HPE7-A01 Q&As

Aruba Certified Campus Access Professional

Pass HP HPE7-A01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/hpe7-a01.html

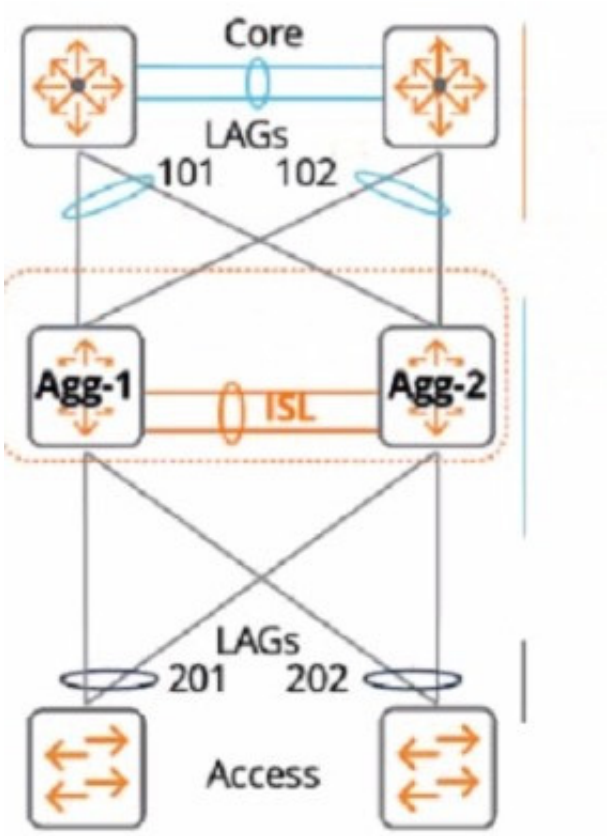
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A customer just upgraded aggregation layer switches and noticed traffic dropping for 120 seconds after the aggregation layer came online again. What is the best way to avoid having this traffic dropped given the topology below?



A. Configure the linkup delay timer to 240 seconds to double the amount of lime for the initial phase to sync

B. Configure the linkup delay timer to exclude LAGS 101 and 102, which will allow time for routing adjacencies to form and to learn upstream routes

C. Configure the linkup delay timer to include LAGs 101 and 102, which will allow time for routing adjacencies lo form and to learn upstream routes

D. Configure the linkup delay timer to 120 seconds, which will allow the right amount of time for the initial phase to sync

Correct Answer: C

Explanation: The reason is that the linkup delay timer is a feature that delays bringing downstream VSX links up, following a VSX device reboot or an ISL flap. The linkup delay timer has two phases: initial synchronization phase and link-up delay phase. The initial synchronization phase is the download phase where the rebooted node learns all the LACP+MAC+ARP+STP database entries from its VSX peer through ISLP. The initial synchronization timer, which is not configurable, is the required time to download the database information from the peer. The link-up delay phase is the duration for installing the downloaded entries to the ASIC, establishing router adjacencies with core nodes and learning upstream routes. The link-up delay timer default value is 180 seconds. Depending on the network size, ARP/routing tables size, you might be required to set the timer to a higher value (maximum 600 seconds). When both VSX devices reboot, the link-up delay timer is not used. Therefore, by configuring the linkup delay timer to include LAGs 101 and 102, which are part of the same VSX device as LAG 201, you can ensure that both devices have enough time to synchronize their databases and form routing adjacencies before bringing down their downstream links.

QUESTION 2

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 MacBooks 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

Correct 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.

QUESTION 3

Using Aruba best practices what should be enabled for visitor networks where encryption is needed but authentication is not required?

A. Wi-Fi Protected Access 3 Enterprise

B. Opportunistic Wireless Encryption

C. Wired Equivalent Privacy

D. Open Network Access

Correct Answer: B

Explanation: Opportunistic Wireless Encryption (OWE) is a feature that provides encryption for open wireless networks without requiring authentication. OWE uses an enhanced version of the 4-way handshake to establish a pairwise key between the client and the AP, which is then used to encrypt the wireless traffic using WPA2 or WPA3 protocols. OWE can be used for visitor networks where encryption is needed but authentication is not required. References: https://www.arubanetworks.com/assets/tg/TG_OWE.pdf

QUESTION 4

How is Dynamic Multicast Optimization (DMO) implemented in an HPE Aruba wireless network?

A. DMO is configured individually tor each SSID in use in the network.

B. The AP uses OOS to provide equal air time for multicast traffic,

C. DMO is configured globally for each SSID in use in the network.

D. The controller converts multicast streams into unicast streams.

Correct Answer: A

The correct answer is A. DMO is configured individually for each SSID in use in the network.

DMO is a feature that allows the AP to convert multicast streams into unicast streams over the wireless link. This enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. DMO is

configured individually for each SSID in use in the network, as different SSIDs may have different multicast requirements.

According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure DMO is:

Dynamic multicast optimization: Select Enabled to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video,

while preserving the bandwidth available to the non-video clients.

The other options are incorrect because:

B. The AP does not use QoS to provide equal air time for multicast traffic. QoS is a feature that prioritizes different types of traffic based on their importance and latency sensitivity. QoS does not affect how multicast streams are transmitted over the wireless link.

C. DMO is not configured globally for each SSID in use in the network. DMO is configured individually for each SSID, as different SSIDs may have different multicast requirements.

D. The controller does not convert multicast streams into unicast streams. The AP does the conversion, as it is closer to the wireless clients and can optimize the transmission based on the client capabilities and channel conditions.

QUESTION 5

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

Correct 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.

QUESTION 6

Which statements are true about VSX LAG? (Select two.)

A. The total number of configured links may not exceed 8 for the pair or 4 per switch

B. Outgoing traffic is switched to a port based on a hashing algorithm which may be either switch in the pair

C. LAG traffic is passed over VSX ISL links only while upgrading firmware on the switch pair

D. Outgoing traffic is preferentially switched to local members of the LAG.

E. Up to 255 VSX lags can be configured on all 83xx and 84xx model switches.

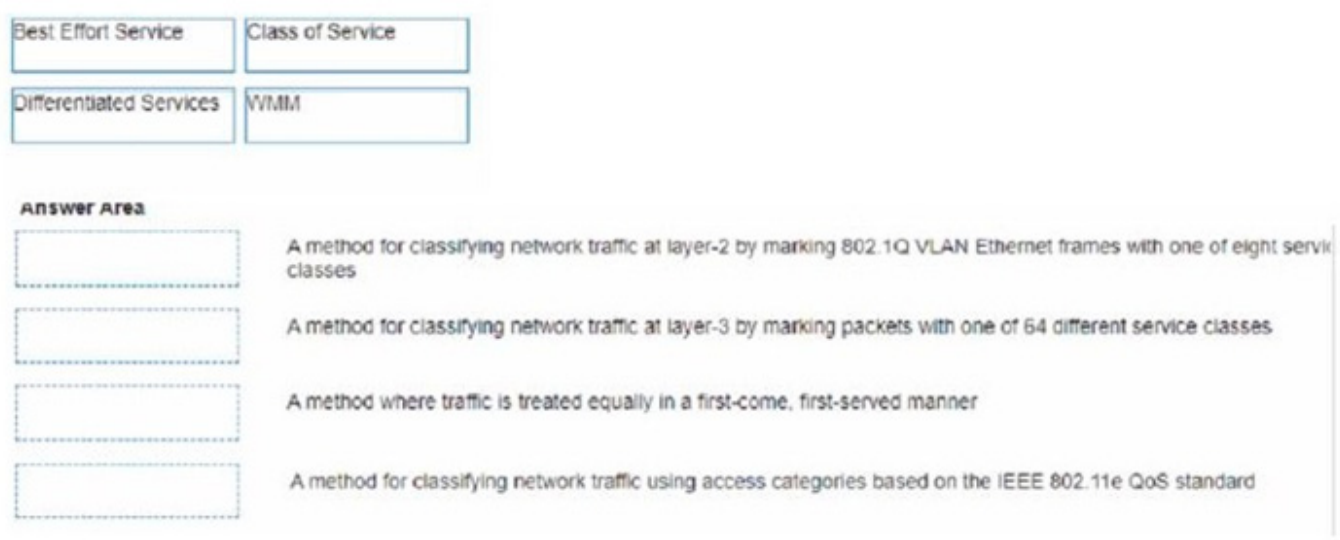
Correct Answer: AD

Explanation: The correct answers are A and D. According to the web search results, VSX LAG is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices1. VSX LAGs span both aggregation switches and appear as one device to partner downstream or upstream devices or both when forming a LAG with the VSX pair2. One of the statements that is true about VSX LAG is that the total number of configured links may not exceed 8 for the pair or 4 per switch1. This means that a VSX LAG across a downstream switch can have at most a total of eight member links, and a switch can have a maximum of four member links. When creating a VSX LAG, it is recommended to select an equal number of member links in each segment for load balancing1. Another statement that is true about VSX LAG is that outgoing traffic is preferentially switched to local members of the LAG2. This means that when active forwarding and active gateway are enabled, north-south and south-north traffic bypasses the ISL link and uses the local ports on the switch. This optimizes the traffic path and reduces the load on the ISL link2. The other statements are false or not relevant for VSX LAG. Outgoing traffic is not switched to a port based on a hashing algorithm, which may be either switch in the pair. This is a characteristic of MLAG (Multi-Chassis Link Aggregation), which is a different feature from VSX LAG. LAG traffic is not passed over VSX ISL links only while upgrading firmware on the switch pair. This is a scenario that may occur when performing hitless upgrades, which is a feature that allows software updates without impacting network availability. The number of VSX lags that can be configured on all 83xx and 84xx model switches is not 255, but depends on the switch model and firmware version. For example, the AOS-CX 10.04 supports up to 64 VSX lags for 8320 switches and up to 128 VSX lags for 8325 and 8400 switches.

QUESTION 7

Match the appropriate QoS concept with its definition. (Options may be used more than once or not at all.)

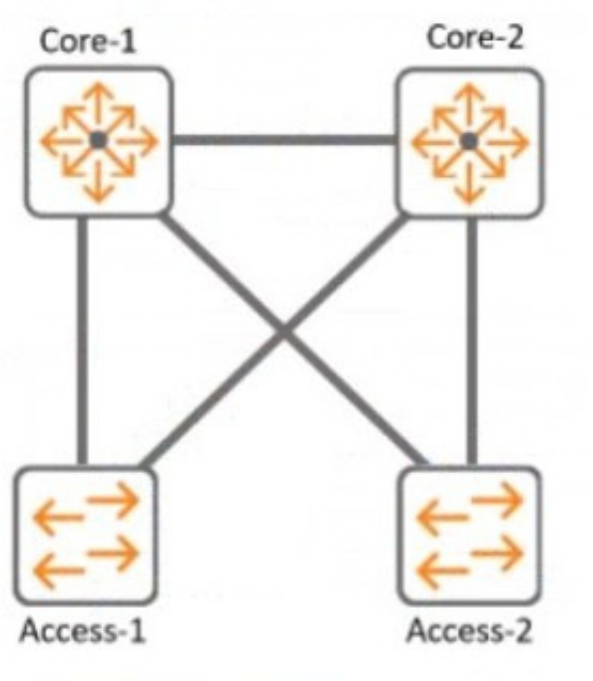
Select and Place:



Correct Answer:

QUESTION 8

Refer to the exhibit.



With Core-1. what is the default value for config-revision?

A. 0

B. 1

C. 1-0

D. 0. 0

Correct Answer: A

Explanation: The default value for config-revision on Core-1 is 0. Config-revision is a parameter that indicates the configuration version of a VSX pair. It is used to synchronize the configuration between the VSX peers and to detect any configuration mismatch. The config-revision value is set to 0 by default on both VSX peers and is incremented by 1 every time a configuration change is made on either peer. The other options are incorrect because they do not reflect the default value of config-revision. 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

QUESTION 9

A network administrator is troubleshooting some issues guest users are having when connecting and authenticating to the network The access switches are AOS-CX switches.

What command should the administrator use to examine information on which role the guest user has been assigned?

A. show aaa authentication port-access interface all client-status

B. show port-access captiveportal profile

C. show port-access role

D. diag-dump captiveportal client verbose

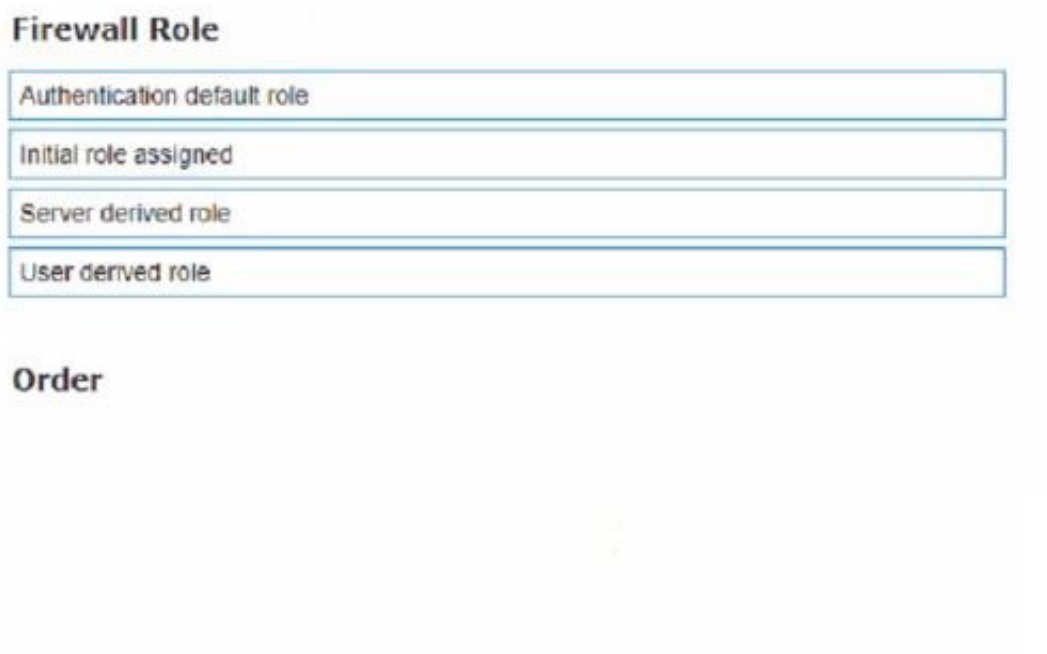
Correct Answer: A

Explanation: The show aaa authentication port-access interface all client-status command displays the status of all clients authenticated by port-based access control on all interfaces. The output includes the MAC address, user role, VLAN ID, and session timeout for each client. This command can be used to examine information on which role the guest user has been assigned by the AOS-CX switch. References: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A- 4F0D-AE7B-9D8E6C5B6A7F.html

QUESTION 10

List the firewall role derivation flow in the correct order.

Select and Place:



Correct Answer:

QUESTION 11

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 administrators role did not have the appropriate level of access on the switch.

The user was not limited to viewing nonsensitive configuration information and a level of 1 was not assigned to their role.

Which default management role should have been assigned for the user?

A. sysadmin

B. operators

C. helpdesk

D. config

Correct Answer: B

Explanation: The default management role that should have been assigned for the user is B. operators.

The operators user role is a predefined role that allows users to view nonsensitive configuration information on the switch, such as interfaces, VLANs, routing protocols, statistics, and more. The operators user role has a privilege level of 1,

which is the lowest level of access on the switch1.

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.

QUESTION 12

A company recently upgraded its campus switching infrastructure with Aruba 6300 CX switches. They have implemented 802.1X authentication on edge ports where laptop and IoT devices typically connect An administrator has noticed that

for PoE devices the pons are delivering the maximum wattage instead of what the device actually needs Upon connecting the loT devices, the devices request their specific required wattage through information exchange.

Concerned about this waste of electricity, what should the administrator implement to solve this problem?

A. Enable AAA authentication to exempt LLDP and/or CDP information

B. Globally enable the QoS trust setting for LLDP and/or CDP

C. Create device profiles with the correct power definitions.

D. Implement a classifier policy with the correct power definitions.

Correct Answer: D

According to the Aruba Documentation Portal1, the Aruba 6300 CX switches support various features to control the PoE devices on specific ports, such as device profiles and classifier policies. These features can help reduce the power consumption and improve the performance of the PoE devices.

1: https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300- 6400/Content/Chp_LEDs/fro-pan-led-630.htm

2: https://www.arubanetworks.com/products/switches/6300-series/

3: https://docs.samsungknox.com/admin/knox-manage/configure/profile/configure-profile- policies/configure-profile-policies-by-device-platform/

QUESTION 13

Due to a shipping error, five (5) Aruba AP-515S and one (1) Aruba CX 6300 were sent directly to your new branch office You have configured a new group persona for the new branch office devices in Central, but you do not know their MAC addresses or serial numbers The office manager is instructed via text message on their smartphone to onboard all the new hardware into Aruba Central

What application must the office manager use on their phone to complete this task?

A. Aruba Onboard App

B. Aruba Central App

C. Aruba CX Mobile App

D. Aruba installer App

Correct Answer: D

Aruba Installer App is a mobile app that simplifies site installations and enables network connectivity for Aruba devices. The app allows the user to scan the barcode of the device and add it to the network using Aruba Central. The app also automates importing Aruba devices into Aruba NetEdit for intelligent configuration management and continuous conformance validation

QUESTION 14

When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

A. QSVI

B. MAC tables

C. UDLD

D. RPVST+

Correct Answer: B

Explanation: The information that the Inter-Switch Link Protocol configuration uses in the configuration created is B. MAC tables. The Inter-Switch Link Protocol (ISL) is a protocol that enables the synchronization of data and state information between two VSX peer switches. The ISL uses a version control mechanism and provides backward compatibility regarding VSX synchronization capabilities. The ISL can span long distances (transceiver dependent) and supports different speeds, such as 10G, 25G, 40G, or 100G1. One of the data components that the ISL synchronizes is the MAC table, which is a database that stores the MAC addresses of the devices connected to the switch and the corresponding ports or VLANs. The ISL ensures that both VSX peers have the same MAC table entries and can forward traffic to the correct destination2. The ISL also synchronizes other data components, such as ARP table, LACP states for VSX LAGs, and MSTP states2.

QUESTION 15

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
```

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Correct Answer: CE

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.

HPE7-A01 PDF Dumps HPE7-A01 Study Guide HPE7-A01 Braindumps