

HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam



NEW QUESTION 1

A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working across the campus which is connected via layer-3. The legacy devices are connected to Aruba CX 6300 switches throughout the campus. Which technology minimizes flooding so the legacy application can work efficiently?

- A. Generic Routing Encapsulation (GRE)
- B. EVPN-VXLAN
- C. Ethernet over IP (EoIP)
- D. Static VXLAN

Answer: B

Explanation:

EVPN-VXLAN is a technology that allows layer-2 communication across layer-3 networks by using Ethernet VPN (EVPN) as a control plane and Virtual Extensible LAN (VXLAN) as a data plane³. EVPN-VXLAN can be used to support legacy applications that communicate at layer-2 across different campuses or data centers that are connected via layer-3. EVPN-VXLAN minimizes flooding by using BGP to distribute MAC addresses and IP addresses of hosts across different VXLAN segments³. EVPN-VXLAN also provides benefits such as loop prevention, load balancing, mobility, and scalability³. References: ³ https://www.arubanetworks.com/assets/tg/TG_EVPN_VXLAN.pdf

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 company recently deployed new Aruba Access Points at different branch offices. Wireless 802.1X authentication will be against a RADIUS server in the cloud. The security team is concerned that the traffic between the AP and the RADIUS server will be exposed.

What is the appropriate solution for this scenario?

- A. Enable EAP-TLS on all wireless devices
- B. Configure RadSec on the AP and Aruba Central.
- C. Enable EAP-TTLS on all wireless devices.
- D. Configure RadSec on the AP and the RADIUS server

Answer: D

Explanation:

This is the appropriate solution for this scenario where wireless 802.1X authentication will be against a RADIUS server in the cloud and the security team is concerned that the traffic between the AP and the RADIUS server will be exposed. RadSec, also known as RADIUS over TLS, is a protocol that provides encryption and authentication for RADIUS traffic over TCP and TLS. RadSec can be configured on both the AP and the RADIUS server to establish a secure tunnel for exchanging RADIUS packets. The other options are incorrect because they either do not provide encryption or authentication for RADIUS traffic or do not involve RadSec. References: <https://www.securew2.com/blog/what-is-radsec/> <https://www.cloudradius.com/radsec-vs-radius/>

NEW QUESTION 5

Which standard supported by some Aruba APs can enable a customer to accurately locate wireless client devices within a few meters?

- A. 802.11mc
- B. 802.11W
- C. 802.11k
- D. 802.11r

Answer: A

Explanation:

The standard that is supported by some Aruba APs and can enable a customer to accurately locate wireless client devices within a few meters is A. 802.11mc. * 802.11mc is an IEEE standard that enables computing devices to measure the distance to nearby Wi-Fi access points using a technique called Fine Timing Measurement (FTM). FTM uses precise timestamps to calculate the round-trip time of Wi-Fi frames between the device and the access point, and then converts it to a distance estimate. By using multiple access points and triangulation methods, the device can determine its location with high accuracy¹. According to the Aruba document 802.11mc Support, this feature is supported on 500 Series, 510 Series, 530 Series, 550 Series, 560 Series and 570 Series access points. These APs act as FTM responders to time measurement queries sent from a client. To configure the AP to send FTM responses, you need to enable the `ftm-responder-enable` parameter in the WLAN SSID profile¹.

NEW QUESTION 6

A system engineer needs to preconfigure several Aruba CX 6300 switches that will be sent to a remote office. An untrained local field technician will do the rollout of the switches and the mounting of several AP-515s and AP-575S. Cables running to the APs are not labeled.

The VLANs are already preconfigured to VLAN 100 (mgmt), VLAN 200 (clients), and VLAN 300 (guests).

What is the correct configuration to ensure that APs will work properly?

A)

```
port-access lldp-group IAP-Group
  seq 10 match sys-desc AP-515
  seq 20 match sys-desc AP-575
port-access role IAP-Role
  description ARUBA AP
  poe-priority high
  trust-mode dscp vlan trunk native 100
  vlan trunk allowed 100,200,300
  enable
port-access device-profile IAP-Profile
  associate role IAP-Role
  associate lldp-group IAP-Group
```

B)

```
port-access lldp-group IAP-Group
  seq 10 match sys-desc 515
  seq 20 match sys-desc 575
port-access role IAP-Role
  description ARUBA AP
  poe-priority high
  trust-mode dscp
  vlan trunk native 100
  vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
  associate role IAP-Role
  associate lldp-group IAP-Group
  no shutdown
```

C)

```
port-access lldp-group IAP-Group
seq 10 match sys-desc 515
seq 20 match sys-desc 575
port-access role IAP-Role
description ARUBA AP
poe-priority high
trust-mode dscp
vlan trunk native 100
vlan trunk allowed 200,300
port-access device-profile IAP-Profile
enable
associate role IAP-Role
associate lldp-group IAP-Group
```

D)

```
port-access lldp-group IAP-Group
seq 10 match sys-desc 515
seq 20 match sys-desc 575
port-access role IAP-Role
description ARUBA AP
poe-priority high
trust-mode dscp
vlan trunk native 100
vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
enable
associate role IAP-Role
associate lldp-group IAP-Group
```

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

Answer: C

Explanation:

Option C is the correct configuration to ensure that APs will work properly. It uses the ap command to configure a port profile for APs with VLAN 100 as the native VLAN and VLAN 200 and 300 as tagged VLANs. It also enables LLDP on the ports to discover the APs and assign them to the port profile automatically. The other options are incorrect because they either do not use the ap command, do not enable LLDP, or do not configure the VLANs correctly. References:
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch03.html

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

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

- AP1 has a radio that generates a 16 dBm signal.
- AP2 has a radio that generates a 13 dBm signal.
- AP1 has an antenna with a gain of 8 dBi.
- AP2 has an antenna with a gain of 12 dBi. The antenna cable for AP1 has a 4 dB loss. The antenna cable for AP2 has a 3 dB loss.

What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?

- A. -9 dBm
- B. 20 dBm
- C. 40 dBm
- D. 15 dBm

Answer: B

Explanation:

The Equivalent Isotropic Radiated Power (EIRP) is the measured radiated power of an antenna in a specific direction. It is also called Equivalent Isotropic Radiated Power. It is the output power when a signal is concentrated into a smaller area by the Antenna. The EIRP can take into account the losses in transmission line, connectors and includes the gain of the antenna. It is represented in dB2. The formula for EIRP is:

$EIRP = P_{TL} + G_a$ where P_T is the output power of the transmitter in dBm, L_c is the cable and connector loss in dB, and G_a is the antenna gain in dBi.

For AP1, the EIRP can be calculated as: $EIRP = 164 + 8 = 20$ dBm

Therefore, the answer B is correct.

References: 1: Aruba Campus Access documents and learning resources 2: EIRP Calculator - Effective Isotropic Radiated Power

NEW QUESTION 9

A customer is using stacked Aruba CX 6200 and CX 6300 switches for access and a VSX pair of Aruba CX 8325 as a collapsed core 802.1X is implemented for authentication. Due to the lack of cabling, some unmanaged switches are still in use. Sometimes devices behind these switches cause network outages. The switch should send a warning to the helpdesk when the problem occurs. You have been asked to implement an effective solution to the problem.

What is the solution for this?

- A. Configure spanning tree on the Aruba CX 8325 switches. Set the trap-option.
- B. Configure loop protection on all edge ports of the Aruba CX 6200 and CX 6300 switches. No trap option is needed.
- C. Configure loop protection on all edge ports of the Aruba CX 6200 and CX 6300 switches. Set up the trap-option.
- D. Configure spanning tree on the Aruba CX 6200 and CX 6300 switches. No trap option is needed.

Answer: C

Explanation:

This is the correct solution to the problem of devices behind unmanaged switches causing network outages due to loops. Loop protection is a feature that allows an Aruba CX switch to detect and prevent loops by sending loop protection packets on each port, LAG, or VLAN on which loop protection is enabled. If a loop protection packet is received by the same switch that sent it, it indicates a loop exists and an action is taken based on the configuration. Loop protection should be configured on all edge ports of the Aruba CX 6200 and CX 6300 switches, which are the ports that connect to end devices or unmanaged switches. The trap-option should be set up to send a warning to the helpdesk when a loop is detected. The other options are incorrect because they either do not configure loop protection or do not set up the trap-option. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-99A8B276-0DA3-4458-AFD8-42BFEC29D4F5.html>

<https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-8561-17DB0311ED8F.html>

NEW QUESTION 10

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.

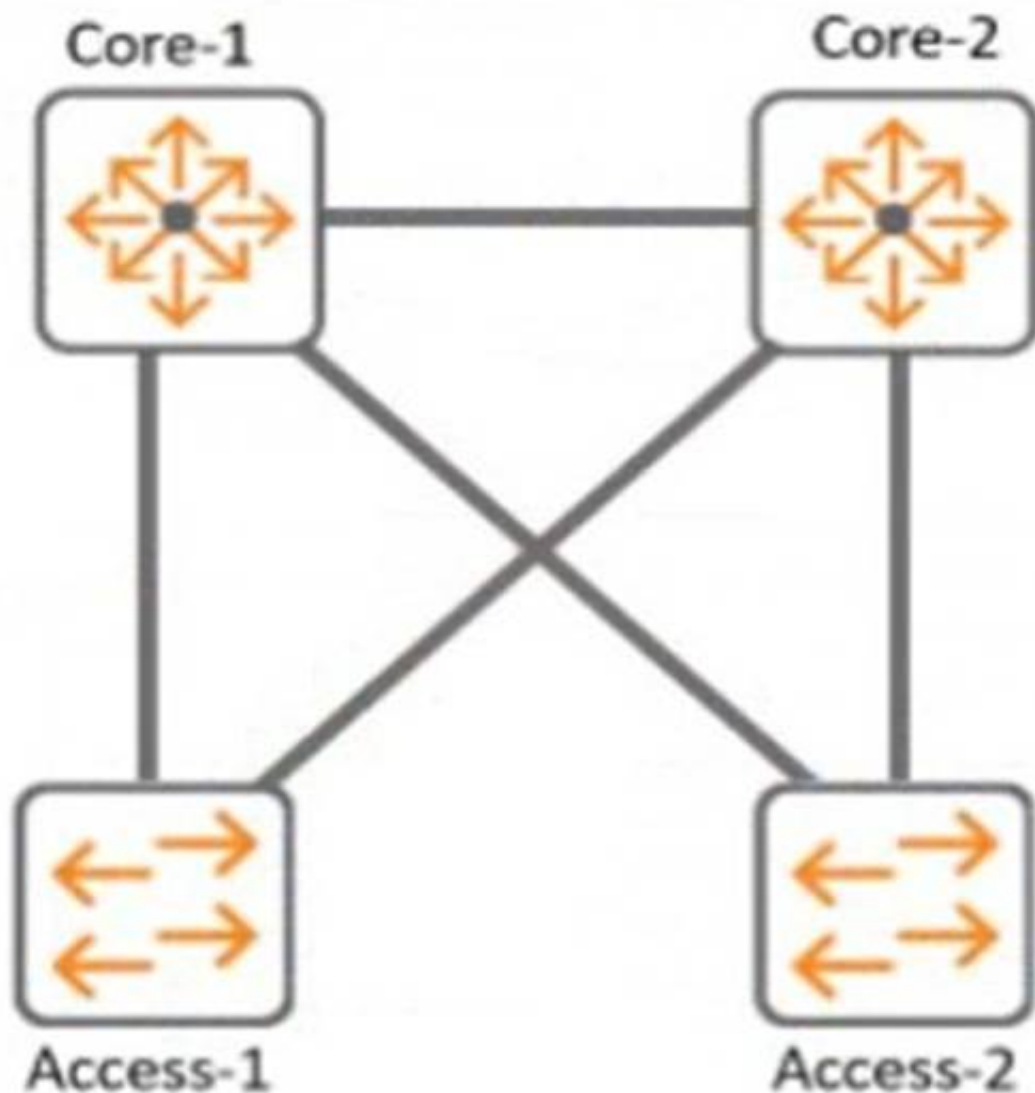
Answer: B

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 10

Refer to the exhibit.



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

- A. 1
- B. 1-0
- C. 0. 0

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>

NEW QUESTION 13

When configuring UBT on a switch what will happen when a gateway role is not specified?

- A. The switch will put the client on the access VLAN
- B. The gateway will assign a default role to the client
- C. The switch will assign the default deny role to the client.
- D. The gateway will send back the deny role to the client.

Answer: A

Explanation:

According to the Aruba Documentation Portal¹, user-based tunneling (UBT) is a feature that uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. UBT enables a switch to provide a centralized security policy, using per- user authentication and access control to ensure consistent access and permissions.

Option A: The switch will put the client on the access VLAN

This is because option A shows how UBT works on an Aruba switch. When a device connects to the network, it is authenticated using either MAC Authentication or 802.1X and triggers an enforcement policy from ClearPass, which contains an enforcement profile with a user role configuration. The user role can be assigned locally on the switch or on ClearPass as part of an enforcement profile. The user role determines the VLAN that the device belongs to and the access policies that apply to it²³.

Therefore, option A is correct.

1: <https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-ubt.htm> 2: <https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html> 3:

<https://community.arubanetworks.com/viewdocument/?DocumentKey=c740df4e-3e26-4cc5-9126-355a18709c44&CommunityKey=2fd943a6-8898-4dbe-915f-4f09e4d3c317&tab=librarydocuments>

NEW QUESTION 18

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:

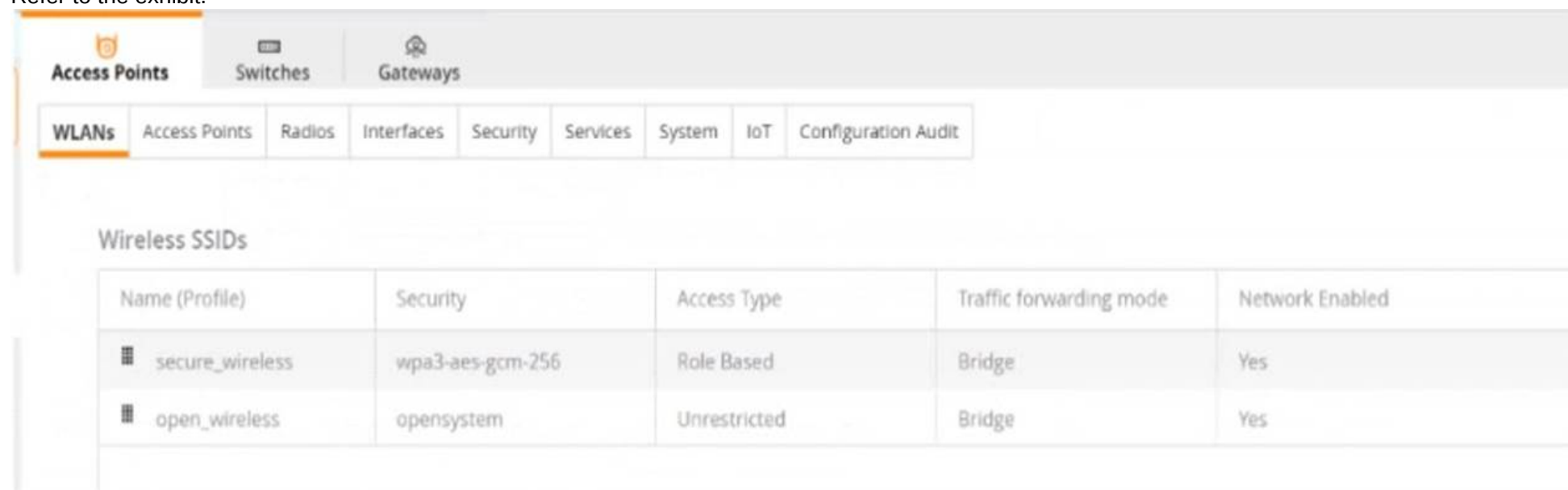
CoA (Change of Authorization) is a feature that allows ClearPass to dynamically change the authorization and access privileges of a device after it has been authenticated¹. CoA uses RADIUS messages to communicate with the network device and instruct it to perform an action, such as reauthenticating the 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 19

Refer to the exhibit.



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 but is not working as expected What would be the correct action to fix the issue?

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

Answer: D

Explanation:

According to the Aruba Campus Access Professional documents¹, WPA3- Enterprise is a security mode that supports 802.1X authentication and encryption with either AES-CCM or AES-GCMP. WPA3-Enterprise also optionally adds usage of Suite-B 192-bit minimum-level security suite that is aligned with Commercial National Security Algorithm (CNSA) for enterprise networks². This mode provides the highest level of security and is suitable for government and financial institutions.

The exhibit shows that the SSID is configured with WPA3-Enterprise (CCM), which uses AES-CCM as the encryption protocol. However, this mode is not compatible with some devices that require CNSA compliance. Therefore, changing the SSID to WPA3-Enterprise (CNSA) would fix the issue and allow all devices to connect to the network.

NEW QUESTION 23

What are the requirements to ensure that WMM is working effectively'? (Select two)

- A. The APs and the controller are Wi-Fi CERTIFIED for WMM which is enabled
- B. All APs need to be from the AP-5xx series and AP-6xx series which are Wi-Fi CERTIFIED 6.
- C. The Client must be Wi-Fi CERTIFIED for WMM and configured for WMM marking.
- D. The Aruba AOS10 APs installed have to be converted to controlled mode
- E. The AP needs to be connected via a tagged VLAN to the wired port

Answer: AC

Explanation:

These are the correct requirements to ensure that WMM (Wi-Fi Multimedia) is working effectively. WMM is a standard that provides quality of service (QoS) for wireless networks by prioritizing traffic into four categories: voice, video, best effort, and background. To use WMM, both the APs and the controller must be Wi-Fi CERTIFIED for WMM, which means they have passed interoperability tests and comply with the standard. WMM must also be enabled on the APs and the controller, which is usually the default setting. The client device must also be Wi-Fi CERTIFIED for WMM and configured for WMM marking, which means it can tag its traffic with the appropriate priority level based on the application type. The other options are incorrect because they are either not related to WMM or not required for WMM to work. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/wlan-qos/wmm.htm
<https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm>

NEW QUESTION 28

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

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.

NEW QUESTION 30

With the Aruba CX 6000 24G switch with uplinks of 1/1/25 and what does the switch do when a client port detects a loop and the do-not-disable parameter is used?

- A. Port status will be validated once status is cleared
- B. An event log message is created.
- C. The network analytics engine is triggered.
- D. Port status led blinks in amber with 100hz.

Answer: B

Explanation:

The correct answer is B. An event log message is created.

The do-not-disable parameter is used to prevent the switch from disabling the port when a loop is detected by the loop-protect feature. Instead, the switch will generate an event log message that indicates the port number and the VLAN ID where the loop was detected. The switch will also send a trap to the SNMP manager, if configured1.

The other options are incorrect because:

? A. Port status will not be validated once status is cleared. The port will remain enabled even if a loop is detected, unless the loop-protect action is changed to tx-disable or tx-rx-disable1.

? C. The network analytics engine will not be triggered by a loop detection. The network analytics engine is a feature that allows users to monitor and troubleshoot network issues using scripts and agents2.

? D. Port status LED will not blink in amber with 100Hz. The port status LED will indicate the normal port status, such as link speed and activity, regardless of the loop detection3.

NEW QUESTION 34

What is a primary benefit of BSS coloring?

- 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 channel12. Each BSS is assigned a color code, which is a 6-bit value that is carried in the PHY header of the Wi-Fi frames12. 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 colors12. This can improve the spectral efficiency and throughput of the network12. The other options are incorrect because they do not describe the primary benefit of BSS coloring.

NEW QUESTION 36

You must ensure the HPEAruba network you are configuring for a client is capable of plug- and-play provisioning of access points. What enables this capability?

- A. UCC Service
- B. LLDP-MED
- C. SRTP
- D. CSMA

Answer: A

Explanation:

The capability that enables plug-and-play provisioning of access points in an HPE Aruba network is the UCC Service. The UCC Service is a cloud-based service that allows the access points to automatically discover and connect to the Aruba Central management platform without any manual intervention. The UCC Service also provides zero-touch configuration, firmware updates, and monitoring for the access points1.

The other options are incorrect because:

? B. LLDP-MED: LLDP-MED is a protocol that enhances the interoperability between network devices and IP phones. It does not enable plug-and-play provisioning of access points2.

? C. SRTP: SRTP is a protocol that provides encryption and authentication for voice and video traffic. It does not enable plug-and-play provisioning of access points3.

? D. CSMA: CSMA is a protocol that regulates how devices share a common medium, such as a wireless channel. It does not enable plug-and-play provisioning of access points.

NEW QUESTION 41

DRAG DROP

Match the terms below to their characteristics (Options may be used more than once or not at all.)

Term	Characteristic
Broadcast	A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address 10.13.4.2 in the other network
IP Directed Broadcast	One/more senders and one/more recipients participate in data transfer traffic
Multicast	Sent to all hosts on a remote network
Unicast	Sent to all NICs on the same network segment as the source NIC

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

a) A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address 10.13.4.2 in the other network -> Unicast
b) One/more senders and one/more recipients participate in data transfer traffic -> Multicast
c) Sent to all hosts on a remote network -> IP Directed Broadcast
d) Sent to all NICs on the same network segment as the source NIC -> Broadcast
References: 1 <https://www.thestudygenius.com/unicast-broadcast-multicast/>
The terms broadcast, IP directed broadcast, multicast, and unicast are different types of communication or data transmission over a network. They differ in how many devices are involved in the communication and how they address the messages. The following table summarizes the characteristics of each term1:

Term	Definition	Example
Broadcast	One-to-all communication, where data is sent to every device on the network	A device with IP address 10.1.3.7 sends a DHCP request to 255.255.255.255
IP Directed Broadcast	One-to-all communication, where data is sent to all hosts on a remote network	A device with IP address 10.1.3.7 sends a ping request to 10.13.4.255
Multicast	One-to-many or many-to-many communication, where data is sent to a group of devices that have joined a multicast group	A device with IP address 10.1.3.7 sends a video stream to 239.0.0.1
Unicast	One-to-one communication, where data is sent to only one device	A device with IP address 10.1.3.7 sends an email to a device with IP address 10.13.4.2

NEW QUESTION 43
Which statement best describes QoS?

- A. Determining which traffic passes specified quality metrics
- B. Scoring traffic based on the quality of the contents
- C. Identifying specific traffic for special treatment
- D. Identifying the quality of the connection

Answer: A

Explanation:
QoS stands for Quality of Service and is a mechanism that allows network devices to prioritize and differentiate traffic based on certain criteria, such as application type, source, destination, etc3. QoS involves identifying specific traffic for special treatment and applying policies and actions to improve its performance or meet certain service level agreements (SLAs)3. QoS can help network devices to manage congestion, delay, jitter, packet loss, bandwidth allocation, etc., for different types of traffic3. QoS can be implemented at various layers of the network stack and across different network domains. References: 3 <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mt-book/qos-overview.html>

NEW QUESTION 44
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 47
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 52

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

Answer: D

Explanation:

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.

NEW QUESTION 57

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

- A. DMO is configured individually for 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.

Answer: A

Explanation:

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.

NEW QUESTION 60

DRAG DROP

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

		Answer Area	
Best Effort Service	Class of Service		A method for classifying network traffic at layer-2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Differentiated Services	WMM		A method for classifying network traffic at layer-3 by marking packets with one of 64 different service classes
			A method where traffic is treated equally in a first-come, first-served manner
			A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

QoS concept: Class of Service Definition: 3) A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standards

QoS concept: Differentiated services Definition: 2) A method for classifying network traffic at layer-3 or marking packets with one of 64 different service classes
QoS concept: WMM Definition: 4) A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standards

NEW QUESTION 64

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 ports are delivering the maximum wattage instead of what the device actually needs. Upon connecting the IoT devices, the devices request their specific required wattage through information exchange.

- A. Concerned about this waste of electricity, what should the administrator implement to solve this problem?
- B. Enable AAA authentication to exempt LLDP and/or CDP information.
- C. Globally enable the QoS trust setting for LLDP and/or CDP.
- D. Create device profiles with the correct power definitions.
- E. Implement a classifier policy with the correct power definitions.

Answer: D

Explanation:

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/>

NEW QUESTION 69

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 73

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

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.

NEW QUESTION 74

.....

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](#)