels use GRE (Generic Routing Encapsulation) as the encapsulation protocol and IPSec as the encryption protocol. If there is a firewall blocking GRE traffic between the AP and the gateway, the VPN tunnels cannot be established. The other options are incorrect because they either do not affect the VPN tunnel formation or do not apply to a Microbranch group. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/gateways/microbranch.htm

https://www.arubanetworks.com/assets/tg/TB_ArubaGateway.pdf

NEW QUESTION 14

You are doing tests in your lab and with the following equipment specifications

- AP1 has a radio that generates a 10 dBm signal
- AP2 has a radio that generates a 11 dBm signal
- AP1 has an antenna with a gain of 9 dBi
- AP2 has an antenna with a gain of 12 dBi.
- The antenna cable for AP1 has a 2 dB loss
- The antenna cable for AP2 has a 3 dB loss

What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for APT?

- A. 26 dBm
- B. 30 dBm
- C. 17 dBm
- D. -12 dBm

Answer: C

Explanation:

The calculated Equivalent Isotropic Radiated Power (EIRP) for AP1 is 17 dBm.

EIRP is the measured radiated power of an antenna in a specific direction. It is equal to the input power to the antenna multiplied by the gain of the antenna. It can also take into account the losses in transmission line, connectors, and other components. The formula for EIRP is:

$$\text{EIRP} = P + G - L$$

where P is the output power of the radio, G is the gain of the antenna, and L is the loss of the cable and connectors.

For AP1, we have:

$$P = 10 \text{ dBm} \quad G = 9 \text{ dBi} \quad L = 2 \text{ dB}$$

Therefore,

$$\text{EIRP} = 10 + 9 - 2 \quad \text{EIRP} = 17 \text{ dBm}$$

NEW QUESTION 15

Describe the difference between Class of Service (CoS) and Differentiated Services Code Point (DSCP).

- A. CoS has much finer granularity than DSCP
- B. CoS is only contained in VLAN Tag fields DSCP is in the IP Header and preserved throughout the IP packet flow
- C. They are similar and can be used interchangeably.
- D. CoS is only used to determine CLASS of traffic DSCP is only used to differentiate between different Classes.

Answer: B

Explanation:

CoS and DSCP are both methods of marking packets for quality of service (QoS) purposes. QoS is a mechanism that allows network devices to prioritize and differentiate traffic based on certain criteria, such as application type, source, destination, etc. CoS stands for Class of Service and is a 3-bit field in the 802.1Q VLAN tag header. CoS can only be used on Ethernet frames that have a VLAN tag, and it can only be preserved within a single VLAN domain. DSCP stands for Differentiated Services Code Point and is a 6-bit field in the IP header. DSCP can be used on any IP packet, regardless of the underlying layer 2 technology, and it can be preserved throughout the IP packet flow, unless it is modified by intermediate devices. References: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mt-book/qos-overview.html> <https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html> <https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html>

NEW QUESTION 20

A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working to a remote site connected via layer-3 All legacy devices are connected to a dedicated Aruba CX 6200 switch at each site.

What technology on the Aruba CX 6200 could be used to meet this requirement?

- A. Inclusive Multicast Ethernet Tag (IMET)
- B. Ethernet over IP (EoIP)
- C. Generic Routing Encapsulation (GRE)
- D. Static VXLAN

Answer: A

Explanation:

VXLAN is a technology that can be used to meet the requirement of using a legacy application that communicates at layer-2 across a layer-3 network. Static VXLAN is a feature that allows the creation of layer-2 overlay networks over a layer-3 underlay network using VXLAN tunnels. Static VXLAN does not require any control plane protocol or VTEP discovery mechanism, and can be configured manually on the Aruba CX 6200 switches. The other options are incorrect because they either do not support layer-2 communication over layer-3 network or are not supported by Aruba CX 6200 switches. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html>

NEW QUESTION 23

A network engineer recently identified that a wired device connected to a CX Switch is misbehaving on the network To address this issue, a new ClearPass policy has been put in place to prevent this device from connecting to the network again.

Which steps need to be implemented to allow ClearPass to perform a CoA and change the access for this wired device? (Select two.)

- A. Confirm that NTP is configured on the switch and ClearPass
- B. Configure dynamic authorization on the switch.
- C. Bounce the switchport
- D. Use Dynamic Segmentation.
- E. Configure dynamic authorization on the switchport

Answer: BC

Explanation:

CoA (Change of Authorization) is a feature that allows ClearPass to dynamically change the authorization and access privileges of a device after it has been authenticated¹. CoA uses RADIUS messages to communicate with the network device and instruct it to perform an action, such as reauthenticating the device, applying a new VLAN or user role, or disconnecting the device².

To enable CoA on a CX switch, the network engineer needs to configure dynamic authorization on the switch, which is a global command that allows the switch to accept RADIUS messages from ClearPass and execute the requested actions³. The network engineer also needs to specify the IP address and shared secret of ClearPass as a dynamic authorization client on the switch³.

To trigger CoA for a specific wired device, the network engineer needs to bounce the switchport, which is an action that temporarily disables and re-enables the port where the device is connected. This forces the device to reauthenticate and receive the new policy from ClearPass. Bouncing the switchport can be done manually by using the interface shutdown and no shutdown commands, or automatically by using ClearPass as a CoA server and sending a RADIUS message with the Port-Bounce-Host AVP (Attribute-Value Pair).

NEW QUESTION 28

DRAG DROP

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Client Insights matches with Built in , AI powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML based classification models to eliminate network bling spots

Client Insights is a solution component of NetConductor that provides built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML- based classification models to eliminate network blind spots. Client Insights uses machine learning to automatically detect, identify, and classify devices on the network, such as IoT devices, BYOD devices, or rogue devices. Client Insights also provides behavioral analytics and anomaly detection to monitor device performance and security posture. Client Insights helps network administrators gain visibility into the device landscape, enforce granular access policies, and troubleshoot issues faster. References: <https://www.arubanetworks.com/products/network-management- operations/central/netconductor/>

https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

Cloud Auth matches with Enables fictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores

Cloud Auth is a solution component of NetConductor that enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores. Cloud Auth is a cloud-native network access control (NAC) solution that is delivered via Aruba Central. Cloud Auth allows network administrators to define user and device groups, assign roles and policies, and enforce access control across wired and wireless networks. Cloud Auth supports MAC authentication for devices that do not support 802.1X, as well as integrations with cloud identity providers such as Azure AD, Google Workspace, Okta, etc. References: <https://www.arubanetworks.com/products/network-management- operations/central/netconductor/>

https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

The Fabric Wizard matches with 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

The Fabric Wizard is a solution component of NetConductor that 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. The Fabric Wizard is a tool that allows network administrators to design, deploy, and manage overlay networks using VXLAN and EVPN protocols. The Fabric Wizard provides a graphical representation of the network topology, devices, and links, and allows users to drag and drop virtual components such as VRFs, VLANs, and subnets. The Fabric Wizard also generates the configuration commands for each device based on the user input and pushes them to the switches and gateways via Aruba Central. References:

<https://www.arubanetworks.com/products/network-management- operations/central/netconductor/>

https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

Policy Manager matches with Defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network
 Policy Manager is a solution component of NetConductor that defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network. Policy Manager is a tool that allows network administrators to create and manage network policies based on user and device identities, roles, and contexts. Policy Manager uses Group Policy Identifier (GPID) to carry policy information in traffic for in-line enforcement. Policy Manager also integrates with Cloud Auth, ClearPass, or third-party solutions to provide flexible network access control. References:

<https://www.arubanetworks.com/products/network-management- operations/central/netconductor/>

https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

NEW QUESTION 30

What is a primary benefit of BSS coloring?

- A. BSS color tags improve performance by allowing APS on the same channel to be farther apart
- B. BSS color tags improve security by identifying rogue APS and tagging them as threats.
- C. BSS color tags are applied on the wireless controllers and can reduce the threshold for interference_
- D. BSS color tags are applied to WI-Fi channels and can reduce the threshold tor interference

Answer: D

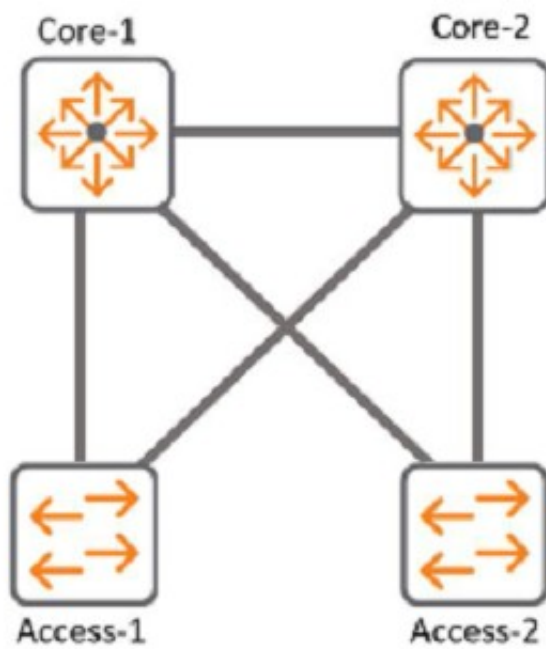
Explanation:

The primary benefit of BSS coloring is D. BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference.

BSS coloring is a mechanism that allows Wi-Fi 6 devices to mark each frame with a color code that identifies the BSS (Basic Service Set) it belongs to. This helps differentiate between frames from different BSSs that share the same channel and avoid unnecessary collisions and backoffs. BSS coloring also introduces an adaptive threshold for interference, which means that Wi-Fi 6 devices can adjust the signal strength value that determines whether a channel is busy or not based on the current network environment. This allows for more efficient use of spectrum and higher throughput in dense scenarios¹².

NEW QUESTION 32

Refer to Exhibit:



With Access-1, What needs to be identically configured With MSTP to load-balance VLANS?

- A. Spanning-tree bpdu-guard setting
- B. Spanning-tree instance vlan mappjng
- C. spanning-tree Cist mapping
- D. Spanning-tree root-guard setting

Answer: B

Explanation:

The correct answer is B. Spanning-tree instance VLAN mapping.

To load-balance VLANs with MSTP, you need to configure the same VLAN-to-instance mapping on all switches in the same MST region. This means that you need to assign different VLANs to different MST instances, and then adjust the spanning tree parameters (such as priority, cost, or port role) for each instance to achieve the desired load balancing. For example, you can make one switch the root for instance 1 and another switch the root for instance 2, and then map half of the VLANs to instance 1 and the other half to instance 2.

According to the Cisco document Understand the Multiple Spanning Tree Protocol (802.1s), one of the steps to configure MST is:

? Split your set of VLANs into more instances and configure different MST settings for each of these instances. In order to easily achieve this, elect Bridge D1 to be the root for VLANs 501 through 1000, and Bridge D2 to be the root for VLANs 1 through 500. These statements are true for this configuration:

Switch D1(config)#spanning-tree mst configuration Switch D1(config-mst)#instance 1 vlan 501-1000 Switch D1(config-mst)#exit

Switch D1(config)#spanning-tree mst 1 priority 0

Switch D2(config)#spanning-tree mst configuration Switch D2(config-mst)#instance 2 vlan 1-500 Switch D2(config-mst)#exit

Switch D2(config)#spanning-tree mst 2 priority 0

The above commands create two MST instances, 1 and 2, and map VLANs 501-1000 to instance 1 and VLANs 1-500 to instance 2. Then, they make switch D1 the root for instance 1 and switch D2 the root for instance 2.

The other options are incorrect because:

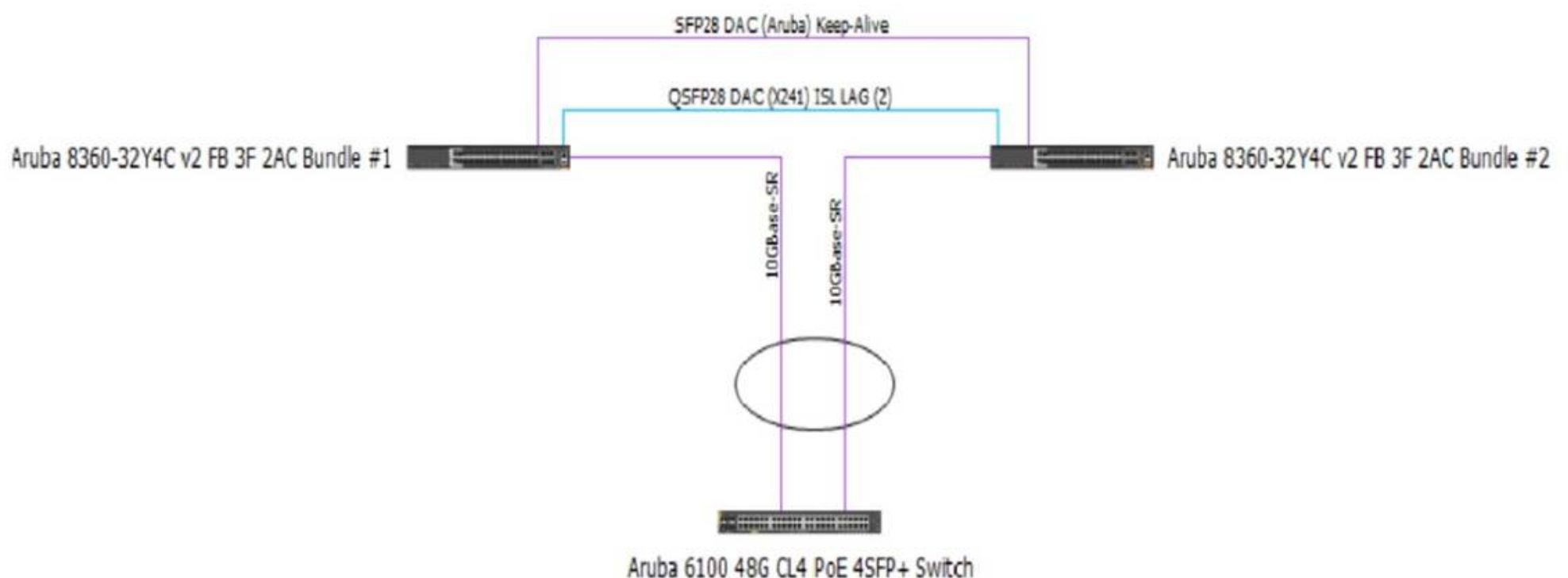
? A. Spanning-tree bpdu-guard setting is a security feature that disables a port if it receives a BPDU from an unauthorized device. It does not affect load balancing with MSTP.

? C. Spanning-tree CIST mapping is not a valid command. CIST stands for Common and Internal Spanning Tree, which is the spanning tree instance that runs within an MST region and interacts with other regions or non-MST switches.

? D. Spanning-tree root-guard setting is another security feature that prevents a port from becoming a root port if it receives superior BPDUs from another switch. It does not affect load balancing with MSTP.

NEW QUESTION 34

Review the exhibit.



You are troubleshooting an issue with a 10.102.39.0/24 subnet which is also VLAN 1000 used for wireless clients on a pair of Aruba CX 8360 switches. The subnet SVI is configured on the 8360 pair, and the DHCP server is a Microsoft Windows Server 2022 Standard with an IP address of 10.200.1.100. The 10.102.250.0/24 subnet is used for switch management.

A large number of DHCP requests are failing. You are observing sporadic DHCP behavior across clients attached to the CX 6100 switch.

Which action may help fix the issue?

A)

Enter the following commands on the VSX primary switch:

```
vsx
vsx-sync dhcp-relay
exit
```

B)

Enter the following commands on the VSX secondary switch:

```
vlan 1000
ip relay-address 10.200.1.100
exit
```

C)

Add an SVI in the 10.102.39.0/24 subnet on the Aruba CX 6100 switch that the APs are connected to.

D)

Enter the following commands on the Aruba CX 6100 switch:

```
interface vlan 1000
ip helper-address 10.200.1.100
exit
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Option C is the only action that configures the DHCP relay on the SVI of VLAN 1000 on the CX 8360 switches. DHCP relay is a feature that allows a switch to forward DHCP requests from clients in one subnet to a DHCP server in another subnet. DHCP relay is required when the DHCP server and the clients are not in the same broadcast domain1.

Option C uses the following commands:

? interface vlan 1000: This command enters the interface configuration mode for the SVI of VLAN 1000, which has an IP address of 10.102.39.1/24 and is used for wireless clients.

? ip helper-address vrf default 10.200.1.100: This command configures the IP address of the DHCP server as a helper address for the SVI, which means that the switch will forward DHCP requests from clients on VLAN 1000 to this address. The vrf default parameter indicates that the SVI and the DHCP server are in the same VRF.

NEW QUESTION 37

A customer is concerned about me unprotected traffic between an AOS-CX switch and a gateway, running on AOSStO. What is a feasible option to protect this traffic?

- A. Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway
- B. Implement an MD5 HMAC function to protect PAPI between the AOS-CX switches and the gateway
- C. Implement a GRE tunnel to protect PAPI between the AOS-CX switches and the gateway
- D. no action is needed, an RSA certificate already encrypts the traffic

Answer: A

Explanation:

According to the Aruba Documentation Portal1, PAPI (Port Aggregation Protocol) is a protocol that allows multiple physical ports to be aggregated into a single logical port for increased bandwidth and performance. PAPI can be used between AOS-CX switches and gateways, or between AOS-CX switches and other devices.

Option A: Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway

This is because option A shows how to implement an IPSec tunnel between two devices using the interface command and the ipsec command. An IPSec tunnel can provide encryption and authentication for PAPI traffic between two devices, such as an AOS-CX switch and a gateway2.

Therefore, option A is a feasible option to protect this traffic.

I hope this helps you. If you need more information, please let me know. 1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7727/Content/Chp_prev_traf_loss/Act_gtw_act_fwd/act-gat-ove-vsx-10.htm 2: <https://community.arubanetworks.com/blogviewer?blogkey=989fc43a-e0df-42db-9c0b-f96d6565a1fa>

NEW QUESTION 41

You are working on a network where the customer has a dedicated router with redundant Internet connections Tor outbound high-importance real-time audio streams from their datacenter All of this traffic.

- originates from a single subnet
- uses a unique range of UDP ports
- is required to be routed to the dedicated router

All other traffic should route normally The SVI for the subnet containing the servers originating the traffic is located on the core routing switch in the datacenter What should be configured?

- A. Configure a new OSPF area including both the core routing switch and the dedicated router
- B. Configure a BGP link between the core routing switch and the dedicated router and route filtering.
- C. Configure Policy Based Routing (PBR) on the core routing switch for the VRF with the servers?? SVI
- D. Configure a dedicated VRF on the core routing switch and make the dedicated router the default route.

Answer: C

Explanation:

The reason is that PBR allows you to route packets based on policies that match certain criteria, such as source or destination IP addresses, ports, protocols, etc.

PBR can also be used to set metrics, next-hop addresses, or tag traffic for different routes.

NEW QUESTION 42

With the Aruba CX 6100 48G switch with uplinks of 1/1/47 and 1/1/48. how do you automate the process of resuming the port operational state once a loop on a client port is cleared?

- A. Configure int 1/1/1-1/1/52 loop-protect disable timer.
- B. Configure global loop-protect disable timer.
- C. Configure int 1/1/1-1/1/46 loop-protect re-enable-timer.
- D. Configure global loop-protect re-enable-timer.

Answer: C

Explanation:

Loop protection is a feature that detects and prevents loops in layer 2 networks. Loop protection can be enabled on ports, LAGs, or VLANs. When loop protection is enabled, the switch sends periodic loop protection messages on the interface and expects to receive them back. If a loop protection message is received back on the same interface, it indicates a loop and the switch takes an action to disable the interface or block traffic on it3. The loop-protect re-enable-timer command is used to configure the length of time the switch waits before re-enabling an interface that was disabled due to loop detection. The default value is 0, which means that the interface remains disabled until manually re-enabled3. To automate the process of resuming the port operational state once a loop on a client port is cleared, the loop-protect re-enable-timer command can be used with a non-zero value on the interface range that includes the client ports3. Therefore, answer C is correct. References: 1: Aruba Campus Access documents and learning resources 3: Configuring loop protection - Aruba

NEW QUESTION 46

you are implementing ClearPass Policy Manager with EAP-TLS for authenticating all corporate-owned devices.
What are two possible solutions to the problem of deploying client certificates to corporate MacBook that are joined to a Windows domain? (Select two.)

- A. ClearPass OnBoard
- B. Windows Server PKI and a GPO
- C. Apple Configurator and a GPO
- D. ClearPass OnGuard
- E. Mobile Device Manager

Answer: AB

Explanation:

The reason is that ClearPass OnBoard is a tool that allows you to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate. This certificate can be obtained from Apple or from a third-party PKI provider.
Apple Configurator is a tool that allows you to configure and deploy Mac computers using a GPO. This tool can also be used to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate.

NEW QUESTION 48

DRAG DROP
Match the topics with the underlying technologies (Options may be used more than once or not at all.)

EVPN-VXLAN

User Based Tunneling (UBT)

Answer Area

Centralized Overlay

Distributed Overlay

Encapsulated in UDP

Generic Routing Encapsulation (GRE)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

EVPN-VXLAN

User Based Tunneling (UBT)

Answer Area

EVPN-VXLAN

Centralized Overlay

EVPN-VXLAN

Distributed Overlay

EVPN-VXLAN

Encapsulated in UDP

User Based Tunneling (UBT)

Generic Routing Encapsulation (GRE)

NEW QUESTION 50

Your customer has asked you to assign a switch management role for a new user The customer requires the user role to only have Web UI access to the System > Log page and only have access to the GET method for REST API for the /logs/event resource
Which default AOS-CX user role meets these requirements?

- A. administrators
- B. auditors
- C. sysops
- D. operators

Answer: A

Explanation:

The auditors role is the default AOS-CX user role that meets the requirements of having Web UI access to the System > Log page and having access to the GET method for REST API for the /logs/event resource. The auditors role has a level of 1 and allows read-only access to most commands except those related to security or passwords. It also allows access to the Web UI and REST API with limited permissions. The other options are incorrect because they either have higher levels of access or do not allow access to the Web UI or REST API. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch01.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch04.html>

NEW QUESTION 52

DRAG DROP

List the WPA 4-Way Handshake functions in the correct order.

Function	Order
Distributes an encrypted GTK to the client	
Exchanges messages for generating PTK	
Proves knowledge of the PMK	
Sets first initialization vector (IV)	

>

<

⬆

⬇

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- ? Proves knowledge of the PMK
- ? Exchanges messages for generating PTK
- ? Distributes an encrypted GTK to the client
- ? Sets first initialization vector (IV)

NEW QUESTION 56

You are deploying a bonded 40 MHz wide channel What is the difference in the noise floor perceived by a client using this bonded channel as compared to an unbonded 20MHz wide channel?

- A. 2dB
- B. 3dB
- C. 8dB
- D. 4dB

Answer: B

Explanation:

The difference in the noise floor perceived by a client using a bonded 40 MHz wide channel as compared to an unbonded 20 MHz wide channel is 3 dB. The noise floor is the level of background noise in a given frequency band. When two adjacent channels are bonded, the noise floor increases by 3 dB because the bandwidth is doubled and more noise is captured. The other options are incorrect because they do not reflect the correct relationship between bandwidth and noise floor. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/rf-fundamentals.htm https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/channel-bonding.htm

NEW QUESTION 59

Which feature supported by SNMPv3 provides an advantage over SNMPv2c?

- A. Transport mapping
- B. Community strings
- C. GetBulk
- D. Encryption

Answer: D

Explanation:

Encryption is a feature supported by SNMPv3 that provides an advantage over SNMPv2c. Encryption protects the confidentiality and integrity of SNMP messages by encrypting them with a secret key. SNMPv2c does not support encryption and relies on community strings for authentication and authorization, which are transmitted in clear text and can be easily intercepted or spoofed. Transport mapping, community strings, and GetBulk are features that are common to both SNMPv2c and SNMPv3. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmp.htm https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmpv3.htm

NEW QUESTION 64

You need to create a keepalive network between two Aruba CX 8325 switches for VSX configuration How should you establish the keepalive connection?

- A. SVI, VLAN trunk allowed all on ISL in default VRF
- B. routed port in custom VRF
- C. loopback 0 and OSPF area 0 in default VRF
- D. SVI, VLAN trunk allowed all on ISL in custom VRF

Answer: B

Explanation:

To establish a keepalive connection between two Aruba CX 8325 switches for VSX configuration, you need to use a routed port in custom VRF. A routed port is a physical port that acts as a layer 3 interface and does not belong to any VLAN. A custom VRF is a virtual routing and forwarding instance that provides logical separation of routing tables. By using a routed port in custom VRF, you can isolate the keepalive traffic from other traffic and prevent routing loops or conflicts. The other options are incorrect because they either do not use a routed port or do not use a custom VRF. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html>

NEW QUESTION 66

Which statements regarding Aruba NAE agents are true? (Select two)

- A. A single NAE script can be used by multiple NAE agents
- B. NAE agents are active at all times
- C. NAE agents will never consume more than 10% of switch processor resources
- D. NAE scripts must be reviewed and signed by Aruba before being used
- E. A single NAE agent can be used by multiple NAE scripts.

Answer: AC

Explanation:

The statements that are true regarding Aruba NAE agents are A and C.

* A. A single NAE script can be used by multiple NAE agents. This means that you can create different instances of the same script with different parameters or settings. For example, you can use the same script to monitor different VLANs or interfaces on the switch1.

* C. NAE agents will never consume more than 10% of switch processor resources. This is a built-in safeguard that prevents the agents from affecting the switch performance or stability. If an agent exceeds the 10% limit, it will be automatically disabled and an alert will be generated2.

The other options are incorrect because:

? B. NAE agents are not active at all times. They can be enabled or disabled by the user, either manually or based on a schedule. They can also be disabled automatically if they encounter an error or exceed the resource limit1.

? D. NAE scripts do not need to be reviewed and signed by Aruba before being used. You can create your own custom scripts using Python and upload them to the switch or Aruba Central. You can also use the scripts provided by Aruba or other sources, as long as they are compatible with the switch firmware version1.

? E. A single NAE agent cannot be used by multiple NAE scripts. An agent is an instance of a script that runs on the switch. Each agent can only run one script at a time1.

NEW QUESTION 69

With Aruba CX 6300. how do you configure ip address 10 10 10 1 for the interface in default state for interface 1/1/1?

- A. int 1/1/1. switching, ip address 10 10 10 1/24
- B. int 1/1/1. no switching, ip address 10 10 10.1/24
- C. int 1/1/1. ip address 10.10.10.1/24
- D. int 1/1/1. routing, ip address 10.10.10 1/24

Answer: B

Explanation:

To configure an IP address for an interface in default state for interface 1/1/1 on Aruba CX 6300 switch, you need to disable switching on the interface first with the command no switching. Then you can assign an IP address with the command ip address. The other options are incorrect because they either do not disable switching or use invalid keywords such as switching or routing. References: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch01.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html

NEW QUESTION 70

What does the 802.3bz standard describe?

- A. 2.5Gb and 5Gb Ethernet ports
- B. 60 W and 90W PoE
- C. AP directed roaming between APs
- D. 60 GHz P2P Wi-Fi

Answer: A

Explanation:

802.3bz is a standard for Ethernet over twisted pair at speeds of 2.5 and 5 Gbit/s. These use the same cabling as the ubiquitous Gigabit Ethernet, yet offer higher speeds. The resulting standards are named 2.5GBASE-T and 5GBASE-T.

Option A: 2.5Gb and 5Gb Ethernet ports

This is because option A shows how to identify the speed of an Ethernet port based on its name and the standard it supports. A port that supports 2.5GBASE-T or 5GBASE-T is a multi-gigabit port that can operate at speeds of up to 2.5 Gbit/s or 5 Gbit/s over twisted pair cables23.

Therefore, option A is correct.

1: https://en.wikipedia.org/wiki/2.5GBASE-T_and_5GBASE-T 2: <https://kb.netgear.com/000049004/What-is-Multi-Gigabit-Ethernet-and-how-can-I-benefit-from-using-NETGEAR-Multi-Gigabit-Ethernet-Switches-in-my-network> 3: <https://arstechnica.com/gadgets/2016/09/5gbps-ethernet-standard-details-8023bz/>

NEW QUESTION 74

A customer has a large number of food-producing machines

- All machines are connected via Aruba CX6200 switches in VLANs 100.110. and 120
- Several external technicians are maintaining this special equipment

What are the correct commands to ensure that no rogue DHCP server will impact the network?

A)

```
dhcp-snooping enable
no dhcp-snooping option 82
dhcp-snooping vlan 100-120
vlan 100
    name cornflakes
vlan 110
    name cornmill
vlan 120
    name packaging
```

```
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcp-snooping trust
```

B)

```
dhcp snooping enable
no dhcp-snooping option 82
vlan 100
    name cornflakes
    dhcp-snooping
vlan 110
    name cornmill
    dhcp-snooping
vlan 120
    name packaging
    dhcp-snooping
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcp snooping trust
```

C)

```
dhcpv4-snooping all vlans
no dhcpv4-snooping option 82
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcpv4-snooping trust
```

D)

```
dhcpv4-snooping
no dhcpv4-snooping option 82
vlan 100
    name cornflakes
    dhcpv4-snooping
vlan 110
    name cornmill
    dhcpv4-snooping
vlan 120
    name packaging
    dhcpv4-snooping
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcpv4-snooping trust
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

configures DHCP snooping on the switch and enables it for VLANs 100, 110, and 120. It also specifies the IP address of the authorized DHCP server and sets the ports connected to the server as trusted. This prevents any unauthorized DHCP server from providing invalid configuration data to the clients on those VLANs. Option B also enables DHCP option-82, which adds information about the switch port and VLAN to the DHCP packets, allowing for more granular control and logging of DHCP transactions.

NEW QUESTION 78

You are configuring an SVI on an Aruba CX switch that needs to have the following characteristics:

- VLANID = 25
- IPv4 address 10.105.43.1 with mask 255.255.255.0
- IPv6 address fd00:5708::f02d:4df6 with a 64 bit prefix length
- member of VRF eng
- VRF eng and VLAN 25 have not yet been created

Which command lists will satisfy the requirements with the least number of commands?

A)

```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43.1 255.255.255.0
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

B)

```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
```

C)

```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipov6 address fd00:5708::f02d:4df6/64
```

D)

```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

The other options either use more commands or do not create the VRF or the VLAN.

Option C uses the following commands:

? vrf eng: This command creates a VRF named eng and enters the VRF configuration mode1.

? vlan 25: This command creates a VLAN with ID 25 and enters the VLAN configuration mode2.

? interface vlan 25: This command creates an SVI on VLAN 25 and enters the interface configuration mode3.

? ip address 10.105.43.1/24 ipv6 address fd00:5780::102d:4df6/64 vrf attach eng: This command assigns an IPv4 address of 10.105.43.1 with a subnet mask of 255.255.255.0 and an IPv6 address of fd00:5780::102d:4df6 with a prefix length of 64 to the SVI, and attaches it to the VRF eng.

NEW QUESTION 82

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

HPE7-A01 Practice Exam Features:

- * HPE7-A01 Questions and Answers Updated Frequently
- * HPE7-A01 Practice Questions Verified by Expert Senior Certified Staff
- * HPE7-A01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * HPE7-A01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The HPE7-A01 Practice Test Here](#)