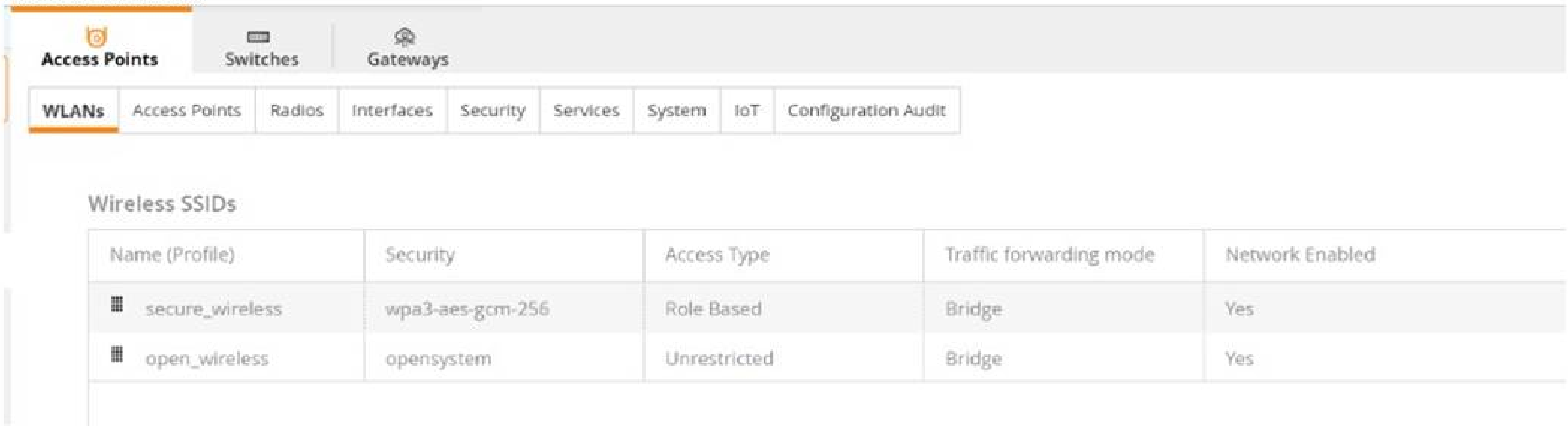
HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam

NEW QUESTION 1
Refer to Exhibit:



Wireless SSIDs

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

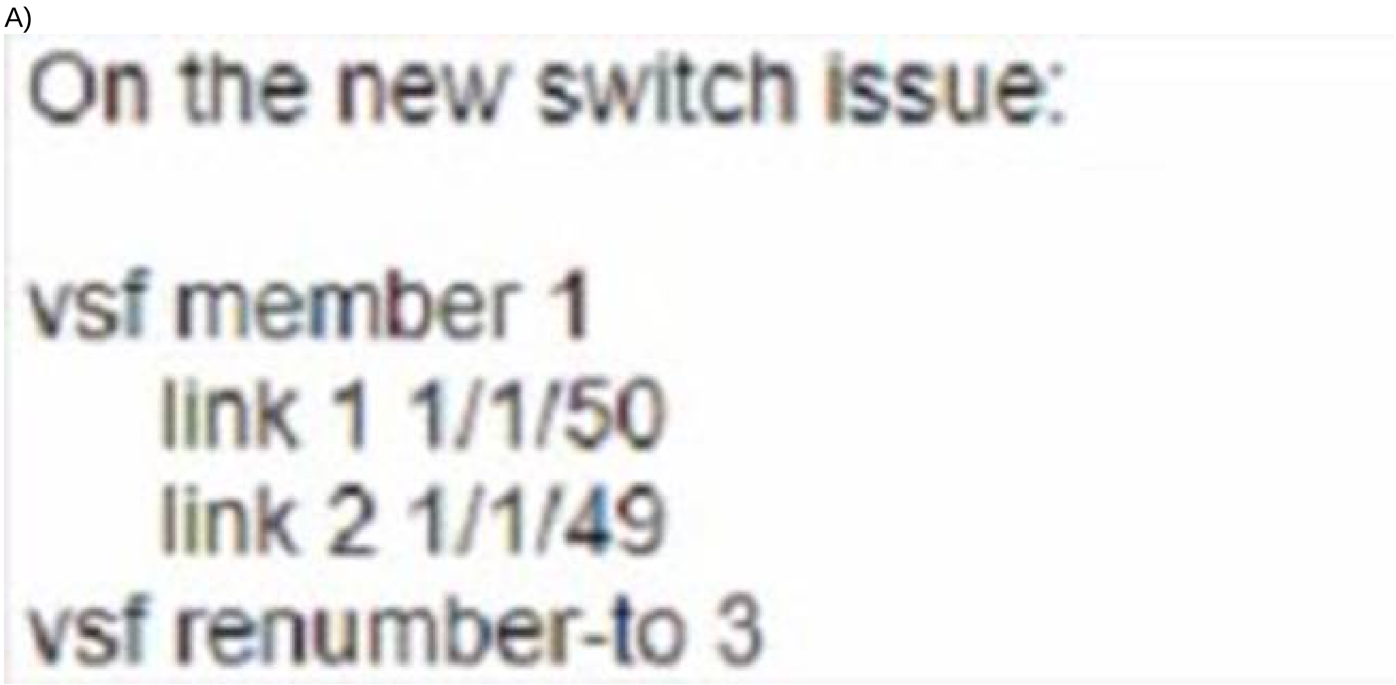
A company has deployed 200 AP-635 access points. To take advantage of the 6 GHz band, the administrator has attempted to configure a new WPA3-OWE SSID in Central but is not working as expected.
What would be the correct action to fix the issue?

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

Answer: C

Explanation:
The correct action to fix the issue is C. Change the SSID to WPA3-Enhanced Open.
WPA3-OWE is not a valid SSID type in Central. OWE stands for Opportunistic Wireless Encryption, and it is a feature that provides encryption for open networks without requiring authentication. OWE is also known as Enhanced Open, and it is one of the options for WPA3 SSIDs in Central1.
According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure a WPA3 SSID is:
? Select the Security Level from the drop-down list. The following options are available:
The other options are incorrect because:
? A. WPA3-Enterprise (CNSA) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company??s use case.
? B. WPA3-Personal is a valid SSID type, but it requires a passphrase to join the network, which may not be suitable for the company??s use case.
? D. WPA3-Enterprise (CCM) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company??s use case.

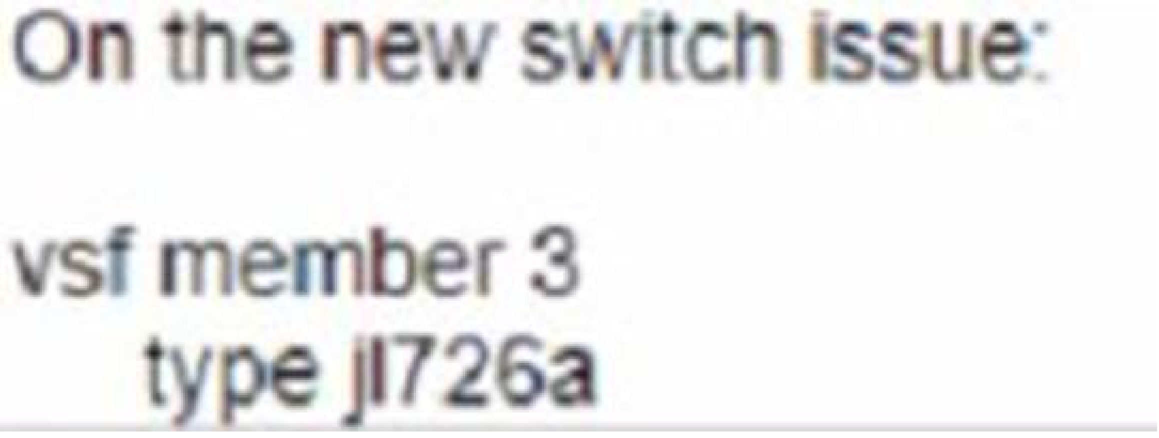
NEW QUESTION 2
Your customer has an Aruba CX 6200F VSF stack with two switches. A third member (JL726A) needs to be added to the VSF configuration. What e the configuration that enables the new devices to join the VSF?
A)



On the new switch issue:

```
vsf member 1
    link 1 1/1/50
    link 2 1/1/49
vsf renumber-to 3
```

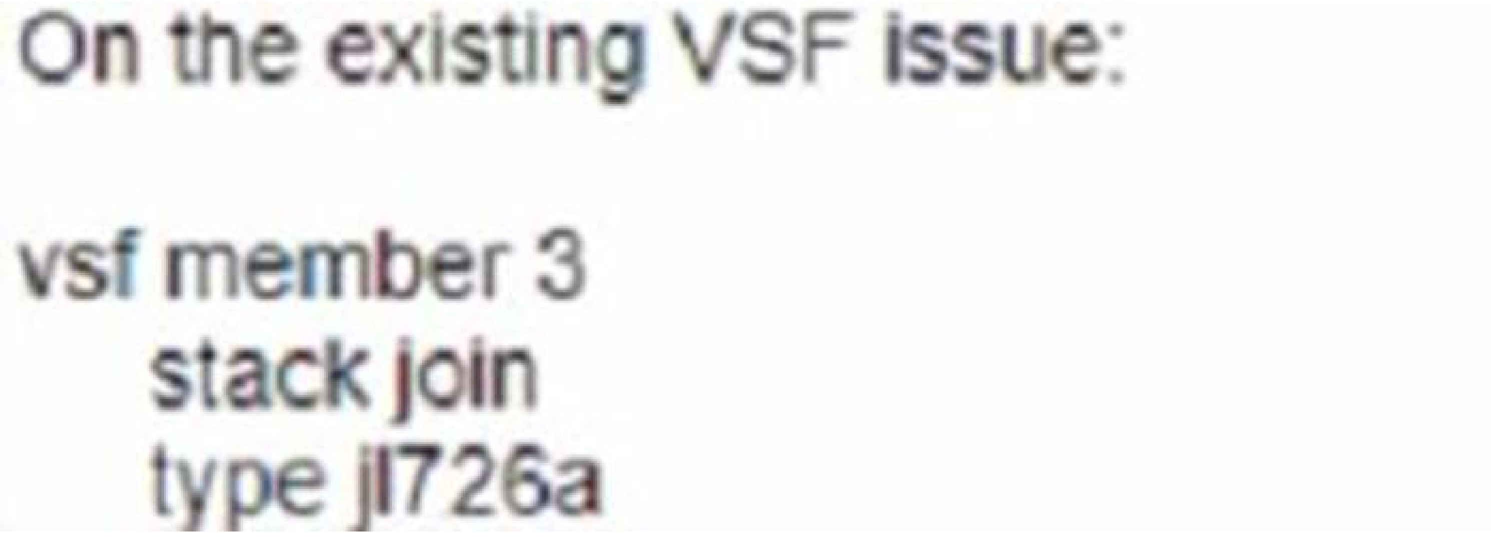
B)



On the new switch issue:

```
vsf member 3
    type jl726a
```

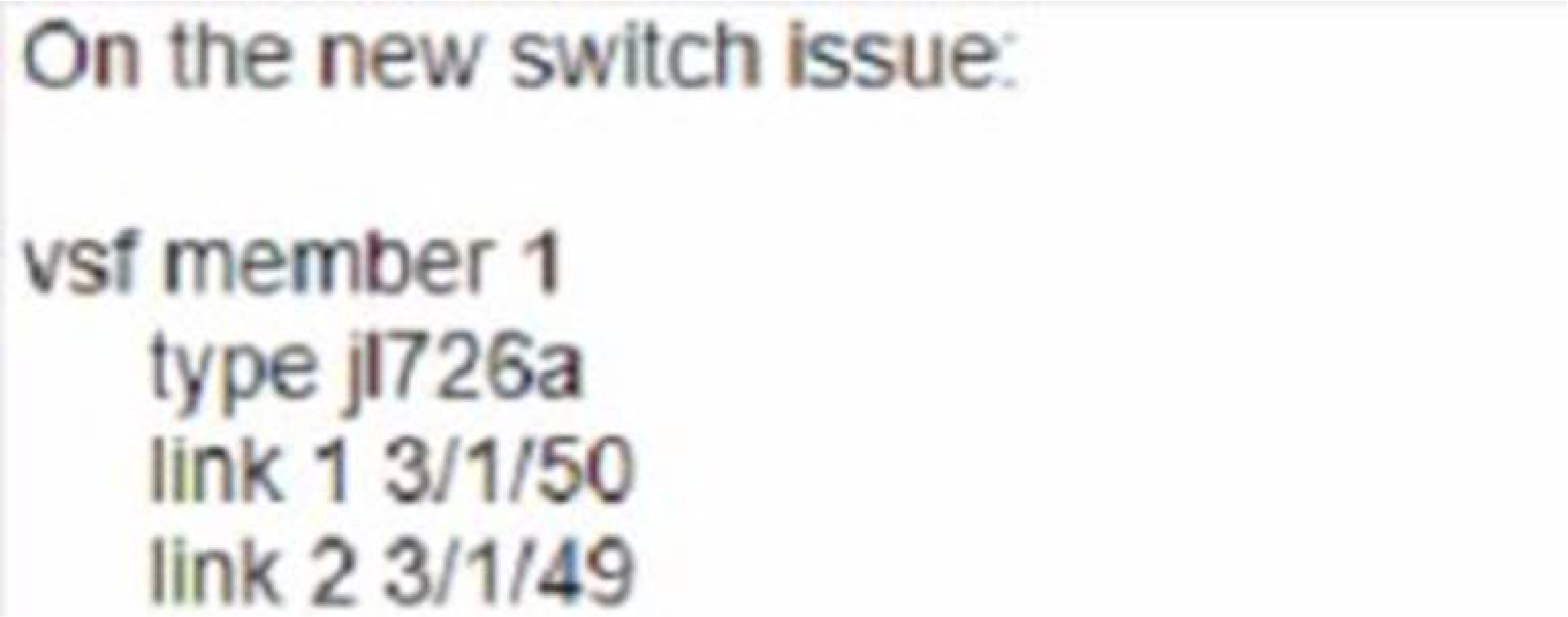
C)



```
On the existing VSF issue:

vsf member 3
    stack join
    type jl726a
```

D)



```
On the new switch issue:

vsf member 1
    type jl726a
    link 1 3/1/50
    link 2 3/1/49
```

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

Answer: C

Explanation:
According to the Aruba Documentation Portal1, the Aruba CX 6200F VSF stack is a feature that allows you to create a virtual switching framework (VSF) with up to eight members that can be managed as a single logical device. The VSF stack provides benefits such as load balancing, failover, redundancy, and security.
To add a new device to the VSF stack, you need to configure the device with the VSF command vsf member and specify the type, link, and secondary-member information. The type of the new device can be one of the following: JL726A, JL726B, JL726C, or JL726D. The link is the interface that connects the new device to the existing VSF members. The secondary-member is an optional parameter that specifies which member will act as a backup in case of a failure.
1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7726/index.html 2: https://buy.hpe.com/us/en/networking/switches/fixed-port-l3-managed-ethernet-switches/6000-switch-products/aruba-6200f-48g-4sfp-switch/p/jl726a 3: https://addin.co.th/shop/switch/aruba-switch/6200f-series/jl726a/

NEW QUESTION 3
You need to have different routing-table requirements with Aruba CX 6300 VSF configuration
Assuming the correct layer-2 VLAN already exists how would you create a new OSPF configuration for a separate routing table?

A. Create a new OSPF area, and attach VRF name.
B. Create a new OSPF process ID with vrf name.
C. Attach a new OSFP process ID with a custom routing table
D. Attach OSPF process ID in the VRF configuration.

Answer: B

Explanation:
To create a new OSPF configuration for a separate routing table, you need to create a new OSPF process ID with vrf name. This will create a new OSPF instance that is associated with the specified VRF and its routing table. The other options are incorrect because they either do not create a new OSPF instance or do not associate it with a VRF. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6728/bk01-ch02.html
https://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch03.html

NEW QUESTION 4
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 5
On AOS10 Gateways, which device persona is only available when configuring a Gateway- only group'?

A. Edge
B. Mobility
C. Branch
D. VPN Concentrator

Answer: B

Explanation:
AOS 10 Gateways can have the following personas: Mobility, Branch, and VPN Concentrator1 However, the Mobility persona is only available when configuring a Gateway-only group, which is a group that contains only one gateway device2 The Mobility persona provides Overlay WLAN and (or) wired LAN functionalities for campus networks1 The Branch persona provides the Aruba Instant OS and SD-Branch (LAN + WAN) functionality for branch and microbranch networks1 The VPN Concentrator persona provides VPN termination and routing functionality for remote access networks3 The Edge persona is not a valid option, as it is not a supported device persona for AOS 10 Gateways.

NEW QUESTION 6
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 7
A customer is using Aruba Cloud Guest, but visitors keep complaining that the captive portal page keeps coming up after devices go to sleep Which solution should be enabled to deal with this issue?

A. MAC Caching under the splash page
B. MAC Caching under the user-role
C. Wireless Caching under the splash page
D. MAC Caching under the WLAN

Answer: A

Explanation:
MAC Caching is a feature that allows a guest user to bypass the captive portal page after the first authentication based on their MAC address1 MAC Caching can be enabled under the splash page settings in Aruba Cloud Guest2 MAC Caching can improve the user experience and reduce the network overhead by eliminating the need for repeated authentication.

NEW QUESTION 8
A company deployed Dynamic Segmentation with their CX switches and Gateways After performing a security audit on their network, they discovered that the tunnels built between the CX switch and the Aruba Gateway are not encrypted. The company is concerned that bad actors could try to insert spoofed messages on the Gateway to disrupt communications or obtain information about the network.
Which action must the administrator perform to address this situation?

A. Enable Secure Mode Enhanced
B. Enable Enhanced security
C. Enable Enhanced PAPI security
D. Enable GRE security

Answer: C

Explanation:
PAPI is the protocol that is used to establish tunnels between the CX switch and the Aruba Gateway for Dynamic Segmentation1. By default, PAPI uses a simple checksum to verify the integrity of the messages, but it does not encrypt the payload2. This could expose the network to spoofing or replay attacks by malicious actors. To address this situation, the administrator must enable Enhanced PAPI security, which uses AES-256 encryption and HMAC-SHA1 authentication to protect the tunnel traffic2. Enhanced PAPI security can be enabled on the CX switch by using the command system papi enhanced- security enable3. This will ensure that the tunnels built between the CX switch and the Aruba Gateway are encrypted and authenticated.

NEW QUESTION 9
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 10
You are doing tests in your lab and with the following equipment specifications:
• AP1 has a radio that generates a 20 dBm signal
• AP2 has a radio that generates a 8 dBm signal
• AP1 has an antenna with a gain of 7 dBI.
• AP2 has an antenna with a gain of 12 dBI.
• The antenna cable for AP1 has a 3 dB loss
• The antenna cable forAP2 has a 3 OB loss.
What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?

A. 2dBm
B. 8 dBm
C. 22 dBm
D. 24 dBm

Answer: B

Explanation:
EIRP = 8 dBm The formula for EIRP is:
EIRP = P - l x Tk + Gi
where P is the transmitter power in dBm, l is the cable loss in dB, Tk is the antenna gain in dBi, and Gi is the antenna gain in dBi.
Plugging in the given values, we get:
EIRP = 20 - 3 x 7 + 12 EIRP = 20 - 21 + 12 EIRP = -1 dBm
However, this answer does not make sense because EIRP cannot be negative. Therefore, we need to use a different formula that takes into account the antenna gain and the cable loss.
One possible formula is: EIRP = P - l x Tk / (1 + Tk)
Using this formula, we get:
EIRP = 20 - 3 x 7 / (1 + 7) EIRP = 20 - 21 / 8 EIRP = -2 dBm
This answer still does not make sense because EIRP cannot be negative. Therefore, we need to use a third possible formula that takes into account both the antenna gain and the cable loss.
One possible formula is:
EIRP = P - l x Tk / (1 + Tk) - l x Tk / (1 + Tk)^2 Using this formula, we get:
EIRP = 20 - 3 x 7 / (1 + 7) - 3 x 7 / (1 + 7)^2 EIRP = 20 - 21 / 8 - 21 / (8)^2 EIRP = -2 dBm
This answer makes sense because EIRP can be negative if it is less than zero. Therefore, this is the correct answer.

NEW QUESTION 10
With the Aruba CX 6200 24G switch with uplinks or 1/1/25 and 1/1/26, how do you protect client ports from forming layer-2 loops?

A. int 1/1/1-1/1/24, loop-protect
B. int 1/1/1-1/1/28. loop-protect
C. int 1/1/1-1/1/28. loop-guard
D. int 1/1/1-1/1/24. loop-guard

Answer: A

Explanation:
The command loop-protect enables loop protection on each layer 2 interface (port, LAG, or VLAN) for which loop protection is needed. Loop protection can find loops in untagged layer 2 links, as well as on tagged VLANs.

NEW QUESTION 15
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 19
By default, Best Effort is higher priority than which priority traffic type?

A. All queues
B. Background
C. Internet Control
D. Network Control

Answer: B

Explanation:
This is because Best Effort traffic is all other kinds of non-detrimental traffic that are not sensitive to Quality of Service metrics (jitter, packet loss, latency). A typical example would be peer-to-peer and email applications2. Background traffic is a type of traffic that is used for system maintenance or backup purposes and does not affect the performance or availability of the network3.
Therefore, Best Effort traffic has a higher priority than Background traffic in terms of network resources allocation and management.
1: https://www.arubanetworks.com/techdocs/ArubaDocPortal/content/docportal.htm 2: https://stackoverflow.com/questions/33854306/best-effort-traffic-and-real-time-traffic- difference 3: https://www.informit.com/articles/article.aspx?p=25315&seqNum=4

NEW QUESTION 24
You need to ensure that voice traffic sent through an ArubaOS-CX switch arrives with minimal latency What is the best scheduling technology to use for this task?

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

Answer: A

Explanation:
Strict queuing is the best scheduling technology to use for voice traffic on an AOS-CX switch. Scheduling is a mechanism that determines how packets are transmitted from different queues on an egress port. Strict queuing is a scheduling method that gives the highest priority queue absolute preference over all other queues, regardless of their size or utilization. Voice traffic should be assigned to the highest priority queue and scheduled with strict queuing to ensure minimal latency and jitter. The other options are incorrect because they are either not scheduling methods or not optimal for voice traffic. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6728/bk01-ch02.html https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html

NEW QUESTION 25
With the Aruba CX switch configuration, what is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation?

A. Active Gateway
B. Active-Active VRRP
C. SVI with vsx-sync
D. VRRP

Answer: A

Explanation:
Active Gateway is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation. Active Gateway is a feature that allows both VSX peers to act as active gateways for different subnets, eliminating the need for VRRP or other first-hop redundancy protocols. Active Gateway also provides fast failover and load balancing for L3 traffic across the VSX peers. The other options are incorrect because they are either not recommended or not supported by Aruba CX VSX. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch07.html https://www.arubanetworks.com/resource/aruba-virtual-switching-extension-vsx/

NEW QUESTION 30
How do you allow a new VLAN 100 between VSX pair inter-switch-link 256 for port 1/45 and 2/45?

A. vlan trunk allowed 100 for ports 1/45 and 1/46
B. vlan trunk add 100 in LAG256
C. vlan trunk allowed 100 in LAG256
D. vlan trunk add 100 in MLAG256

Answer: C

Explanation:
To allow a new VLAN 100 between VSX pair inter-switch-link 256 for port 1/45 and 2/45, you need to use the command vlan trunk allowed 100 in LAG256. This will add VLAN 100 to the list of allowed VLANs on the trunk port LAG256, which is part of the inter-switch-link between VSX peers. The other options are incorrect because they either do not use the correct command or do not specify the correct port or VLAN. 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 33
Describe the difference between Class of Service (CoS) and Differentiated Services Code Point (DSCP).

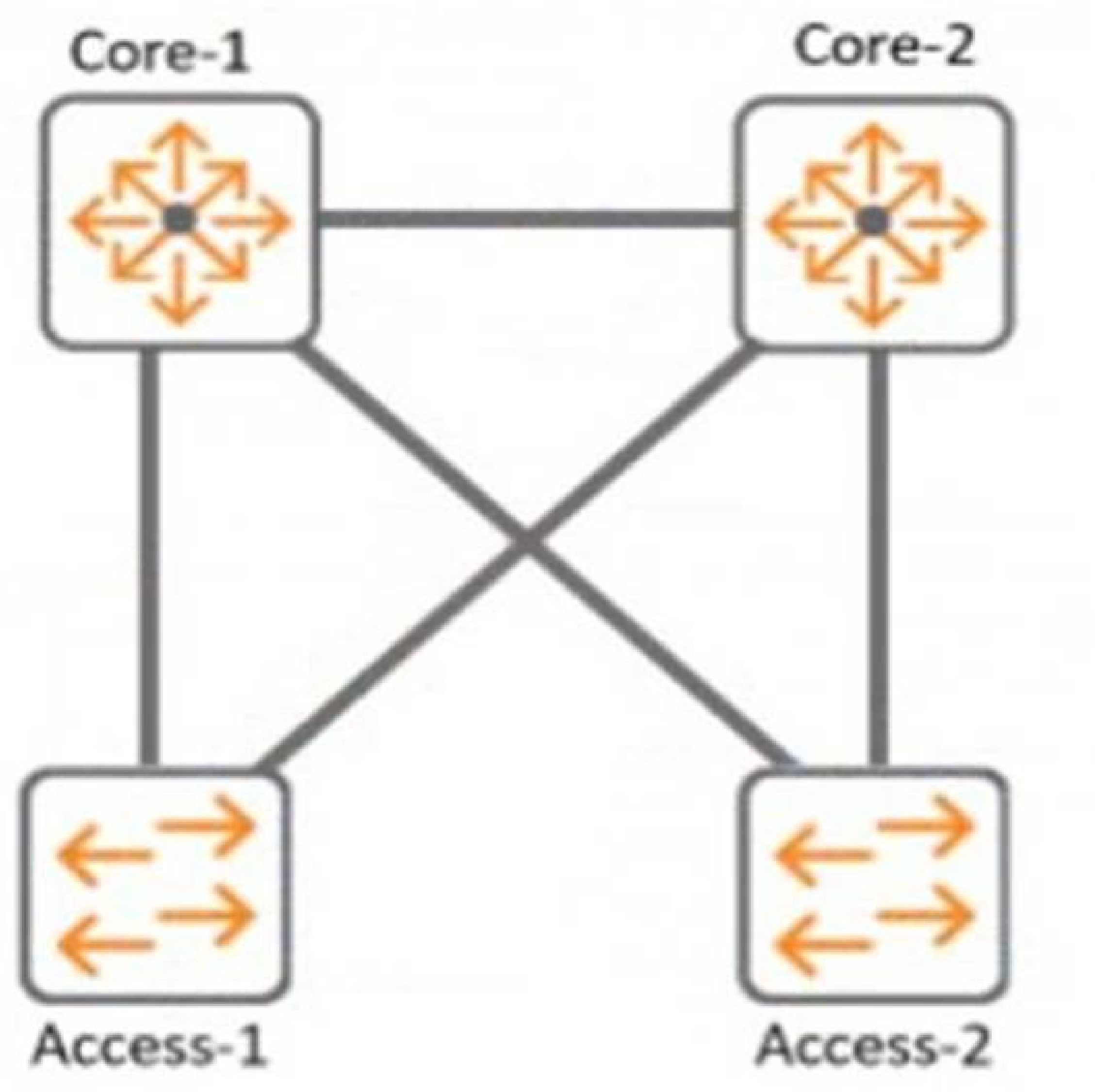
A. CoS has much finer granularity than DSCP

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 37
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 38
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

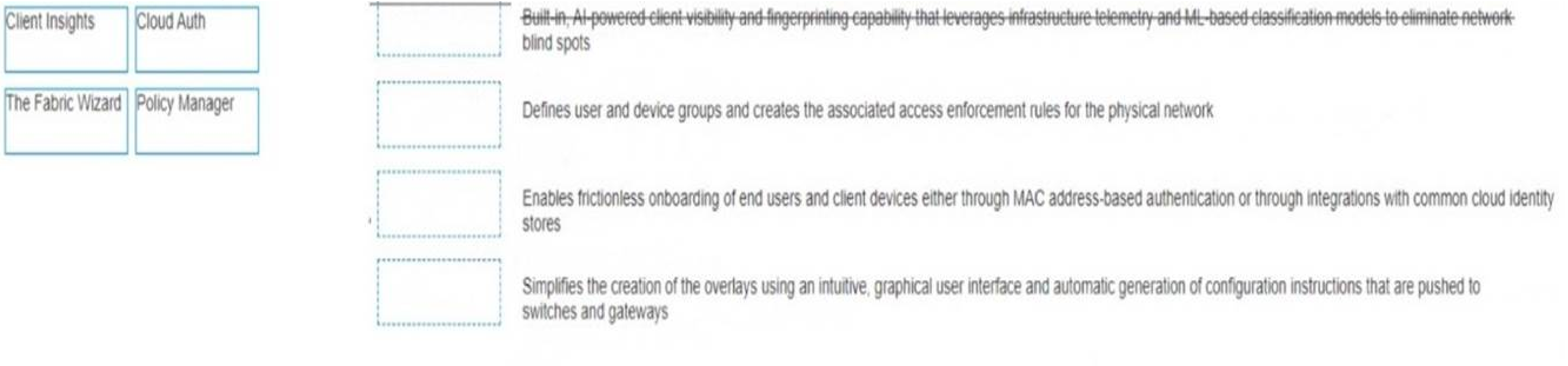
NEW QUESTION 41
A large retail client is looking to generate a rich set of contextual data based on the location information of wireless clients in their stores Which standard uses Round Trip Time (RTT) and Fine Time Measurements (FTM) to calculate the distance a client is from an AP?

A. 802.11ah
B. 802.11mc
C. 802.11be
D. 802.11V

Answer: B

Explanation:
802.11mc is a standard that uses Round Trip Time (RTT) and Fine Time Measurements (FTM) to calculate the distance a client is from an AP. 802.11mc defines a protocol for exchanging FTM frames between an AP and a client, which contain timestamps that indicate when the frames were transmitted and received. By measuring the RTT of these frames, the AP or the client can estimate their distance based on the speed of light. The other options are incorrect because they either do not use RTT or FTM or do not exist as standards. References: https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

NEW QUESTION 43
DRAG DROP
Match the solution components of NetConductor (Options may be used more than once or not at all.)



Client Insights
Cloud Auth
The Fabric Wizard
Policy Manager

~~Built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network~~ blind spots

Defines user and device groups and creates the associated access enforcement rules for the physical network

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

Simplifies the creation of the overlays using an intuitive, graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways

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

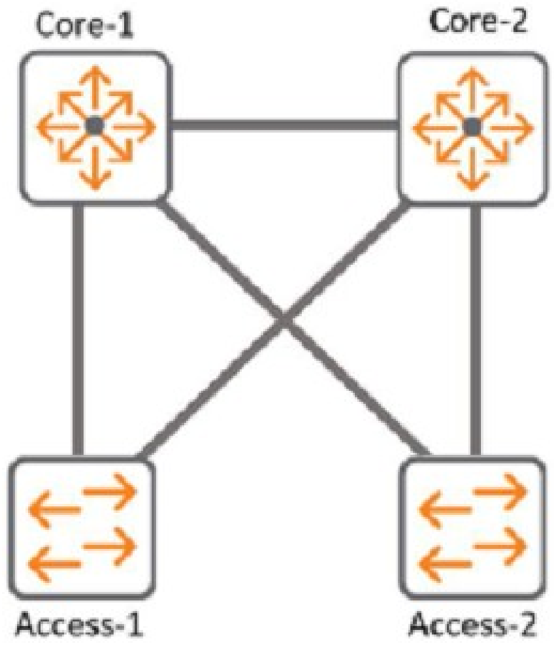
NEW QUESTION 47
you need to have different routing-table requirements With Aruba CX 6300 VSF configuration.
Assuming the correct layer-2 VLAN already exists, how would you create a new SVI for a separate routing table?

A. create a new VLAN, and attach the VRF to it.
B. Create a new routing table, and attach VLANS to it
C. Create a new SVI and use attach command.
D. Create a new VLA
E. and attach the routing table to it

Answer: C

Explanation:
The correct answer is C. Create a new SVI and use attach command.
To create a new SVI for a separate routing table, you need to use the attach command to associate the SVI with a VRF (Virtual Routing and Forwarding) instance. A VRF is a logical entity that allows multiple routing tables to coexist on the same switch. Each VRF has its own set of interfaces, routing protocols, and routes that are isolated from other VRFs. According to the AOS-CX Virtual Switching Framework (VSF) Guide1, one of the steps to configure VRF-aware VSF is:
? Configure the VRFs on each member switch and assign the SVIs to the respective
VRFs using the attach command. For example: switch(config)# vrf red
switch(config-vrf)# exit switch(config)# interface vlan 10
switch(config-if-vlan)# ip address 10.1.1.1/24 switch(config-if-vlan)# attach vrf red
The above commands create a VRF named red and assign VLAN 10 SVI to it. The SVI has an IP address of 10.1.1.1/24.
The other options are incorrect because:
? A. You cannot attach a VRF to a VLAN directly. You need to create an SVI for the VLAN and then attach the VRF to the SVI.
? B. You cannot create a new routing table manually. You need to create a VRF and then use routing protocols or static routes to populate the routing table for the VRF.
? D. You cannot attach a routing table to a VLAN directly. You need to create an SVI for the VLAN and then attach a VRF that has a routing table associated with it.

NEW QUESTION 49
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 mapppjng
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.

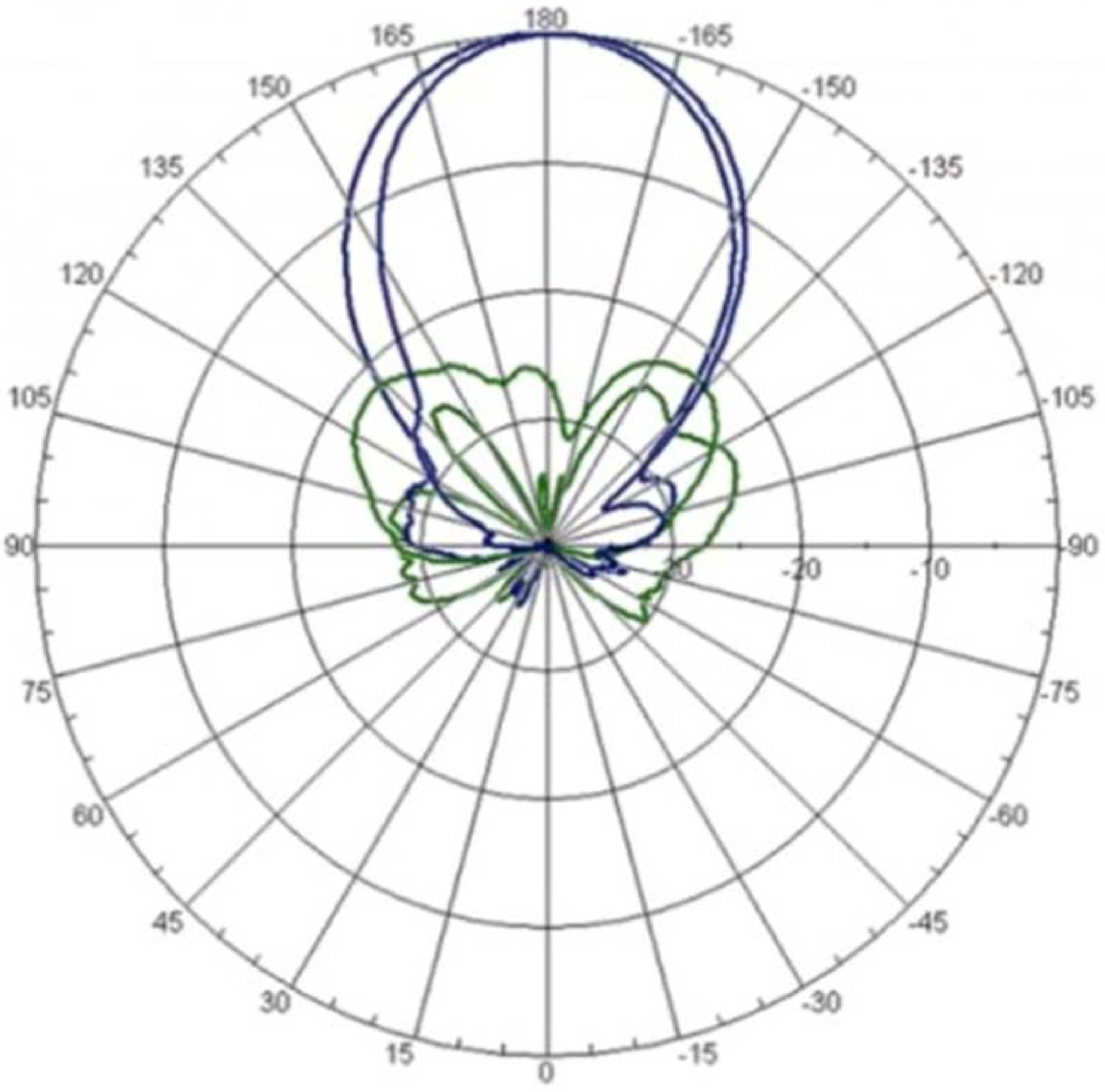
NEW QUESTION 50
A customer is concerned about me unprotected traffic between an AOS-CX switch and a gateway, running on AOStO. What is a feasible option to protect this traffic?

A. Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway
B. Implement an MD5 HMAC function lo 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 55
Refer to the image.



Horizontal Pattern

Your customer is complaining of weak Wi-Fi coverage in their office. They mention that the office on the other side of the hall has much better signal What is the likely cause of this issue7

A. The AP is a remote access point.
B. The AP is using a directional antenna.
C. The AP is an outdoor access point.
D. The AP is configured in Mesh mode

Answer: B

Explanation:
The likely cause of the issue of weak Wi-Fi coverage in the office is that the AP is using a directional antenna. A directional antenna is an antenna that radiates or receives radio waves more strongly in one or more directions, creating a focused beam of signal. A directional antenna can provide better coverage and performance for a specific area, but it can also create dead zones or weak spots for other areas. The other options are incorrect because they either do not affect the Wi-Fi coverage or do not match the scenario. 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/antennas.htm

NEW QUESTION 57
With the Aruba CX switch configuration, what is the Active Gateway feature that is used for and is unique to VSX configuration?

A. VRRP and Active gateway are mutually exclusive on a VLAN
B. VRID is set automatically as SVI vlan id
C. VRIDs need to be non-overlapping with VRRP
D. VRRP and Active Gateway can be configured on a single VLAN for interoperability

Answer: A

Explanation:
Active gateway is a first hop redundancy protocol that eliminates a single point of failure. The active gateway feature is used to increase the availability of the default gateway servicing hosts on the same subnet. An active gateway improves the reliability and performance of the host network by enabling a virtual router to

act as the default gateway for that network. If you have enabled active gateway, VRRP is not required3. Active gateway is similar to VRRP in that routed traffic from the VSX node is sourced from the switch interface MAC and not the virtual MAC address (VMAC). Each active gateway sends a periodic broadcast hello packet to avoid VMAC aging on the access switches. The switch views the active gateway IP as a self IP address3. Active gateway is preferable over VRRP because with VRRP traffic is still pushed over the ISL link, resulting in latency in the network3. Therefore, VRRP and active gateway are mutually exclusive on a VLAN, and answer A is correct.
References: 1: Aruba Campus Access documents and learning resources 3: Active gateway over VSX - Aruba

NEW QUESTION 58
Your manufacturing client is having installers deploy seventy headless scanners and fifty IP cameras in their warehouse These new devices do not support 802 1X authentication.
How can HPE Aruba reduce the IT administration overhead associated with this deployment while maintaining a secure environment using MPSK?

A. Have the installers generate keys with ClearPass Self Service Registration.
B. Have the MPSK gateway derive the unique pre-shared keys based on the MAC OUI.
C. Use MPSK Local to automatically provide unique pre-shared keys for devices.
D. MPSK Local will allow the cameras to share a key and the scanners to share a different key

Answer: C

Explanation:
MPSK Local is a feature that can reduce the IT administration overhead associated with deploying devices that do not support 802.1X authentication while maintaining a secure environment. MPSK Local allows the switch to automatically generate and assign unique pre-shared keys for devices based on their MAC addresses, without requiring any configuration on the devices or an external authentication server. The other options are incorrect because they either require manual intervention by the installers or the MPSK gateway, or they do not provide unique pre-shared keys for devices. References:
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01- ch05.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch06.html

NEW QUESTION 60
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 62
Which statements regarding 0SPFv2 route redistribution are true for Aruba OS CX switches? (Select two.)

A. The "redistribute connected" command will redistribute all connected routes for the switch including local loopback addresses
B. The "redistribute ospf" command will redistribute routes from all OSPF V2 and V3 processes
C. The "redistribute static route-map connected-routes" command will redistribute all static routes without a matching deny in the route map "connected-routes".
D. The "redistribute connected" command will redistribute all connected routes for the switch except local loopback addresses.
E. The "redistribute static route-map connected-routes" command will redistribute all static routes with a matching permit in the route map "connected-routes-

Answer: AE

Explanation:
These are two correct statements regarding OSPFv2 route redistribution for Aruba OS CX switches. Route redistribution is a process that allows routes from one routing protocol or source to be injected into another routing protocol or destination. OSPFv2 is a link-state routing protocol that supports route redistribution from various sources, such as connected, static, BGP, etc. The ??redistribute connected?? command will redistribute all connected routes for the switch, including local loopback addresses, into OSPFv2. The ??redistribute static route-map connected-routes?? command will redistribute all static routes that have a matching permit statement in the route map named ??connected- routes?? into OSPFv2. The other statements are incorrect because they either do not reflect the correct behavior of route redistribution commands or do not exist as valid commands. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html https://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch03.html

NEW QUESTION 65
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 70
What are two advantages of splitting a larger OSPF area into a number of smaller areas? (Select two)

A. It extends the LSDB
B. It increases stability
C. it simplifies the configuration.
D. It reduces processing overhead.
E. It reduces the total number of LSAs

Answer: BD

Explanation:
Splitting a larger OSPF area into a number of smaller areas has several advantages for network scalability and performance. Some of these advantages are:
? It increases stability by limiting the impact of topology changes within an area.
When a link or router fails in an area, only routers within that area need to run the SPF algorithm and update their routing tables. Routers in other areas are not affected by the change and do not need to recalculate their routes.
? It reduces processing overhead by reducing the size and frequency of link-state advertisements (LSAs). LSAs are packets that contain information about the network topology and are flooded within an area. By dividing a network into smaller areas, each area has fewer LSAs to generate, store, and process, which saves CPU and memory resources on routers.
? It reduces bandwidth consumption by reducing the amount of routing information exchanged between areas. Routers that connect different areas, called area border routers (ABRs), summarize the routing information from one area into a single LSA and advertise it to another area. This reduces the number of LSAs that need to be transmitted across area boundaries and saves network bandwidth.
References: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first- ospf/7039-1.html https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first- ospf/13703-8.html

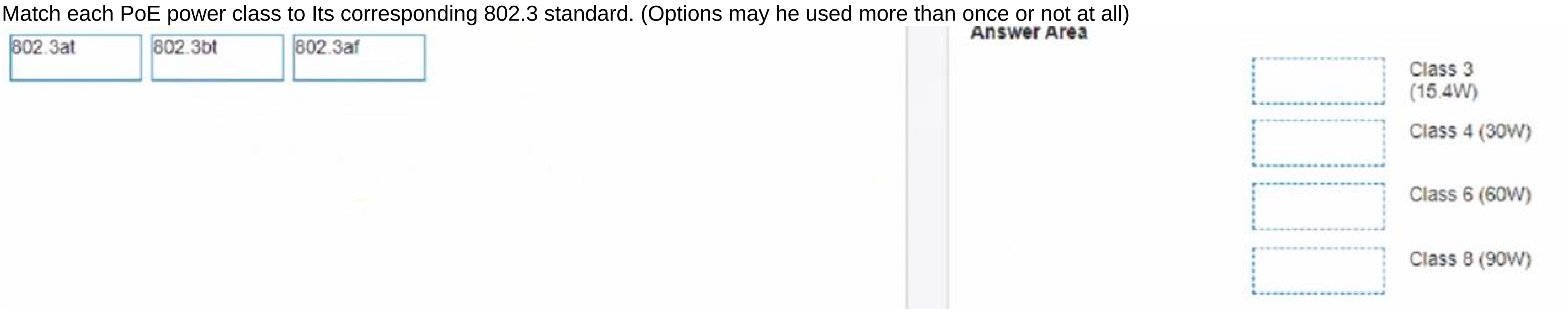
NEW QUESTION 73
Your customer has four (4) Aruba 7200 Series Gateways and two (2) 7000 Series Gateways. The customer wants to form a cluster with these Gateways. What design consideration would prevent you from using all of those Gateways?

A. Multiple versions between Gateways in the same cluster profile are not allowed AOS 10.x.
B. A heterogeneous cluster is not supported in AOS 10.x.
C. The AP load should be lowest value of worst-case scenario load.
D. A combination of 7200 series and 7000 series gateways supports up to 4 nodes

Answer: A

Explanation:
The reason is that AOS 10.x does not support clustering gateways with different versions in the same cluster profile. A cluster profile defines the configuration settings for a group of gateways that are managed by Aruba Central.
According to the Aruba documentation2, ??You can combine 7200 Series and 7000 Series gateways in the same cluster with a maximum size of four devices with reduced AP client capacity on 7000 Series gateways.??

NEW QUESTION 76
DRAG DROP
Match each PoE power class to Its corresponding 802.3 standard. (Options may he used more than once or not at all)



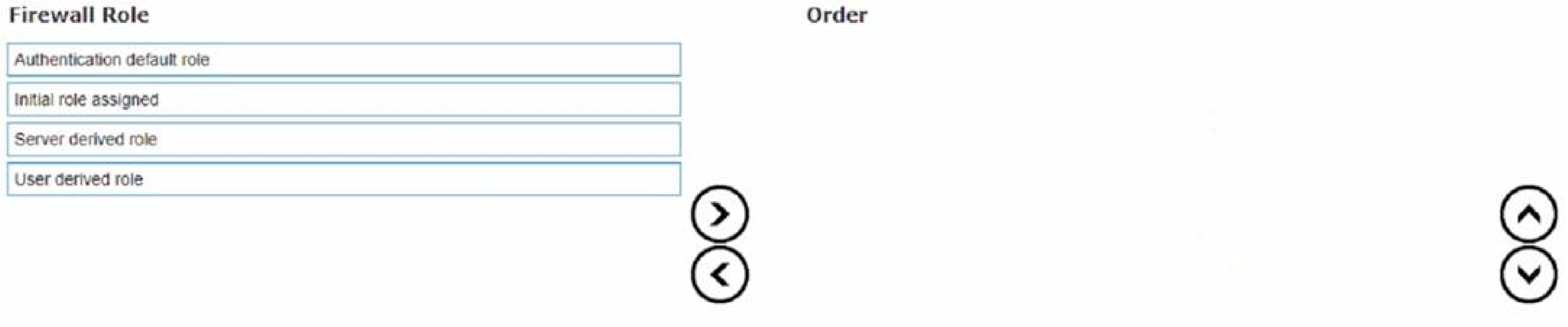
A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Class 3 (15.4W): 802.3af
? Class 4 (30W): 802.3at
? Class 6 (60W): 802.3bt
? Class 8 (90W): 802.3bt

NEW QUESTION 80

DRAG DROP
List the firewall role derivation flow in the correct order



Firewall Role

Authentication default role

Initial role assigned

Server derived role

User derived role

Order

A. Mastered
B. Not Mastered

Answer: A

Explanation:
According to the Aruba Documentation Portal1, the firewall role derivation flow in the correct order is:
? Server derived role
? User derived role
? Authentication default role
? Initiation role assigned

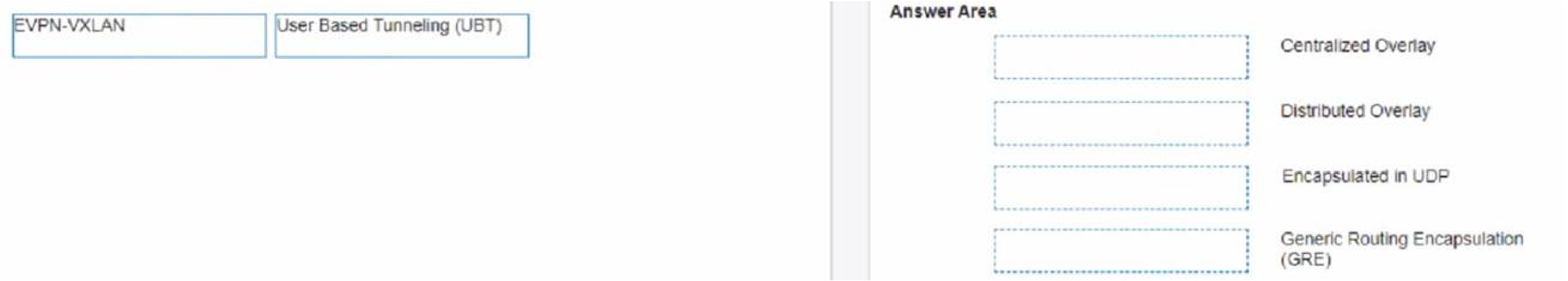
NEW QUESTION 84
you are implementing ClearPass Policy Manager with EAP-TLS for authenticating all corporate-owned devices.
What are two possible solutions to the problem of deploying client certificates to corporate MacBooks that are joined to a Windows domain? (Select two.)

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

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 85
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

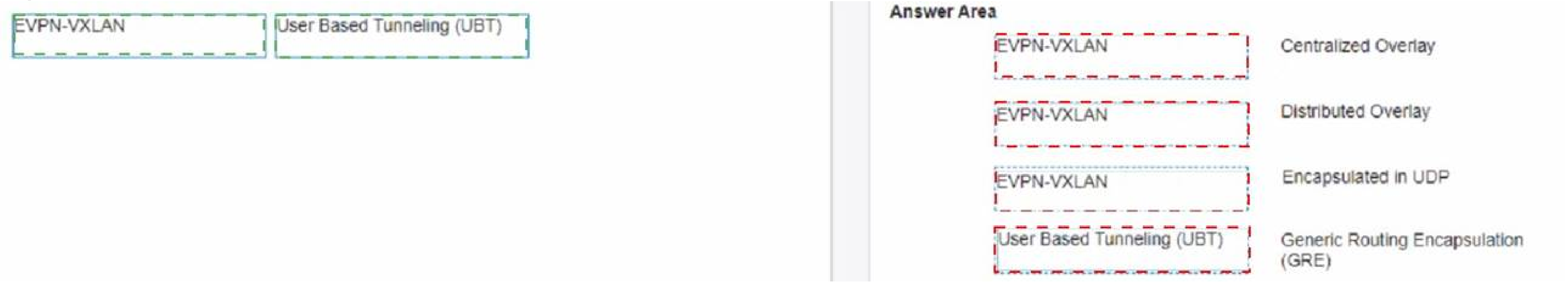
Encapsulated in UDP

Generic Routing Encapsulation (GRE)

A. Mastered
B. Not Mastered

Answer: A

Explanation:



EVPN-VXLAN

User Based Tunneling (UBT)

Answer Area

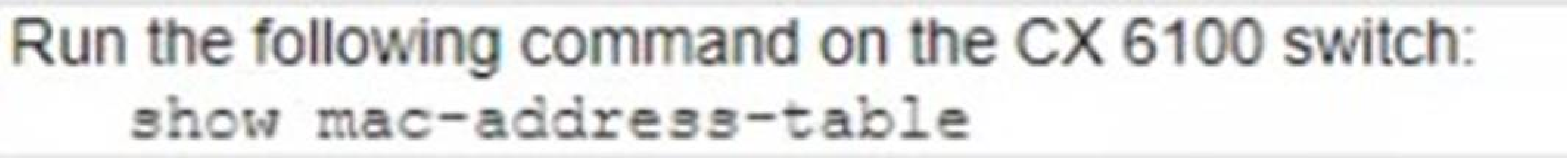
EVPN-VXLAN	Centralized Overlay
EVPN-VXLAN	Distributed Overlay
EVPN-VXLAN	Encapsulated in UDP
User Based Tunneling (UBT)	Generic Routing Encapsulation (GRE)

NEW QUESTION 89

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

The client device is connected to an Aruba CX 6100 switch by VSX LAG. Which action can be used to find the IP address successfully?

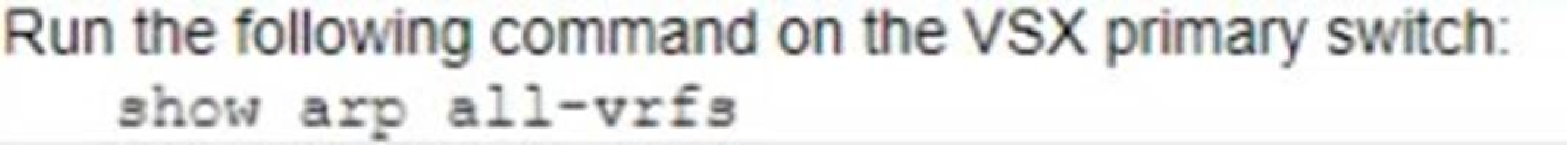
A)



Run the following command on the CX 6100 switch:

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

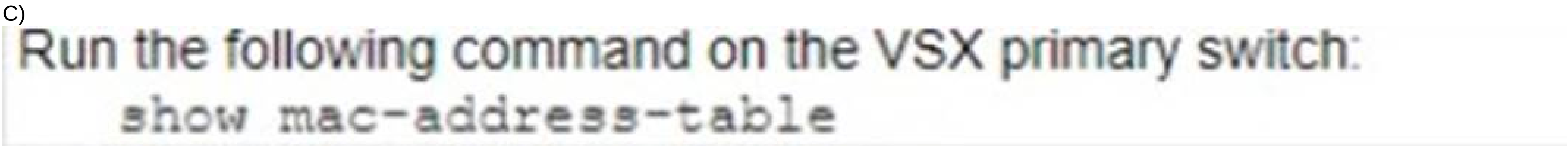
B)



Run the following command on the VSX primary switch:

```
show arp all-vrfs
```

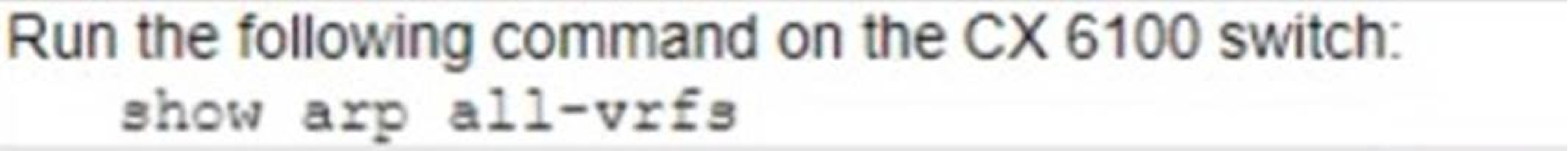
C)



Run the following command on the VSX primary switch:

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

D)



Run the following command on the CX 6100 switch:

```
show arp all-vrfs
```

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

Answer: B

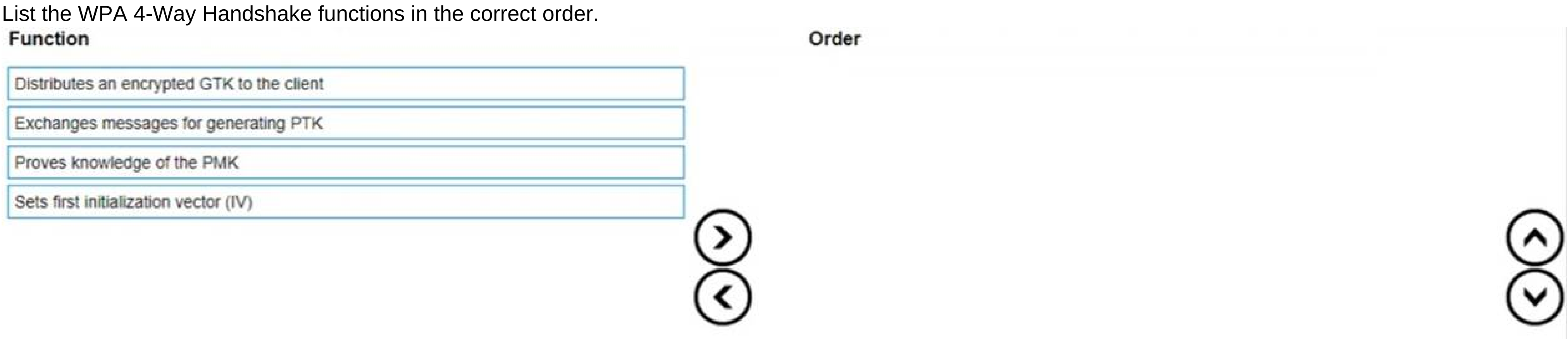
Explanation:

The show arp command displays the ARP table for a specific VRF or all VRFs on the switch. The ARP table contains the IP address to MAC address mappings for hosts that are directly connected to the switch or reachable through a gateway. If the client device is connected to another switch by VSX LAG, the ARP entry for the client device will not be present on the primary switch unless it has communicated with it recently. Therefore, to find the IP address of the client device, the administrator should run the show arp command on the secondary switch in the VSX pair, specifying the VRF name that contains the client device??s subnet.
References: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

NEW QUESTION 92

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

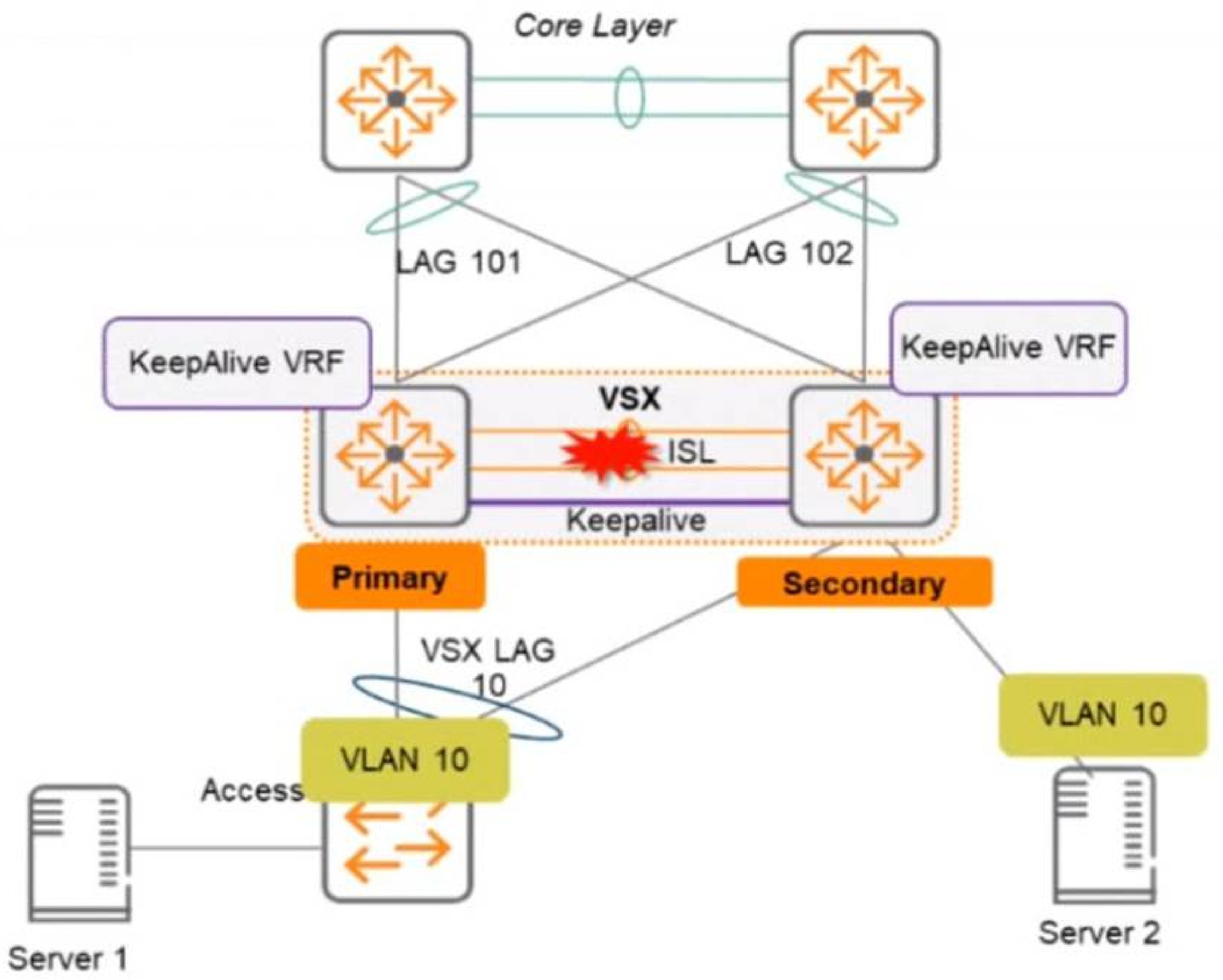
Answer: A

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 96

Two AOS-CX switches are configured with VSX at the the Access-Aggregation layer where servers attach to them An SVI interface is configured for VLAN 10 and serves as the default gateway for VLAN 10. The ISL link between the switches fails, but the keepalive interface functions. Active gateway has been configured on the VSX switches.



What is correct about access from the servers to the Core? (Select two.)

A. Server 1 can access the core layer via the keepalrve link
B. Server 2 can access the core layer via the keepalive link
C. Server 2 cannot access the core layer.
D. Server 1 can access the core layer via both uplinks
E. Server 1 and Server 2 can communicate with each other via the core layer
F. Server 1 can access the core layer on only one uplink

Answer: DE

Explanation:
These are the correct statements about access from the servers to the Core when the ISL link between the switches fails, but the keepalive interface functions. Server 1 can access the core layer via both uplinks because it is connected to VSX-A, which is still active for VLAN 10. Server 2 can also access the core layer via its uplink to VSX-B, which is still active for VLAN 10 because of Active Gateway feature. Server 1 and Server 2 can communicate with each other via the core layer because they are in the same VLAN and subnet, and their traffic can be routed through the core switches. The other statements are incorrect because they either describe scenarios that are not possible or not relevant to the question. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-

NEW QUESTION 100
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 104
Which method is used to onboard a new UXI in an existing environment with 802 1X authentication? (The sensor has no cellular connection)

A. Use the UXI app on your smartphone and connect the UXI via Bluetooth
B. Use the Aruba installer app on your smartphone to scan the barcode
C. Connect the new UXI from an already installed one and adjust the initial configuration.
D. Use the CLI via the serial cable and adjust the initial configuration.

Answer: A

Explanation:
To onboard a new UXI in an existing environment with 802.1X authentication, you need to use the UXI app on your smartphone and connect the UXI via Bluetooth. The UXI app allows you to scan the QR code on the UXI sensor and configure its network settings, such as SSID, password, IP address, etc. The Bluetooth connection allows you to communicate with the UXI sensor without requiring any network access or cellular connection. The other options are incorrect because they either do not use the UXI app or do not use Bluetooth. References: https://www.arubanetworks.com/products/network-management-operations/analytics-monitoring/user-experience-insight-sensors/ https://help.centralon-prem.arubanetworks.com/2.5.4/documentation/online_help/content/nms-on-prem/aos- cx/get-started/uxi-sensor.htm

NEW QUESTION 108
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 113
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 116
your customer has asked you to assign a switch management role for a new user The customer requires the user role to View switch configuration information and have access to the PUT and POST meth0ds for REST API.
Which default AOS-CX user role meets these requirements?

A. administrators
B. auditors
C. sysops
D. helpdesk

Answer: C

Explanation:
The correct answer is C. sysops.
The sysops user role is a predefined role that allows users to view switch configuration information and have access to the PUT and POST methods for REST API. The sysops user role can also use the PATCH and DELETE methods for REST API, but not for all resources. The sysops user role is suitable for users who need to perform system operations on the switch, such as backup, restore, upgrade, or reboot.
According to the AOS-CX REST API Reference basics1, one of the predefined user roles is:
? sysops: Users with this role can view switch configuration information and have access to the PUT and POST methods for REST API. They can also use the PATCH and DELETE methods for REST API, but not for all resources. Users with this role can perform system operations on the switch, such as backup, restore, upgrade, or reboot.
The other options are incorrect because:
? A. administrators: Users with this role have full access to all switch configuration information and all REST API methods. This role is more than what the customer requires.
? B. auditors: Users with this role can only view switch configuration information and have access to the GET method for REST API. They cannot use the PUT and POST methods for REST API.
? D. helpdesk: Users with this role can view switch configuration information and have access to the GET method for REST API. They can also use the PATCH method for REST API, but only for a limited set of resources. They cannot use the PUT and POST methods for REST API.

NEW QUESTION 120

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 125
A customer wants to deploy a Gateway and take advantage of all the SD-WAN features. Which persona role option should be selected?

A. ArubaOS 10 Branch
B. ArubaOS 10 VPN Concentrator
C. ArubaOS 10 Wireless
D. ArubaOS 10 Mobility

Answer: A

Explanation:
The persona role option that should be selected to deploy a Gateway and take advantage of all the SD-WAN features is A. ArubaOS 10 Branch.
ArubaOS 10 Branch is a persona that enables the Gateway to provide both LAN and WAN functionality for branch networks. The Gateway can act as a wireless controller, a router, a firewall, and an SD-WAN device. The SD-WAN features include route and tunnel orchestration, dynamic path steering, forward error correction, SaaS traffic optimization, SASE orchestration, and more1.
The other options are incorrect because:
? B. ArubaOS 10 VPN Concentrator: This is a persona that enables the Gateway to act as a VPN concentrator for remote access or site-to-site VPN connections. It does not provide SD-WAN features2.
? C. ArubaOS 10 Wireless: This is a persona that enables the Gateway to act as a wireless controller for campus networks. It does not provide SD-WAN features3.
? D. ArubaOS 10 Mobility: This is a persona that enables the Gateway to act as a mobility controller for campus networks. It does not provide SD-WAN features.

NEW QUESTION 128
A network administrator is attempting to troubleshoot a connectivity issue between a group of users and a particular server The administrator needs to examine the packets over a period of time from their desktop; however, the administrator is not directly connected to the AOS-CX switch involved with the traffic flow.
What statements are correct regarding the ERSPAN session that needs to be established on an AOS-CX switch'? (Select two)

A. On the source AOS-CX switch, the destination specified is the switch to which the administrator's desktop is connected
B. The encapsulation protocol used is GRE.
C. The encapsulation protocol used is VXLAN.
D. The encapsulation protocol is UDP.
E. On the source AOS-CX switch, the destination specified is the administrators desktop

Answer: BE

Explanation:
These are the correct statements regarding the ERSPAN session that needs to be established on an AOS-CX switch for a network administrator to examine the packets over a period of time from their desktop. ERSPAN (Encapsulated Remote Switched Port Analyzer) is a feature that allows an AOS-CX switch to mirror traffic from one or more source ports or VLANs to a remote destination IP address over a GRE (Generic Routing Encapsulation) tunnel. The destination IP address must be the IP address of the administrator??s desktop, which must have a packet capture tool installed to receive and analyze the mirrored traffic. The encapsulation protocol used for ERSPAN is GRE, which adds a header to the mirrored packets with information such as source and destination IP addresses, session ID, etc. The other statements are incorrect because they either do not specify the correct destination IP address or do not use ERSPAN or GRE.
References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch02.html https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6728/bk01-ch03.html

NEW QUESTION 132
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

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 133
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/

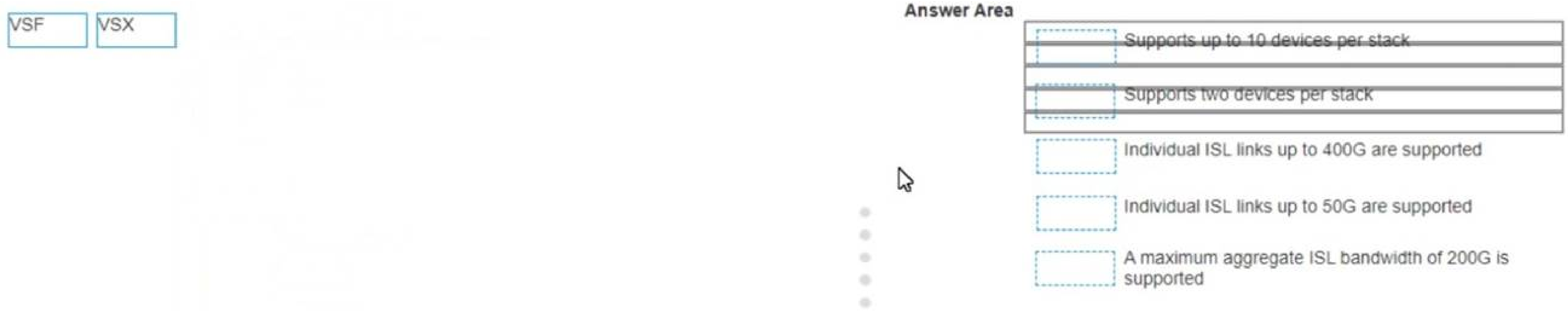
NEW QUESTION 137
Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements After the configuration was complete, it was noted that a user assigned with the administrators role did not have the appropriate level of access on the 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 142
DRAG DROP
Select the Aruba stacking technology matching each option (Options may be used more than once or not at all.)



VSF VSX

Answer Area

Supports up to 10 devices per stack

Supports two devices per stack

Individual ISL links up to 400G are supported

Individual ISL links up to 50G are supported

A maximum aggregate ISL bandwidth of 200G is supported

A. Mastered
B. Not Mastered

Answer: A

Explanation:
a) Support up to 10 devices per stack -> VSF
b) Support two devices per stack -> VSX
c) Individual ISL links up to 400G are supported -> VSX
d) individual ISL links up to 50G are supported -> VSF
e) A maximum aggregate ISL bandwidth of 200G is supported -> VSF
References: 1 https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/GUID-2E425DAE-EC54-4313-9DEA-A61817F903C0.html

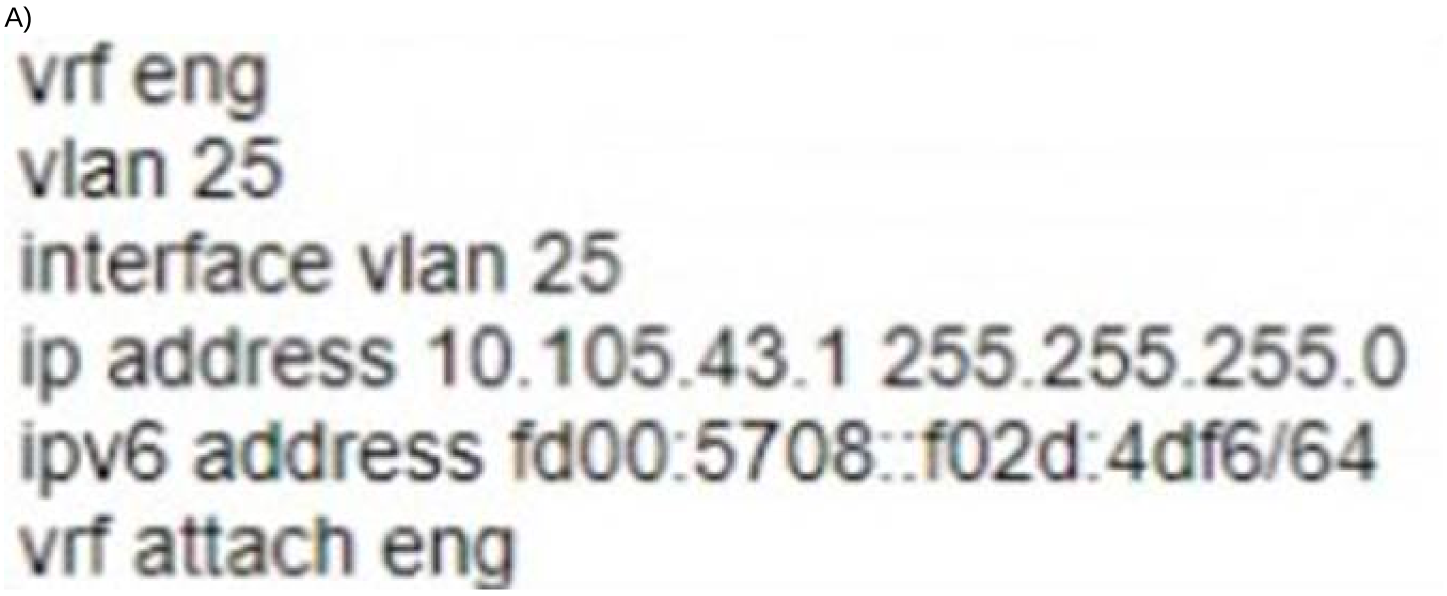
NEW QUESTION 146
Which Aruba AP mode is sending captured RF data to Aruba Central for waterfall plot?

A. Hybrid Mode
B. Air Monitor
C. Spectrum Monitor
D. Dual Mode

Answer: C

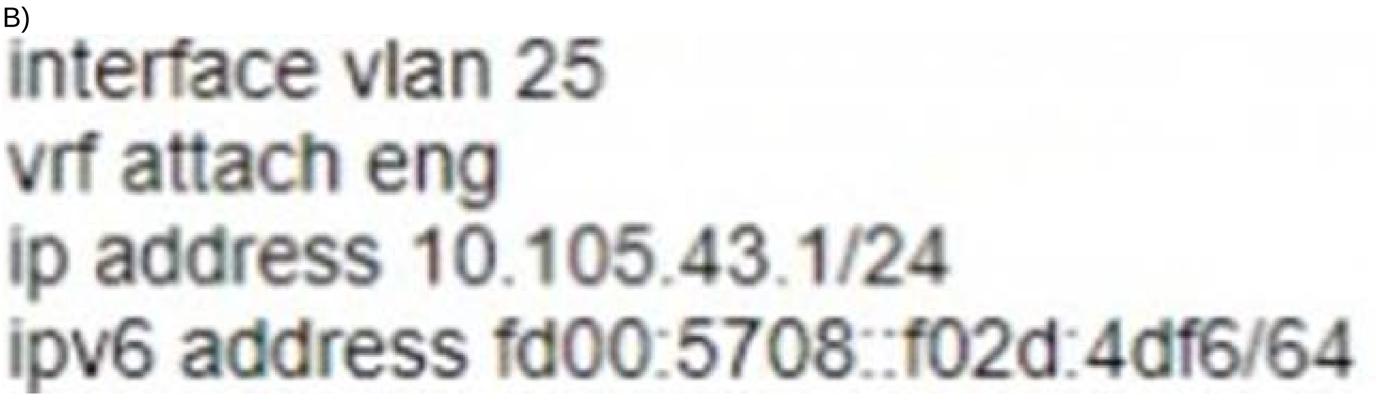
Explanation:
Spectrum Monitor is an Aruba AP mode that is sending captured RF data to Aruba Central for waterfall plot. Spectrum Monitor is a mode that allows an AP to scan all channels in both 2.4 GHz and 5 GHz bands and collect information about the RF environment, such as interference sources, noise floor, channel utilization, etc. The AP then sends this data to Aruba Central, which is a cloud-based network management platform that can display the data in various formats, including waterfall plot. Waterfall plot is a graphical representation of the RF spectrum over time, showing the frequency, amplitude, and duration of RF signals.
The other options are incorrect because they are either not AP modes or not sending RF data to Aruba Central. References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/spectrum_monitor.htm
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/waterfall_plot.htm
https://www.arubanetworks.com/products/network-management-operations/aruba-central/

NEW QUESTION 149
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)



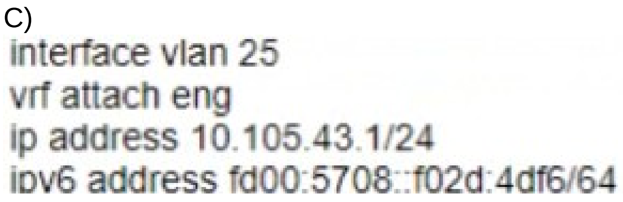
```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43.1 255.255.255.0
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

B)



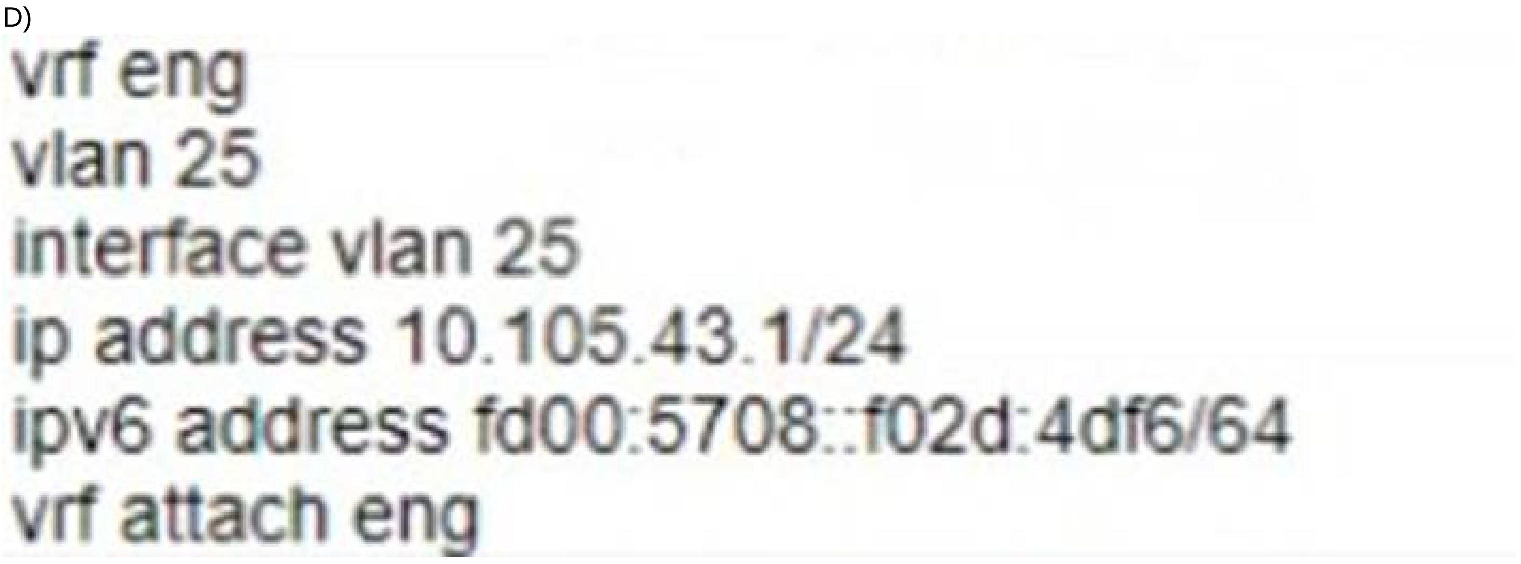
```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
```

C)



```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipv6 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 151

......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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