HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam

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

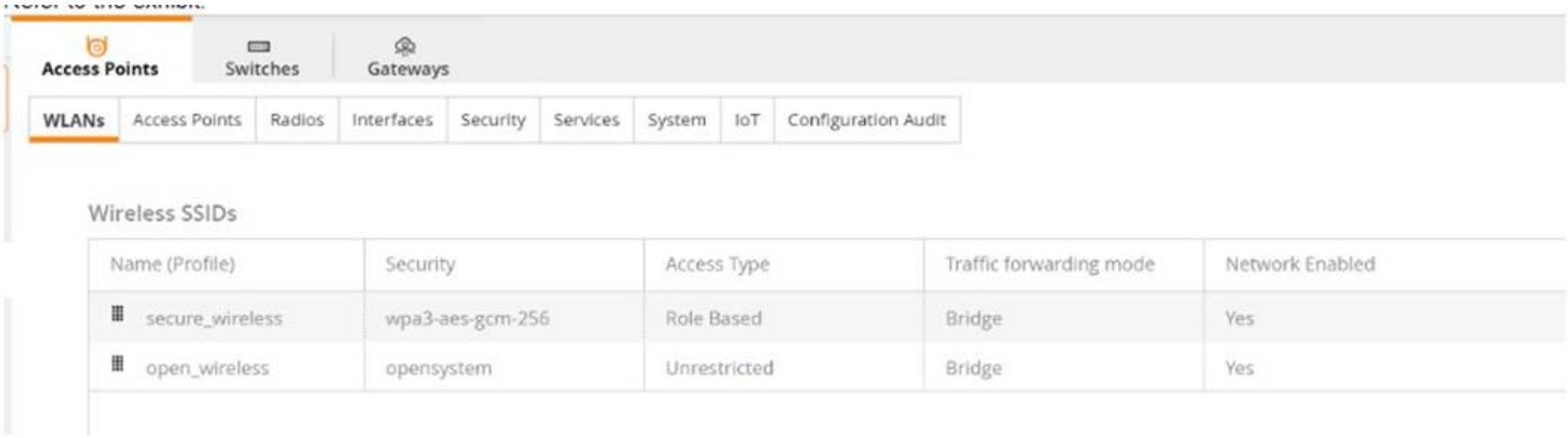
NEW QUESTION 2
How is Multicast Transmission Optimization implemented in an HPE Aruba wireless network?

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

Answer: D

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

NEW QUESTION 3
Refer to Exhibit:



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?

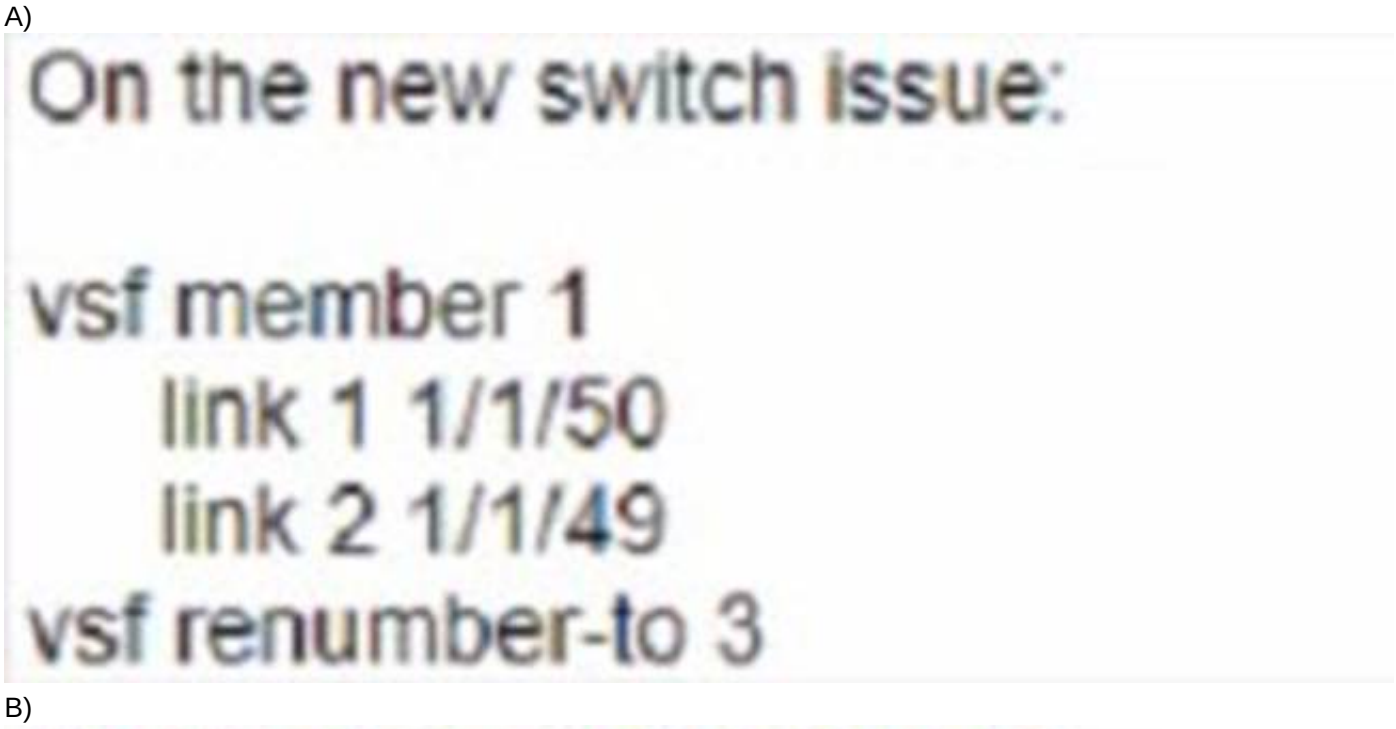
A. Change the SSID to WPA3-Enterprise (CNSA).
B. Change the SSID to WPA3-Personal.
C. Change the SSID to WPA3-Enhanced Open.
D. Change the SSID to WPA3-Enterprise (CCM).

Answer: C

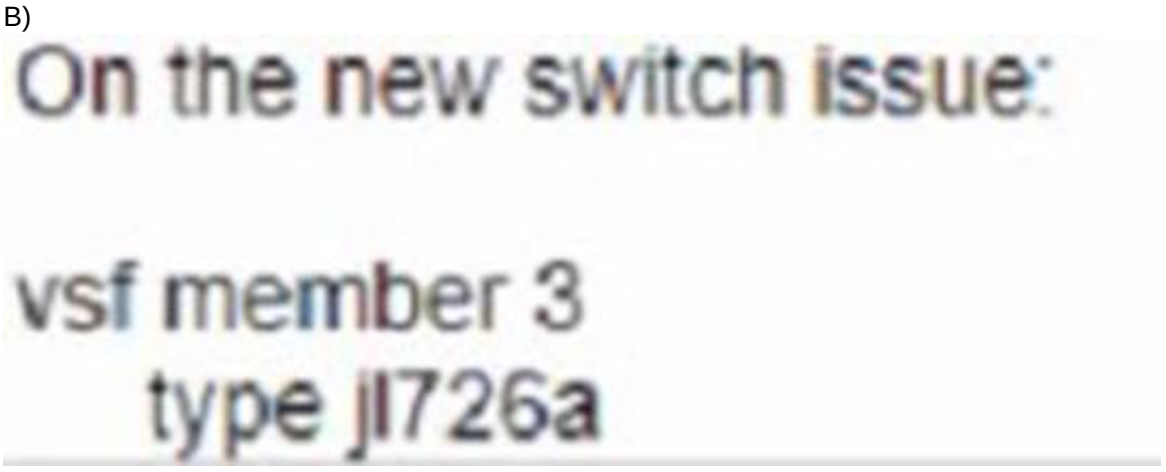
Explanation:
The correct action to fix the issue is C. Change the SSID to WPA3-Enhanced Open.
WPA3-OWE is not a valid SSID type in Central. OWE stands for Opportunistic Wireless Encryption, and it is a feature that provides encryption for open networks without requiring authentication. OWE is also known 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.

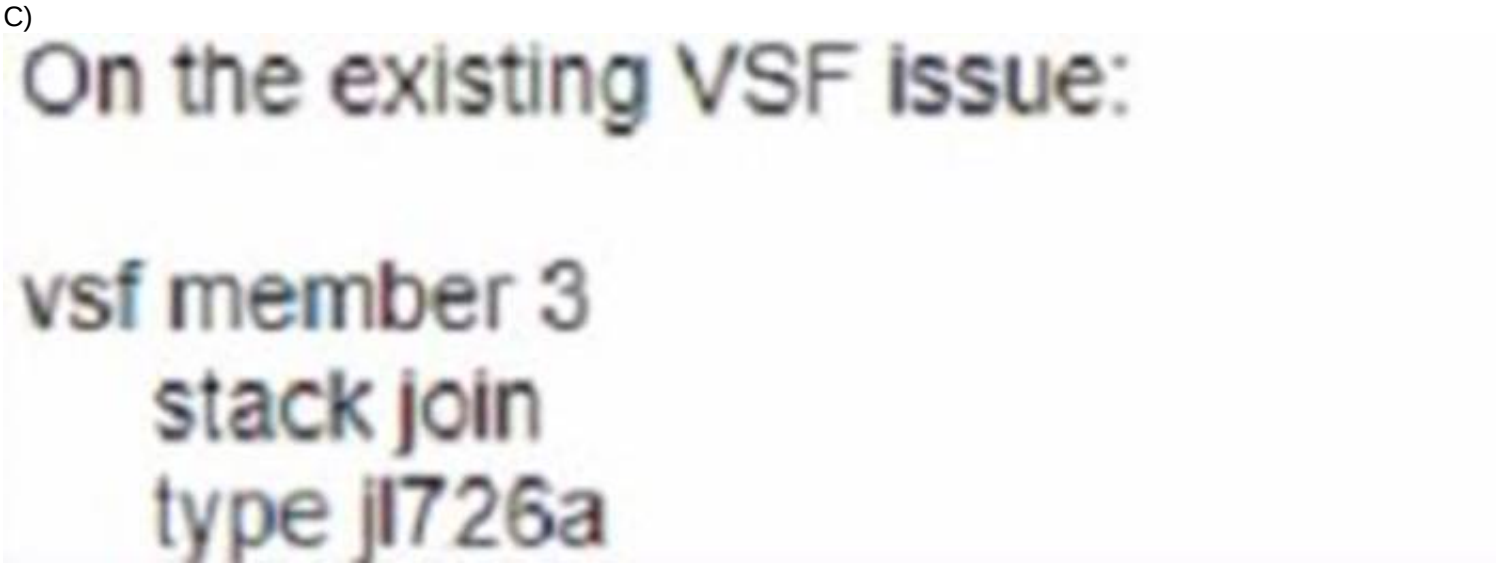
NEW QUESTION 4
Your customer has an Aruba CX 6200F VSF stack with two switches. A third member (JL726A) needs to be added to the VSF configuration. What e the configuration that enables the new devices to join the VSF?
A)



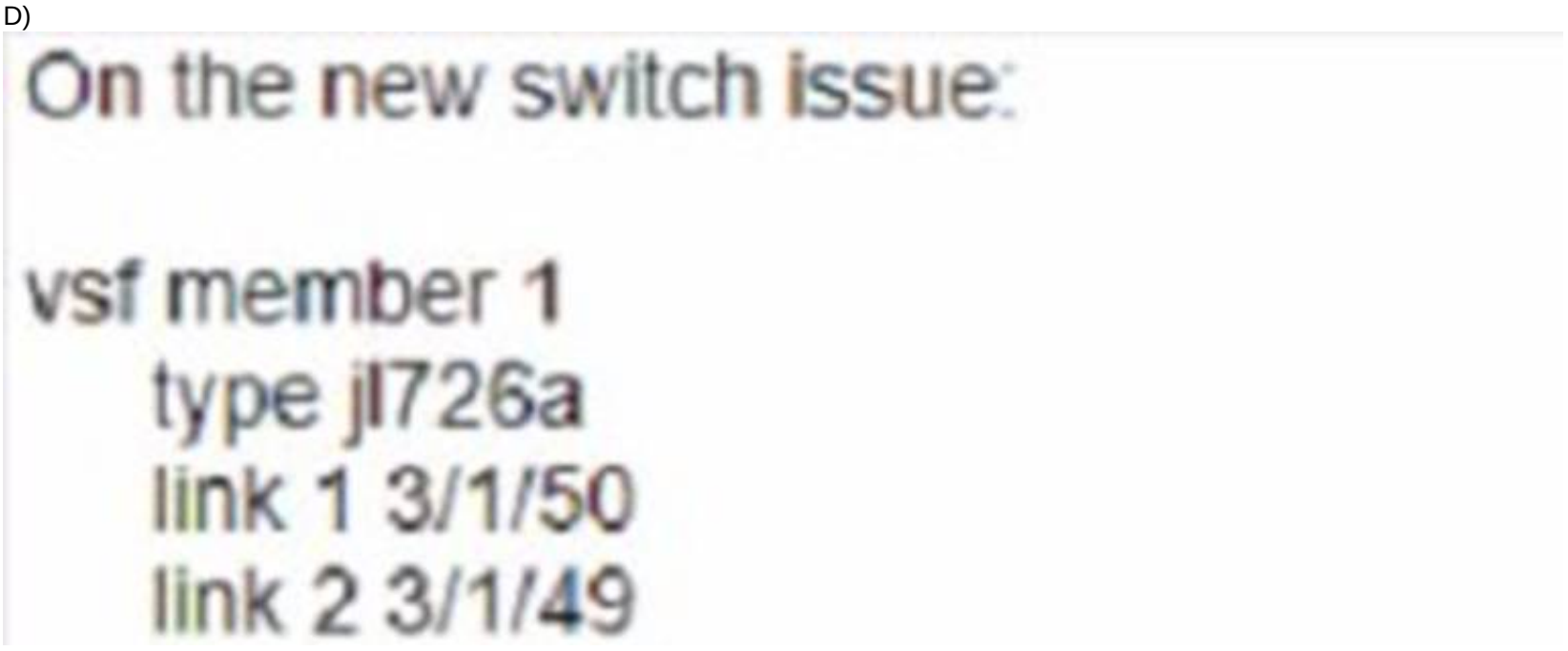
B)



C)



D)



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 5
You need to drop excessive broadcast traffic on an ingress port or an ArubaOS-CX switch. What is the best feature to use for this task?

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

Answer: C

Explanation:
According to the Aruba Documentation Portal1, the ArubaOS-CX switch supports various features to control the ingress traffic on specific ports, such as rate limiting, QoS shaping, and access control. These features can help reduce the impact of excessive broadcast traffic on the network performance and availability.
This is because rate limiting is a feature that allows you to limit the inbound or outbound traffic on a port based on a percentage of the port capacity or a fixed amount of bytes per second. Rate limiting can help prevent broadcast storms by reducing the amount of broadcast packets that enter or leave a port
https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-access-control.htm 2:
https://community.arubanetworks.com/blogs/esupport1/2021/02/08/broadcast-storm-containment-in-aruba-pvos-switches 3:
https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998- 8160_ssw_mcg/content/ch05.html

NEW QUESTION 6
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 7
A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working across the campus which is connected via layer-3. The legacy devices are connected to Aruba CX 6300 switches throughout the campus. Which technology minimizes flooding so the legacy application can work efficiently?

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

Answer: B

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

NEW QUESTION 8
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 9
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 10
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 10
Your Aruba CX 6300 VSF stack has OSPF adjacency over SVI 10 with LAG 1 to a neighboring device The following configuration was created on the switch:

```
vlan 20,30,40
!
interface vlan 20
    ip address 10.10.20.1/24
!
interface vlan 30
    ip address 10.10.30.1/24
!
interface vlan 40
    ip address 10.10.40.1/24
```

A)

```
vlan 20, 30,40
    ospf passive
```

B)

```
interface vlan 20,30,40
    ip ospf passive
```

C)

```
router ospf 1
 area 0
 passive-interface
    vlan 20,30,40
```

D)

```
router ospf 1
    area 0
        redistribute local
```

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

Answer: B

Explanation:
OSPF (Open Shortest Path First) is a routing protocol that uses link-state information to calculate the best path to each destination in the network. OSPF establishes adjacencies with neighboring routers to exchange routing information and maintain a consistent view of the network topology1.
To establish an OSPF adjacency, the routers need to have some common parameters, such as the area ID, the network type, the hello interval, the dead interval, and the authentication method2. The routers also need to have a matching subnet mask on the interface that connects them3.
In this case, the Aruba CX 6300 VSF stack has an SVI (Switched Virtual Interface) on VLAN 10 with an IP address of 10.1.1.1/24 and a LAG (Link Aggregation Group) on port 1/1/1 and port 2/1/1 that connects to a neighboring device. The SVI is configured with OSPF area 0 and network type broadcast. The LAG is configured with OSPF passive mode, which means that it will not send or receive OSPF hello packets.
The neighboring device has an interface with an IP address of 10.1.1.2/24 and a LAG on port 1/0/1 and port 2/0/1 that connects to the Aruba CX 6300 VSF stack. The interface is configured with OSPF area 0 and network type broadcast.
Since the Aruba CX 6300 VSF stack and the neighboring device have the same area ID, network type, subnet mask, and default hello and dead intervals on their interfaces, they will be able to establish an OSPF adjacency over SVI 10 with LAG 1. The OSPF passive mode on the LAG will not affect the adjacency, because it only applies to the LAG interface, not the SVI interface.

NEW QUESTION 15
A client is connecting to 802.1X SSID that has been configured in tunnel mode with the default AP-group settings.
After receiving Access-Accept from the RADIUS server, the Aruba Gateway will send Access-Accept to the AP through which tunnel?

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

Answer: C

Explanation:
According to the Aruba Documentation Portal1, 802.1X is a standard for port- based network access control that uses a RADIUS server to authenticate and authorize wireless clients. 802.1X can be configured in different modes, such as bridge mode, tunnel mode, or split tunnel mode.
Option C: GRE tunnel
This is because option C shows how to configure an SSID in tunnel mode with the default AP-group settings on an Aruba switch. In tunnel mode, all client traffic from the access points is tunneled back to the controller and the controller would in turn put the client traffic onto the network2. The GRE protocol is used to encapsulate and decapsulate the traffic between the access points and the controller3.
Therefore, option C is correct.
1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html 2: https://community.arubanetworks.com/discussion/bridge-and-tunnel-mode 3: https://www.twingate.com/blog/ipsec-tunnel-mode

NEW QUESTION 20
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 25
When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

A. QSVI
B. MAC tables
C. UDLD
D. RPVST+

Answer: B

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

NEW QUESTION 30
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 31
What is used to retrieve data stored in a Management Information Base (MIS)?

A. SNMPv3
B. DSCP
C. TLV
D. CDP

Answer: A

Explanation:
The correct answer is A. SNMPv3.
SNMPv3 is a protocol that is used to retrieve data stored in a Management Information Base (MIB), which is a database of managed objects in a network. SNMPv3 provides security and access control features that are not available in earlier versions of SNMP. SNMPv3 can also use encryption to protect the data from unauthorized access or modification.
According to the Aruba Certified Professional – Campus Access document1, one of the skills that this certification validates is:
? Implement and Analyze the output from common network monitoring tools
The document also mentions that the candidate should have a distinguished understanding of different protocols across vendors, which implies that they should be familiar with SNMPv3 and how it can be used to access MIB data.

NEW QUESTION 35
You are helping an onsite network technician bring up an Aruba 9004 gateway with ZTP for a branch office The technician was to plug in any port for the ZTP process to start Thirty minutes after the gateway was plugged in new users started to complain they were no longer able to get to the internet. One user who reported the issue stated their IP address is 172.16 0.81 However, the branch office network is supposed to be on 10.231 81.0/24.

What should the technician do to alleviate the issue and get the ZTP process started correctly?

A. Turn off the DHCP scope on the gateway, and set DNS correctly on the gateway to reach Aruba Activate
B. Move the cable on the gateway from port G0/0V1 tc port G0 0.0
C. Move the cable on the gateway to G0/0/1. and add the device's MAC and Serial number in Central
D. Factory default and reboot the gateway to restart the process.

Answer: B

Explanation:
Aruba 9004 gateway supports ZTP on port G0/0/0 by default1. If the gateway
is connected to a different port, such as G0/0/V1, it will not be able to communicate with Aruba Activate and Aruba Central, which are required for ZTP2. Moreover, port G0/0/V1 is configured as a DHCP server by default, which can cause IP address conflicts with the existing network3. Therefore, the technician should move the cable on the gateway to port G0/0/0, which will allow the gateway to obtain an IP address from the network DHCP server and start the ZTP process. The other options are not correct because they will not solve the issue or enable ZTP. For example, option D will not work because factory defaulting and rebooting the gateway will not change the port configuration or behavior3.

NEW QUESTION 37
A customer is using stacked Aruba CX 6200 and CX 6300 switches for access and a VSX pair of Aruba CX 8325 as a collapsed core 802 1X is implemented for authentication. Due to the lack of cabling, some unmanaged switches are still in use Sometimes devices behind these switches cause network outages The switch should send a warning to the helpdesk when the problem occurs You have been asked to implement an effective solution to the problem
What is the solution for this?

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

Answer: C

Explanation:
This is the correct solution to the problem of devices behind unmanaged switches causing network outages due to loops. Loop protection is a feature that allows an Aruba CX switch to detect and prevent loops by sending loop protection packets on each port, LAG, or VLAN on which loop protection is enabled. If a loop protection packet is received by the same switch that sent it, it indicates a loop exists and an action is taken based on the configuration. Loop protection should be configured on all edge ports of the Aruba CX 6200 and CX 6300 switches, which are the ports that connect to end devices or unmanaged switches. The trap-option should be set up to send a warning to the helpdesk when a loop is detected. The other options are incorrect because they either do not configure loop protection or do not set up the trap-option. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-99A8B276-0DA3-4458-AFD8-42BFEC29D4F5.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-8561-17DB0311ED8F.html

NEW QUESTION 41
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 43
You are doing tests in your lab and with the following equipment specifications
• AP1 has a radio that generates a 10 dBm signal
• AP2 has a radio that generates a 11 dBm signal
• AP1 has an antenna with a gain of 9 dBi
• AP2 has an antenna with a gain of 12 dBi.
• The antenna cable for AP1 has a 2 dB loss
• The antenna cable for AP2 has a 3 dB loss
What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for APT?

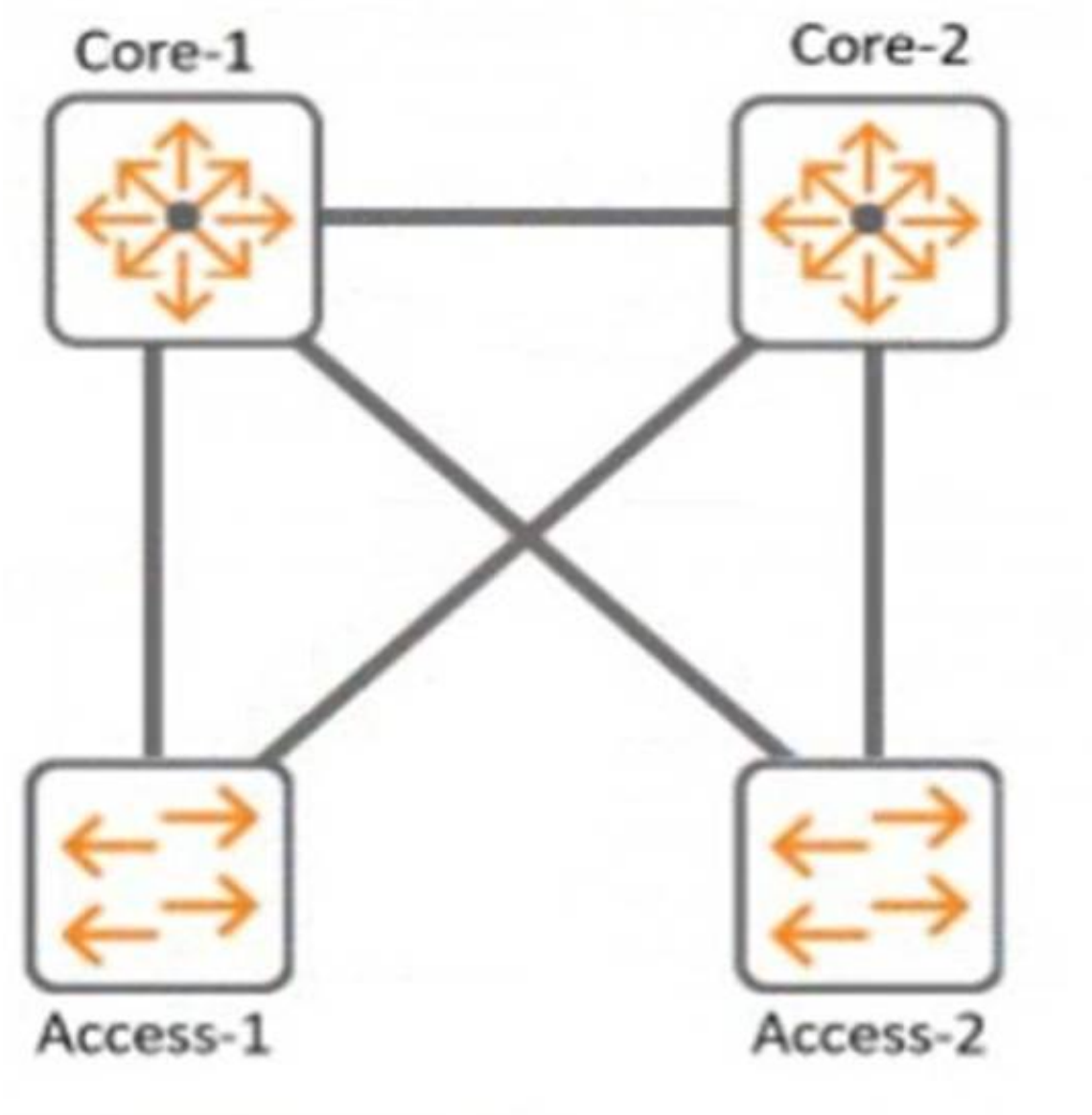
A. 26 dBm
B. 30 dBm
C. 17 dBm
D. -12 dBm

Answer: C

Explanation:
The calculated Equivalent Isotropic Radiated Power (EIRP) for AP1 is 17 dBm.
EIRP is the measured radiated power of an antenna in a specific direction. It is equal to the input power to the antenna multiplied by the gain of the antenna. It can also take into account the losses in transmission line, connectors, and other components. The formula for EIRP is:
EIRP = P + G - L
where P is the output power of the radio, G is the gain of the antenna, and L is the loss of the cable and connectors.
For AP1, we have:

P = 10 dBm G = 9 dBi L = 2 dB
Therefore,
EIRP = 10 + 9 - 2 EIRP = 17 dBm

NEW QUESTION 48
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 49
Using Aruba best practices what should be enabled for visitor networks where encryption is needed but authentication is not required?

A. Wi-Fi Protected Access 3 Enterprise
B. Opportunistic Wireless Encryption
C. Wired Equivalent Privacy
D. Open Network Access

Answer: B

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

NEW QUESTION 51
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.

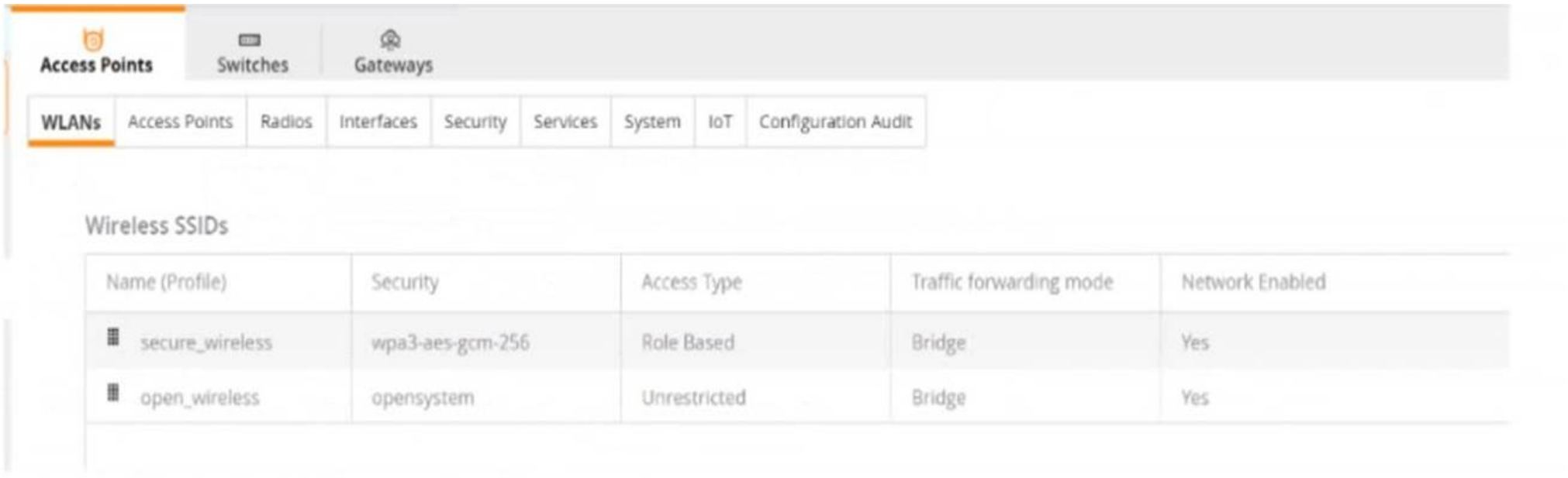
NEW QUESTION 52
A new network design is being considered to minimize client latency in a high-density environment. The design needs to do this by eliminating contention overhead by dedicating subcarriers to clients.
Which technology is the best match for this use case?

A. OFDMA
B. MU-MIMO
C. QWMM
D. Channel Bonding

Answer: A

Explanation:
OFDMA (Orthogonal Frequency Division Multiple Access) is a technology that can minimize client latency in a high-density environment by eliminating contention overhead by dedicating subcarriers to clients. OFDMA allows multiple clients to transmit simultaneously on different subcarriers within the same channel, reducing contention and increasing efficiency. MU-MIMO (Multi-User Multiple Input Multiple Output) is a technology that allows multiple clients to transmit simultaneously on different spatial streams within the same channel, but it does not eliminate contention overhead. QWMM (Quality of Service Wireless Multimedia) is a technology that prioritizes traffic based on four access categories, but it does not eliminate contention overhead. Channel Bonding is a technology that combines two adjacent channels into one wider channel, increasing bandwidth but not
eliminating contention overhead. References: https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf
https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf

NEW QUESTION 56
Refer to the exhibit.



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?

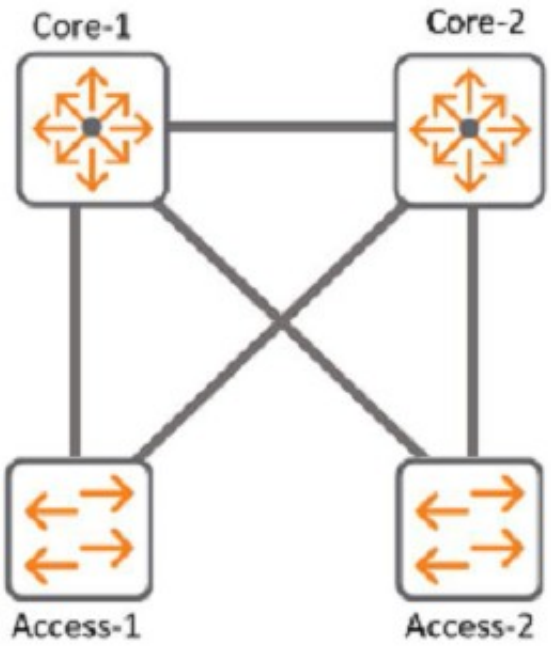
A. Change the SSID to WPA3-Enhanced Open
B. Change the SSID to WPA3-Enterprise (CCM).
C. Change the SSID to WPA3-Personal
D. Change the SSID to WPA3-Enterpnse (CNSA).

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 60

Refer to Exhibit:



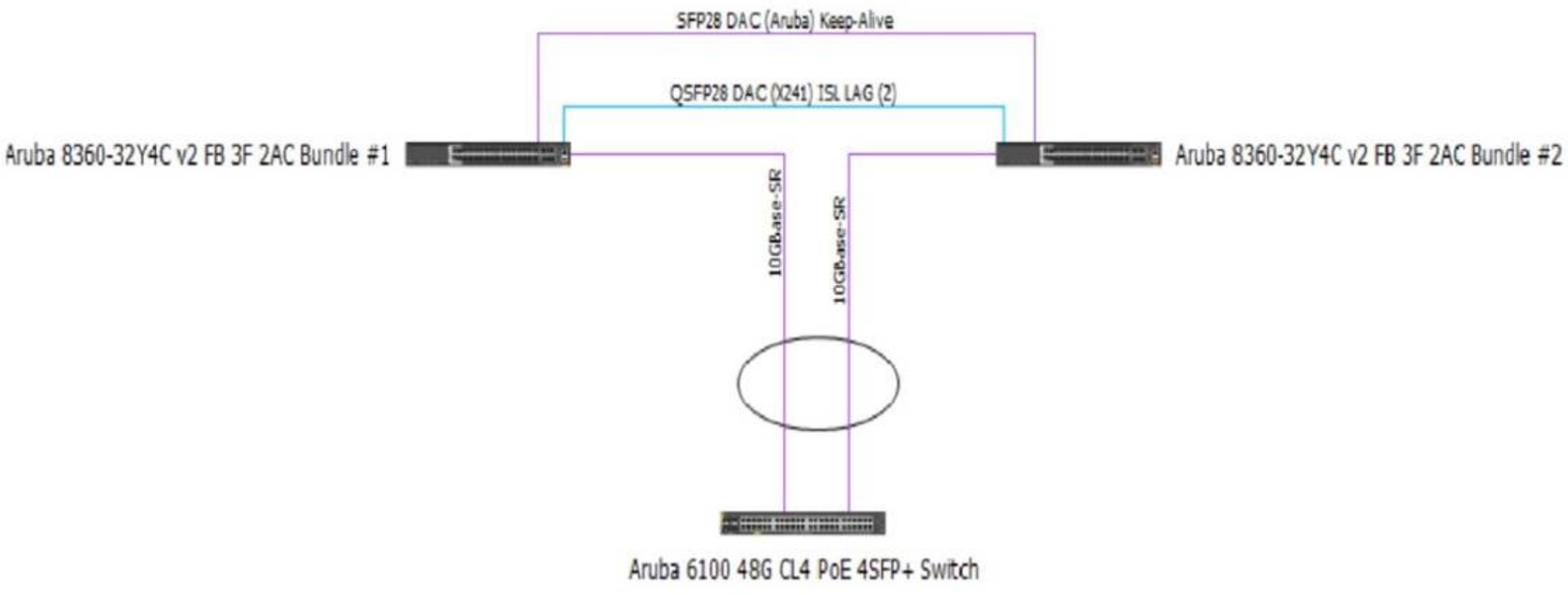
With Access-1, What needs to be identically configured With MSTP to load-balance VLANS?

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 62
Review the exhibit.



You are troubleshooting an issue with a 10 102.39 0/24 subnet which is also VLAN 1000 used Tor wireless clients on a pair of Aruba CX 8360 switches The subnet SVI is configured on the 8360 pair, and the DHCP server is a Microsoft Windows Server 2022 Standard with an IP address of 10 200 1.100. The 10.102.250.0/24 subnet is used for switch management.
A large number of DHCP requests are failing You are observing sporadic DHCP behavior across clients attached to the CX 6100 switch.
Which action may help fix the issue?

A)
Enter the following commands on the VSX primary switch:

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

B)
Enter the following commands on the VSX secondary switch:

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

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

D)
Enter the following commands on the Aruba CX 6100 switch:

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

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

Answer: C

Explanation:
Option C is the only action that configures the DHCP relay on the SVI of VLAN 1000 on the CX 8360 switches. DHCP relay is a feature that allows a switch to forward DHCP requests from clients in one subnet to a DHCP server in another subnet. DHCP relay is required when the DHCP server and the clients are not in the same broadcast domain1.
Option C uses the following commands:
? interface vlan 1000: This command enters the interface configuration mode for the SVI of VLAN 1000, which has an IP address of 10.102.39.1/24 and is used for wireless clients.
? ip helper-address vrf default 10.200.1.100: This command configures the IP address of the DHCP server as a helper address for the SVI, which means that the switch will forward DHCP requests from clients on VLAN 1000 to this address. The vrf default parameter indicates that the SVI and the DHCP server are in the same VRF.

NEW QUESTION 65
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 68
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 69
Your customer is interested in hearing more about how roles can help keep consistent policy enforcement in a distributed overlay fabric How would you explain this concept to them"

A. Group Based Policy ID is applied on egress VTEP after device authentication and policy is enforced on ingress VTEP
B. Role-based policies are tied to IP addresses which have an advantage over IP-based policies and role names are sent between VTEPs
C. Group Based Policy ID is applied on ingress VTEP after device authentication and policy is enforced on egress VTEP
D. Role-based policies enhance User Based Tunneling across the campus network and the policy traffic is protected with iPsec

Answer: C

Explanation:
This is the correct explanation of how roles can help keep consistent policy enforcement in a distributed overlay fabric. Roles are used to assign group based policy IDs (GBPs) to devices after they authenticate with ClearPass or a local database. GBPs are then used to tag the traffic from the devices and send them to the ingress VTEP, which applies the GBP on the VXLAN header. The egress VTEP then enforces the policy based on the GBP and the destination device. The other options are incorrect because they either do not describe the correct sequence of events or do not use the correct terms. 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 70
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 71
In AOS 10. which session-based ACL below will only allow ping from any wired station to wireless clients but will not allow ping from wireless clients to wired stations"? The wired host ingress traffic arrives on a trusted port.

A. ip access-list session pingFromWired any user any permit
B. ip access-list session pingFromWired user any svc-icmp deny any any svc-icmp permit
C. ip access-list session pingFromWired any any svc-icmp permit user any svc-icmp deny
D. ip access-list session pingFromWired any any svc-icmp deny any user svc-icmp permit

Answer: D

Explanation:
A session-based ACL is applied to traffic entering or leaving a port or VLAN based on the direction of the session initiation. To allow ping from any wired station to wireless clients but not vice versa, a session-based ACL should be used to deny icmp echo traffic from any source to any destination, and then permit icmp echo-reply traffic from any source to user destination. The user role represents wireless clients in AOS 10. References: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID- BD3E0A5F-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html
https://techhub.hpe.com/eginfolib/networking/docs/arubaos-switch/security/GUID-EA0A5B3C-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html

NEW QUESTION 76
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 79
DRAG DROP
Match the terms below to their characteristics (Options may be used more than once or not at all.)

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

A. Mastered
B. Not Mastered

Answer: A

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

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

NEW QUESTION 83
Which component is used by the Aruba Network Analytics Engine (NAE)?

A. JSON-based scripts
B. Lisp-based agents
C. Ruby-based scripts
D. Current State Database

Answer: A

Explanation:
The component that is used by the Aruba Network Analytics Engine (NAE) is D. Current State Database.
The Current State Database is a database that stores the configuration and state information of the switch, such as interfaces, VLANs, routing protocols, statistics, and more. The NAE can access this database through the AOS-CX REST API and monitor the values of any data point using monitors. The NAE can also track the history of the values in a time-series database and correlate them with network events or configuration changes1. The Current State Database provides NAE with direct visibility into the entire current state of the device, which enables intelligent troubleshooting and automation of network tasks1. The other options are incorrect because:
? A. JSON-based scripts: JSON is a data format that is used to exchange information between applications. It is not a scripting language that can be used by NAE. NAE scripts are written in Python, which is a popular and powerful programming language1.
? B. Lisp-based agents: Lisp is a family of programming languages that are mainly used for artificial intelligence and functional programming. It is not a language that can be used by NAE. NAE agents are instances of scripts that run on the switch and collect relevant network information and trigger alerts or actions1.
? C. Ruby-based scripts: Ruby is a general-purpose programming language that is known for its expressiveness and elegance. It is not a language that can be used by NAE. NAE scripts are written in Python, which is a popular and powerful programming language1.

NEW QUESTION 87
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 PKl 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.

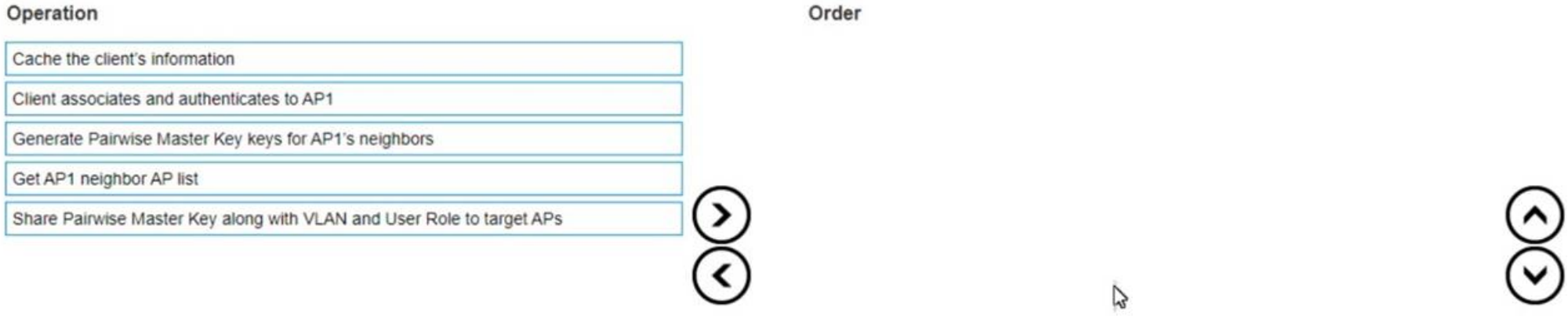
NEW QUESTION 88
You are building a configuration in Central that will be used for a standardized network design for small sites for your company, you want to use GUI configuration for gateways and Aps, while template configuration for switches. You need to align with Aruba best practices.
Which set of 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 93
DRAG DROP
What is the order of operations tor Key Management service for a wireless client roaming from AP1 to AP2?



A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://www.arubanetworks.com/techdocs/Instant_85_WebHelp/Content/instant-ug/wlan-ssid-conf/conf-fast-roam.htm

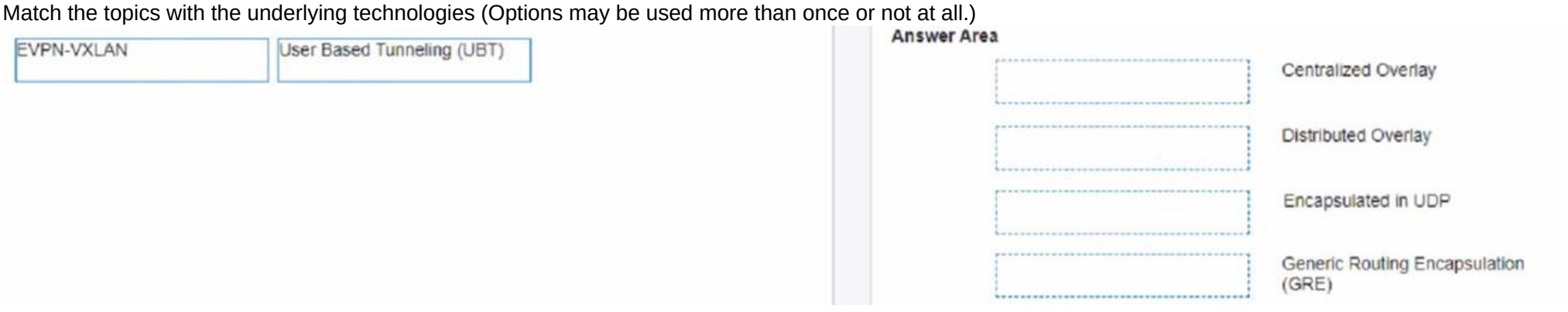
NEW QUESTION 95
You are setting up a customer's 15 headless IoT devices that do not support 802.1X. What should you use?

A. Multiple Pre-Shared Keys (MPSK) Local
B. Clearpass with WPA3-PSK
C. Clearpass with WPA3-AES
D. Multiple Pre-Shared Keys (MPSK) with WPA3-AES

Answer: A

Explanation:
MPSK Local is a feature that can be used to set up 15 headless IoT devices that do not support 802.1X authentication. 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 802.1X authentication, which is not supported by the IoT devices, or WPA3 encryption, which is not supported by Aruba CX switches. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch06.html

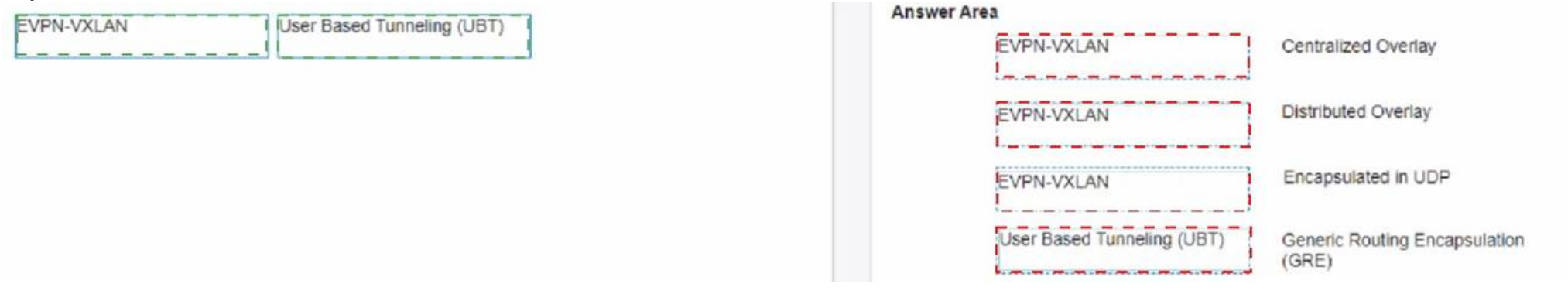
NEW QUESTION 98
DRAG DROP
Match the topics with the underlying technologies (Options may be used more than once or not at all.)



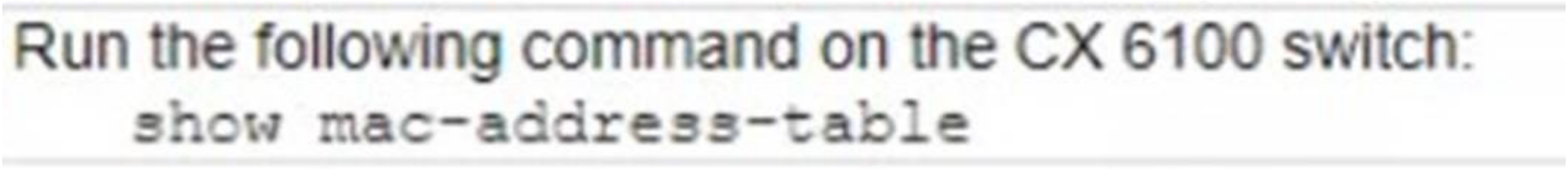
A. Mastered
B. Not Mastered

Answer: A

Explanation:

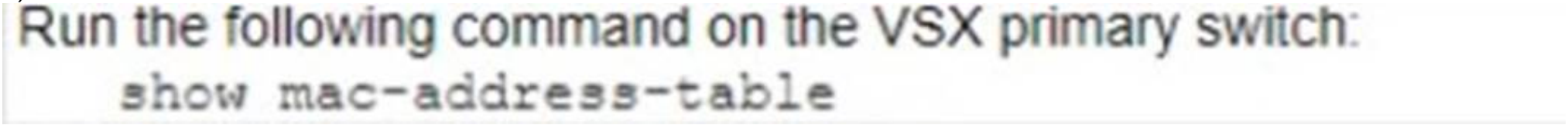


NEW QUESTION 103
You are troubleshooting an issue with a pair of Aruba CX 8360 switches configured with VSX Each switch has multiple VRFs. You need to find the IP address of a particular client device with a known MAC address You run the "show arp" command on the primary switch in the pair but do not 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)

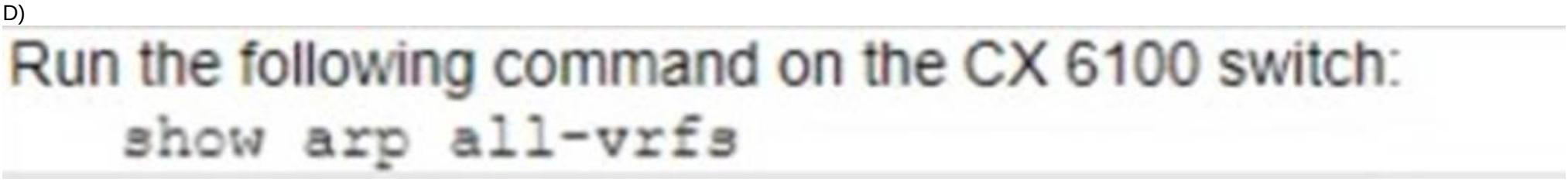


B)

C)



D)



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

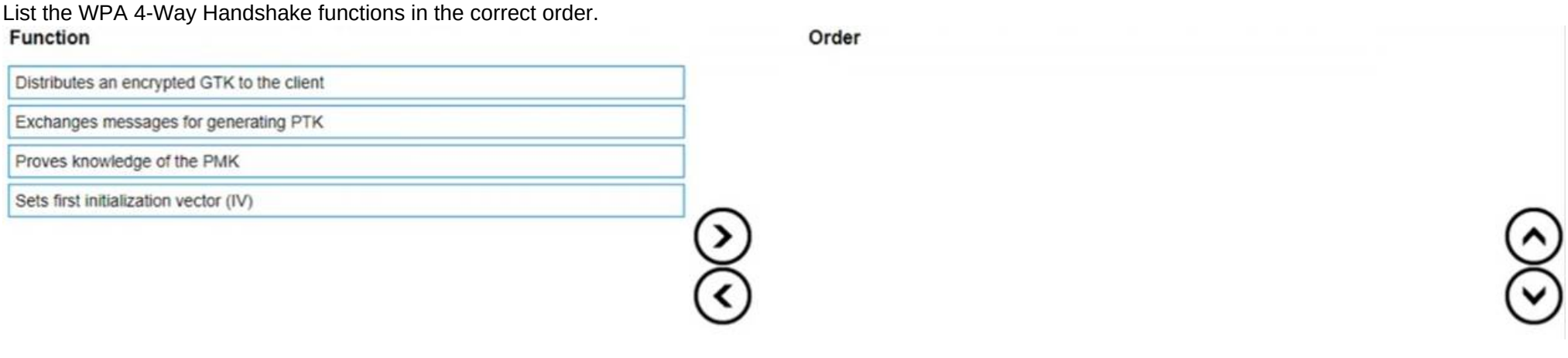
NEW QUESTION 107
Your customer has asked you to assign a switch management role for a new user The customer requires the user role to only have Web UI access to the System > Log page and only have access to the GET method for REST API for the /logs/event resource
Which default AOS-CX user role meets these requirements?

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

Answer: A

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

NEW QUESTION 111
DRAG DROP
List the WPA 4-Way Handshake functions in the correct order.

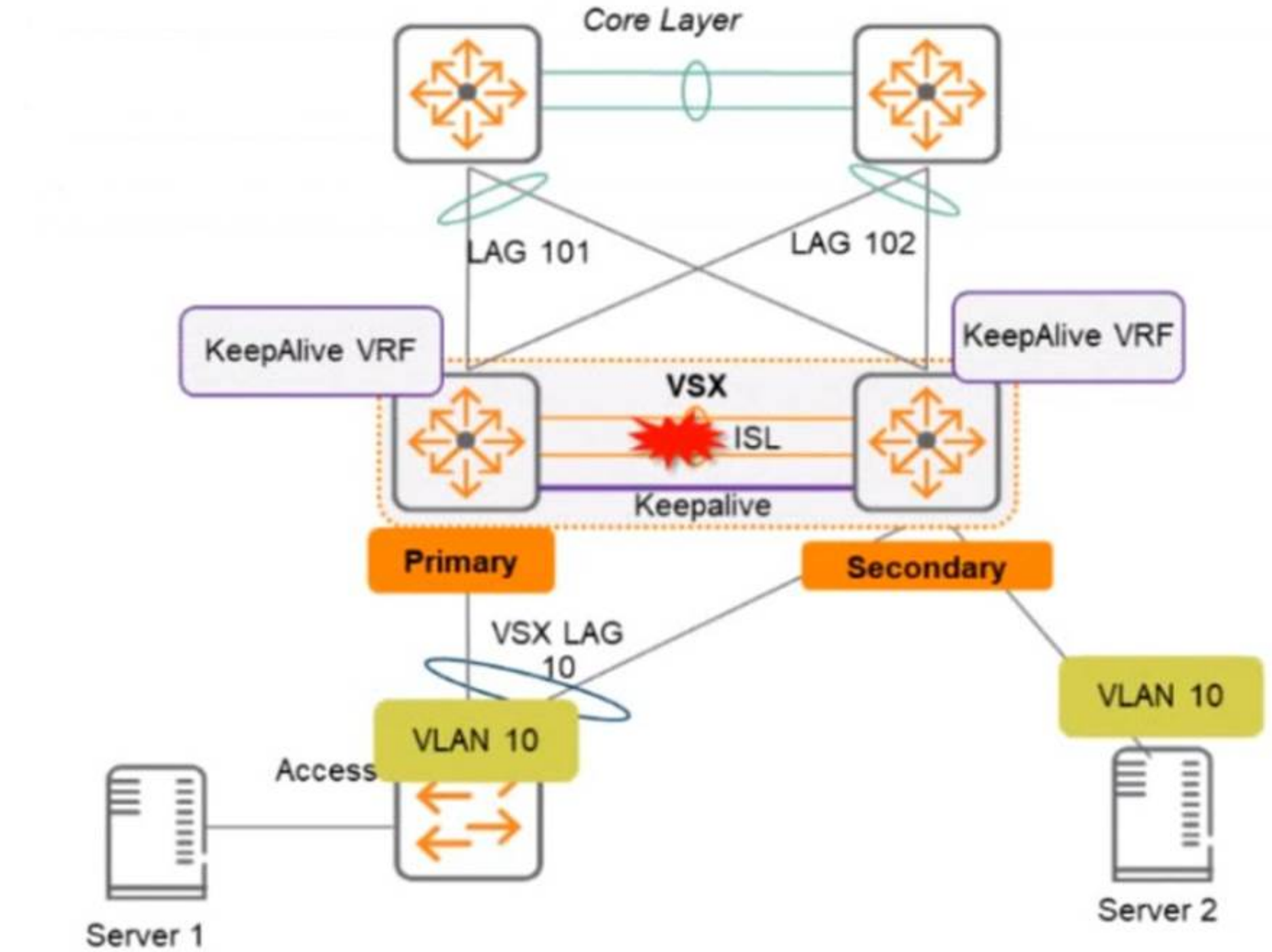


A. Mastered
B. Not Mastered

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 113
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 118
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 120
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 125
With the Aruba CX switch configuration, what is the Active Gateway feature that is used for and is unique to VSX configuration?

A. Sixteen different VMACs are supported total as shared.
B. Active Gateway can once MSTP instances are created for VLAN load sharing.
C. Sixteen different VMACS are supported for each IPV4 and IPV6 stack simultaneously
D. copied over the ISL link for an optimized path.

Answer: C

Explanation:
The active gateway feature is used to provide active-active layer 3 default gateway for hosts on the same subnet. It allows the switch to convert multicast streams into unicast streams over the wireless link, which improves the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. The active gateway feature is unique to VSX configuration because it eliminates the need for VRRP and avoids traffic being pushed over the ISL link, which can cause latency in the network12.
The correct answer to the question is C. Sixteen different VMACs are supported for each IPv4 and IPv6 stack simultaneously. This means that you can have a maximum of eight VMACs for IPv4, and a maximum of eight VMACs for IPv6, on a VSX pair. Only 15 VMACs are supported on 6400 switch series2.
The other options are incorrect because:
? A. Sixteen different VMACs are not supported total as shared. They are supported for each IPv4 and IPv6 stack separately.
? B. Active gateway can be used without MSTP instances. MSTP is a protocol that allows multiple spanning tree instances to coexist on the same switch, but it does not affect how active gateway works.
? D. Active gateway does not copy traffic over the ISL link for an optimized path. It avoids using the ISL link for routed traffic and uses the local switch interface MAC instead of the virtual MAC address (VMAC) for source address1.

NEW QUESTION 129
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

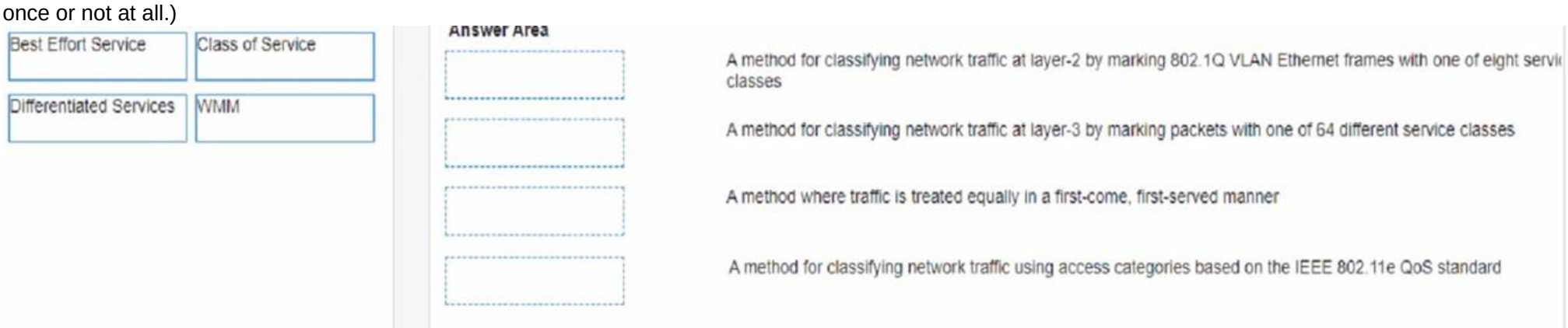
NEW QUESTION 134
Which statements regarding Aruba NAE agents are true? (Select two)

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

Answer: AC

Explanation:
The statements that are true regarding Aruba NAE agents are A and C.
* A. A single NAE script can be used by multiple NAE agents. This means that you can create different instances of the same script with different parameters or settings. For example, you can use the same script to monitor different VLANs or interfaces on the switch1.
* C. NAE agents will never consume more than 10% of switch processor resources. This is a built-in safeguard that prevents the agents from affecting the switch performance or stability. If an agent exceeds the 10% limit, it will be automatically disabled and an alert will be generated2.
The other options are incorrect because:
? B. NAE agents are not active at all times. They can be enabled or disabled by the user, either manually or based on a schedule. They can also be disabled automatically if they encounter an error or exceed the resource limit1.
? D. NAE scripts do not need to be reviewed and signed by Aruba before being used. You can create your own custom scripts using Python and upload them to the switch or Aruba Central. You can also use the scripts provided by Aruba or other sources, as long as they are compatible with the switch firmware version1.
? E. A single NAE agent cannot be used by multiple NAE scripts. An agent is an instance of a script that runs on the switch. Each agent can only run one script at a time1.

NEW QUESTION 135
DRAG DROP
Match the appropriate QoS concept with its definition. (Options may be used more than once or not at all.)



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 138
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 141
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 loT 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 144
With Aruba CX 6300. how do you configure ip address 10 10 10 1 for the interface in default state for interface 1/1/1?

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

Answer: B

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

NEW QUESTION 149
Your customer currently has lwo (2) 5406 modular switches with MSTP configured as their core switches. You are proposing a new solution. What would you explain regarding the Aruba CX VSX switch pair when the Primary VSX node is replaced and the system MAC is replaced?

A. VSX will select the MAC address from a node that is the lower ID.
B. Configure vMAC on the Primary VSX node under VSX to retain MAC after hardware replacement.
C. VSX will select the MAC address from a node that is a higher ID.
D. During the initial VSX configuration, the system-mac is assigned with a fixed MAC based on VSX ID.

Answer: D

Explanation:
The system-mac command is used to configure a fixed MAC address for the VSX system. This MAC address is used as the source MAC address for all routed traffic from the VSX node. The system-mac command is highly recommended for preventing traffic disruptions when the primary VSX switch restores after the secondary VSX switch, such as during a primary switch hardware replacement or a power outage2. During the initial VSX configuration, the system-mac is assigned with a fixed MAC based on VSX ID. The system- mac command can be used to change this default MAC address if needed2. Therefore, answer D is correct.
References: 1: Aruba Campus Access documents and learning resources 2: system-mac - Aruba

NEW QUESTION 151
What is an OSPF transit network?

A. a network that uses tunnels to connect two areas
B. a special network that connects two different areas
C. a network on which a router discovers at least one neighbor
D. a network that connects to a different routing protocol

Answer: A

Explanation:
An OSPF transit network is a network that has at least two routers that are connected by a multi-access link and can forward traffic for other networks1. A transit network is different from a stub network, which has only one router connected to it and does not forward traffic for other networks2. A transit network is also different from a virtual link, which is a logical connection between two areas that are not physically adjacent2. A transit network is not necessarily connected to a different routing protocol, although it can be if the router performs redistribution2. Therefore, the correct answer is C. A network on which a router discovers at least one neighbor.

NEW QUESTION 153
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 154
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?

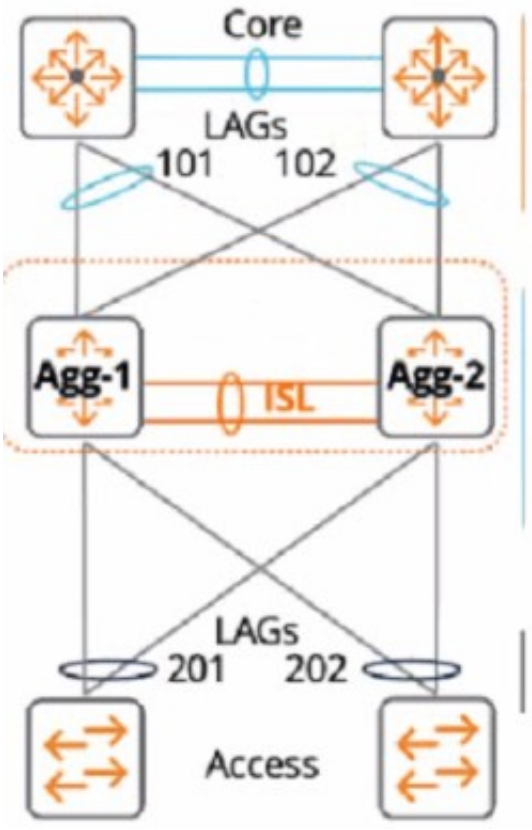
A. sysadmin
B. operators
C. helpdesk
D. config

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 155
A customer just upgraded aggregation layer switches and noticed traffic dropping for 120 seconds after the aggregation layer came online again. What is the best way to avoid having this traffic dropped given the topology below?



A. Configure the linkup delay timer to 240 seconds to double the amount of lime for the initial phase to sync
B. Configure the linkup delay timer to exclude LAGS 101 and 102, which will allow time for routing adjacencies to form and to learn upstream routes
C. Configure the linkup delay timer to include LAGs 101 and 102, which will allow time for routing adjacencies lo form and to learn upstream routes
D. Configure the linkup delay timer to 120 seconds, which will allow the right amount of time for the initial phase to sync

Answer: C

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

NEW QUESTION 156
.....

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