Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam

https://www.2passeasy.com/dumps/HPE7-A01/

NEW QUESTION 1
The customer needs a network hardware refresh to replace an aging Aruba 5406R core switch pair using spanning tree configuration with Aruba CX 8360-32YC switches What is the benefit of VSX clustering with the new solution?

A. stacked data-plane
B. faster MSTP converge processing
C. dual Aruba AP LAN port connectivity for PoE redundancy
D. dual control plane provides better resiliency

Answer: D

Explanation:
VSX clustering is a feature that allows two Aruba CX switches to operate as a single logical device, providing high availability, scalability, and simplified management. VSX clustering has several benefits over spanning tree configuration, such as:
? Dual control plane provides better resiliency. Unlike stacking, where switches share a single control plane, VSX switches have independent control planes that synchronize their states over an inter-switch link (ISL). This means that if one switch fails or reboots, the other switch can continue to operate without affecting traffic flows or network services.
? Active-active forwarding provides better performance. Unlike spanning tree, where some links are blocked to prevent loops, VSX switches use all available links for forwarding traffic, providing load balancing and increased bandwidth utilization.
? Multichassis LAG provides better redundancy. Unlike single-chassis LAG, where all member ports belong to one switch, VSX switches can form multichassis LAGs with downstream or upstream devices, where member ports are distributed across both switches. This provides link redundancy and seamless failover in case of switch or port failure.
References: https://www.arubanetworks.com/assets/tg/TG_VSX.pdf

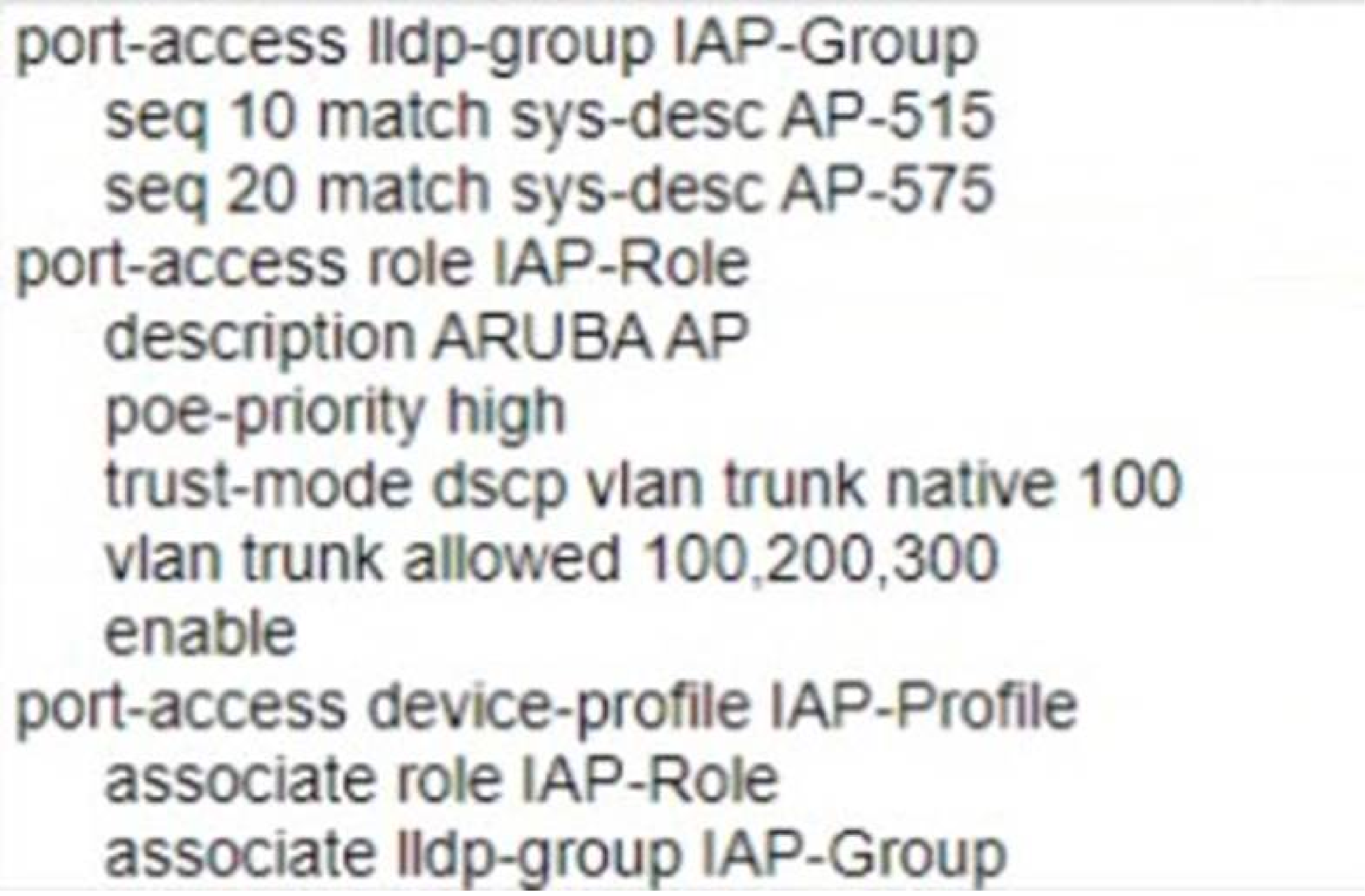
NEW QUESTION 2
What is true regarding 802.11k?

A. It extends radio measurements to define mechanisms for wireless network management of stations
B. It reduces roaming delay by pre-authenticating clients with multiple target APs before a client roams to an AP
C. It provides mechanisms for APs and clients to dynamically measure the available radio resources.
D. It considers several metrics before it determines if a client should be steered to the 5GHz band, including client RSSI

Answer: C

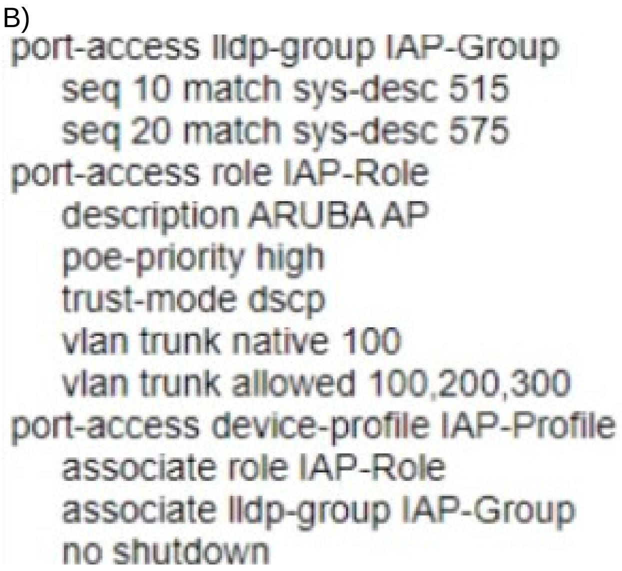
Explanation:
802.11k is a standard that provides mechanisms for APs and clients to dynamically measure the available radio resources in a wireless network. 802.11k defines radio resource management (RRM) functions, such as neighbor reports, link measurement, beacon reports, etc., that allow APs and clients to exchange information about the RF environment and make better roaming decisions. The other options are incorrect because they describe other standards, such as 802.11r, 802.11v, or 802.11ax. References: https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

NEW QUESTION 3
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 theAPs 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)



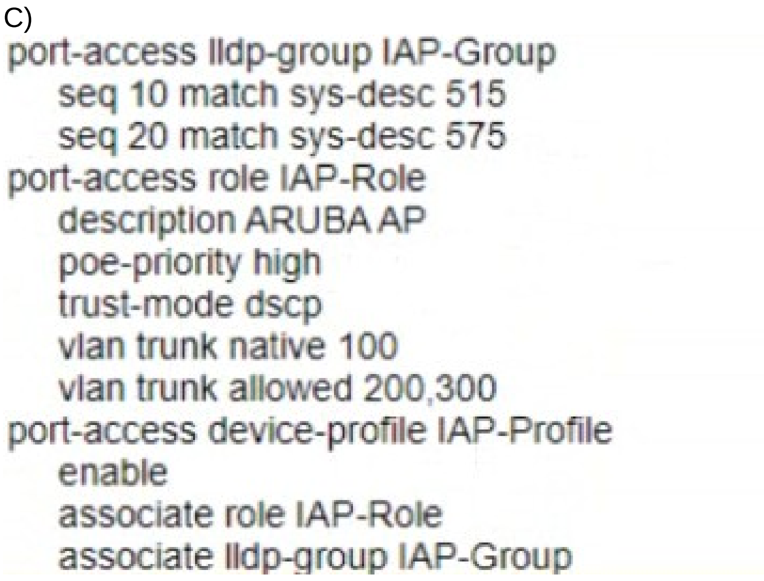
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc AP-515
    seq 20 match sys-desc AP-575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp vlan trunk native 100
    vlan trunk allowed 100,200,300
    enable
port-access device-profile IAP-Profile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

B)



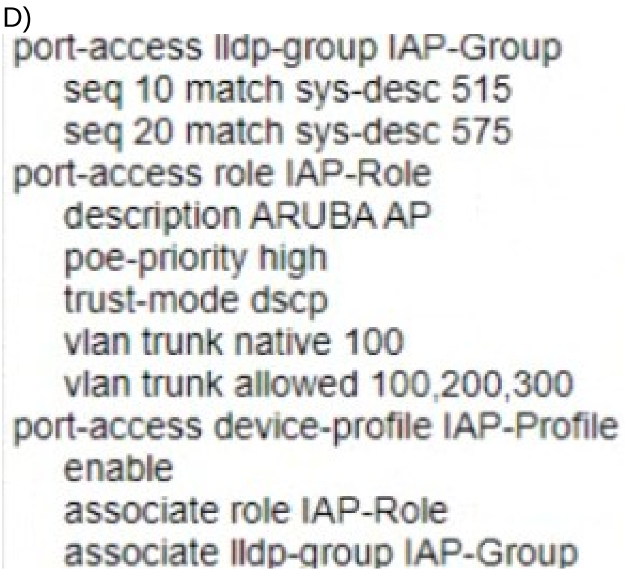
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    associate 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 4
A customer wants to provide wired security as close to the source as possible The wired security must meet the following requirements:
-allow ping from the IT management VLAN to the user VLAN
-deny ping sourcing from the user VLAN to the IT management VLAN
The customer is using Aruba CX 6300s
What is the correct way to implement these requirements?

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

Answer: C

Explanation:
An inbound ACL is applied to traffic entering a port or VLAN. An outbound ACL is applied to traffic leaving a port or VLAN4. To deny ping sourcing from the user VLAN to the IT management VLAN, an inbound ACL on the user VLAN should be used to filter icmp echo traffic toward the IT management VLAN. Icmp echo-

reply traffic is not needed to be allowed because it is already permitted by default5. References: 4 https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html 5 https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-0C3A9D0F-6E5B-4E1A-AF3C-8D8B2F9C1A7B.html

NEW QUESTION 5
What steps are part of the Key Management workflow when a wireless device is roaming from AP1 to AP2? (Select two.)

A. AP1 will cache the client's information and send it to the Key Management service
B. The Key Management service receives from AirMatch a list of all AP2's neighbors
C. The Key Management service receives a list of all AP1 s neighbors from AirMatch.
D. The Key Management service then generates R1 keys for AP2's neighbors.
E. A client associates and authenticates with the AP2 after roaming from AP1

Answer: AD

Explanation:
The correct steps that are part of the Key Management workflow when a wireless device is roaming from AP1 to AP2 are A and D.
* A. AP1 will cache the client??s information and send it to the Key Management service. This is true because when a client associates and authenticates with AP1, AP1 will generate a pairwise master key (PMK) for the client and store it in its cache. AP1 will also send the PMK and other client information, such as MAC address, VLAN, and SSID, to the Key Management service, which is a centralized service that runs on Aruba Mobility Controllers (MCs) or Mobility Master (MM) devices1. The Key Management service will use this information to facilitate fast roaming for the client.
* D. The Key Management service then generates R1 keys for AP2??s neighbors. This is true because when the Key Management service receives the client information from AP1, it will use the PMK to derive R0 and R1 keys for the client. R0 keys are used to generate R1 keys, which are used to generate pairwise transient keys (PTKs) for encryption. The Key Management service will distribute the R1 keys to AP2 and its neighboring APs, which are determined by AirMatch based on RF proximity2. This way, when the client roams to AP2 or any of its neighbors, it can skip the 802.1X authentication and use the R1 key to quickly generate a PTK with the new AP3.
* B. The Key Management service receives from AirMatch a list of all AP2??s neighbors. This is false because the Key Management service does not receive this information from AirMatch directly. AirMatch is a feature that runs on MCs or MM devices and optimizes the RF performance of Aruba devices by using machine learning algorithms. AirMatch periodically sends neighbor reports to all APs, which contain information about their nearby APs based on signal strength and interference. The APs then send these reports to the Key Management service, which uses them to determine which APs should receive R1 keys for a given client2.
* C. The Key Management service receives a list of all AP1 s neighbors from AirMatch. This is false for the same reason as B. The Key Management service does not receive this information from AirMatch directly, but from the APs that send their neighbor reports.
* E. A client associates and authenticates with the AP2 after roaming from AP1. This is false because a client does not need to authenticate with AP2 after roaming from AP1 if it has already authenticated with AP1 and received R1 keys from the Key Management service. The client only needs to associate with AP2 and perform a four-way handshake using the R1 key to generate a PTK for encryption3. This is called fast roaming or 802.11r roaming, and it reduces the latency and disruption caused by full authentication.
1: ArubaOS 8.7 User Guide 2: ArubaOS 8.7 User Guide 3: ArubaOS 8.7 User Guide : ArubaOS 8.7 User Guide

NEW QUESTION 6
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 7
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 8
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 9
Your customer is having connectivity issues with a newly-deployed Microbranch group The access points in this group are online in Aruba Central, but no VPN tunnels are forming.
What is the most likely cause of this issue?

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

Answer: C

Explanation:
This is the most likely cause of the issue where the access points in a Microbranch group are online in Aruba Central, but no VPN tunnels are forming. A Microbranch group is a group that contains both APs and Gateways and allows them to form VPN tunnels for secure communication. The VPN tunnels use GRE (Generic Routing Encapsulation) as the encapsulation protocol and IPSec as the encryption protocol. If there is a firewall blocking GRE traffic between the AP and the gateway, the VPN tunnels cannot be established. The other options are incorrect because they either do not affect the VPN tunnel formation or do not apply to a Microbranch group. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/gateways/microbranch.htm https://www.arubanetworks.com/assets/tg/TB_ArubaGateway.pdf

NEW QUESTION 10
A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working to a remote site connected via layer-3 All legacy devices are connected to a dedicated Aruba CX 6200 switch at each site.
What technology on the Aruba CX 6200 could be used to meet this requirement?

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

Answer: A

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

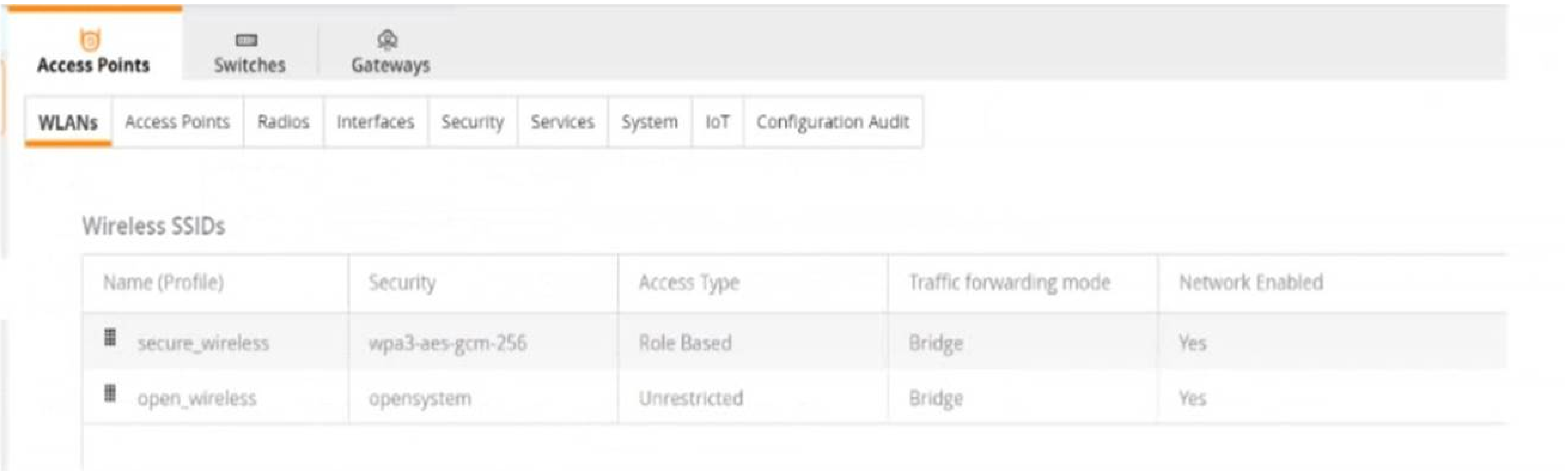
NEW QUESTION 10
A network engineer recently identified that a wired device connected to a CX Switch is misbehaving on the network To address this issue, a new ClearPass policy has been put in place to prevent this device from connecting to the network again.
Which steps need to be implemented to allow 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 12
Refer to the 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

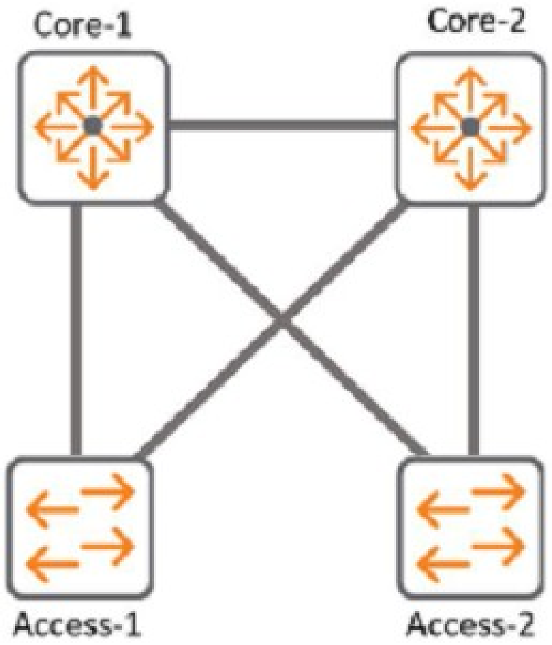
A company has deployed 200 AP-635 access points. To but is not working as expected What would be the correct action to fix the issue?

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 16
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 21
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 24
You are working on a network where the customer has a dedicated router with redundant Internet connections Tor outbound high-importance real-time audio streams from their datacenter All of this traffic.
• originates from a single subnet
• uses a unique range of UDP ports
• is required to be routed to the dedicated router
All other traffic should route normally The SVI for the subnet containing the servers originating the traffic is located on the core routing switch in the datacenter What should be configured?

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

Answer: C

Explanation:
The reason is that PBR allows you to route packets based on policies that match certain criteria, such as source or destination IP addresses, ports, protocols, etc. PBR can also be used to set metrics, next-hop addresses, or tag traffic for different routes.

NEW QUESTION 26
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 29
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 33
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 34
A customer wants to enable wired authentication across all their CX switches One of the requirements is that the switch must be able to authenticate a single computer connected through a VoIP phone.
Which feature should be enabled to support this requirement?

A. Multi-Domain Authentication
B. Device-Based Mode
C. MAC Authentication
D. Multi-Auth Mode

Answer: A

Explanation:
Multi-Domain Authentication is the feature that should be enabled to support the requirement that the switch must be able to authenticate a single computer connected through a VoIP phone. Multi-Domain Authentication is a feature that allows an Aruba CX switch to apply different authentication methods and policies to different devices connected to the same port. For example, a VoIP phone and a computer can be connected to the same port using a single cable, but they can be authenticated separately using different credentials and assigned to different VLANs. The other options are incorrect because they either do not support multiple devices on the same port or do not provide authentication.
References: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-7D9E9F6E-5C2A-4F7E-BE6D-A2C3A6C7B9F9.html
https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

NEW QUESTION 35
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.??

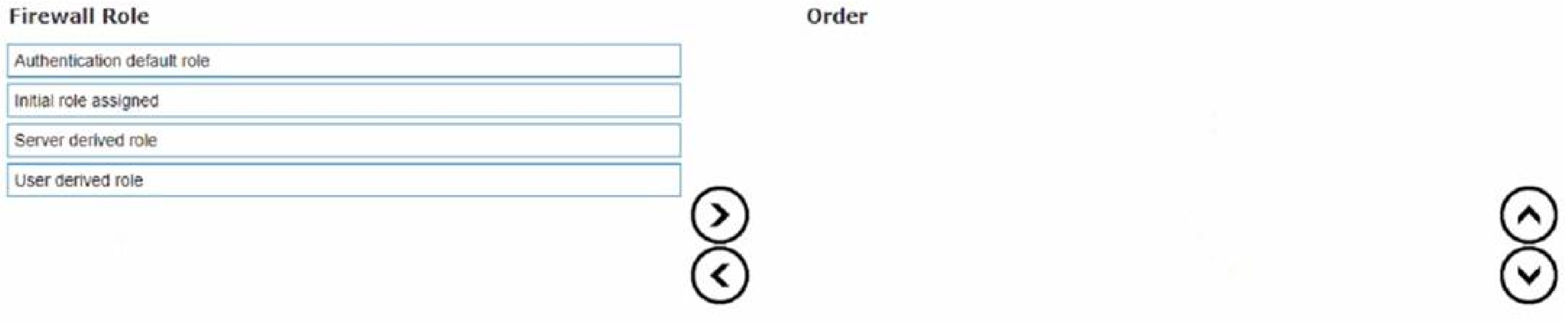
NEW QUESTION 36
What is enabled by LLDP-MED? (Select two.)

A. Voice VLANs can be automatically configured for VoIP phones
B. APs can request power as needed from PoE-enabled switch ports
C. iSCSl client devices can request to have flow control enabled
D. GVRP VLAN information can be used to dynamically add VLANs to a trunk
E. iSCSl client devices can set the required MTU setting for the port.

Answer: AB

Explanation:
These are two benefits enabled by LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery). LLDP-MED is an extension of LLDP that provides additional capabilities for network devices such as VoIP phones and APs. One of the capabilities is to automatically configure voice VLANs for VoIP phones, which allows them to be placed in a separate VLAN from data devices and receive QoS and security policies. Another capability is to request power as needed from PoE-enabled switch ports, which allows APs to adjust their power consumption and performance based on the available power budget. The other options are incorrect because they are either not enabled by LLDP-MED or not related to LLDP-MED. References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-qos/lldp-med.htm
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/poe.htm

NEW QUESTION 37
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 42
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.

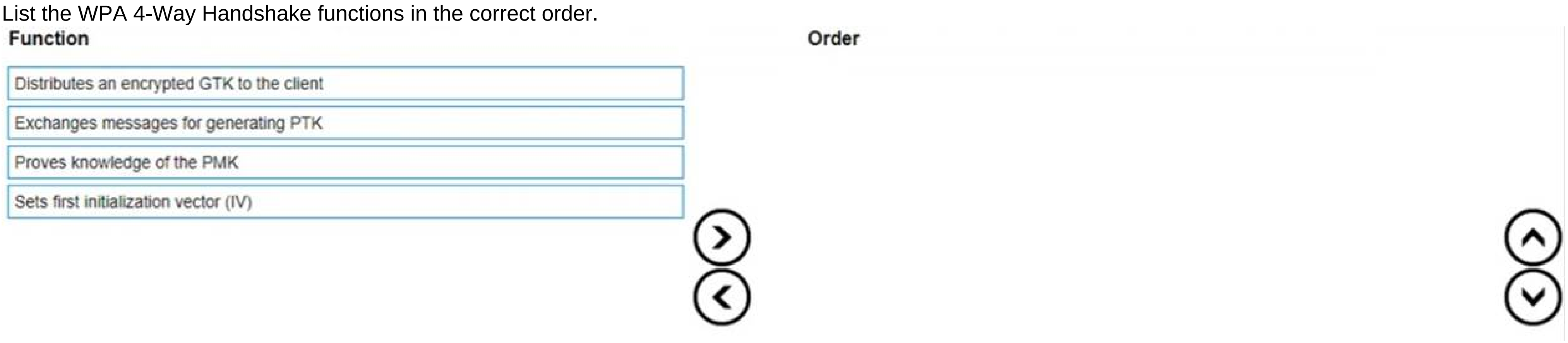
NEW QUESTION 45
You are building a configuration in Central that will be used for a standardized network design for small sites for your company, you want to use GUI configuration for gateways and Aps, while template configuration for switches. You need to align with Aruba best practices.
Which set of actions will satisfy these requirements?

A. Create one group in Central for switches a second group for AP
B. and a third group for gateways Create a unique site for each location, and assign devices to the appropriate site.
C. Create one group in Central for switches and a second group for APs and gateway
D. Create a unique site for each location, and assign devices to the appropriate site.
E. Create a single group in Centra
F. Create a unique site for each location, and assign devices to the appropriate site.
G. Create a single group in Centra
H. Create a unique site for each type of device, and assign devices to the appropriate site.

Answer: C

Explanation:
This is because option C shows how to create a single group in Central with different configuration methods defined for each device type. For example, you can create a group with the name Group1, and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (Group1). If a device type in the group is marked for template-based configuration method, the group name is prefixed with TG (TG Group1). You can use Group1 as the group ID for workflows such as user management, monitoring, reports, and audit trail2.
https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/abt- groups.htm 2:
https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/groups.htm

NEW QUESTION 49
DRAG DROP
List the WPA 4-Way Handshake functions in the correct order.



Function

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

Order

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 54
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 57
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 59
......