HP.HPE7-A01.vNov-2023.by.Karen.39q

Number: HPE7-A01
Passing Score: 800
Time Limit: 120
File Version: 5.0

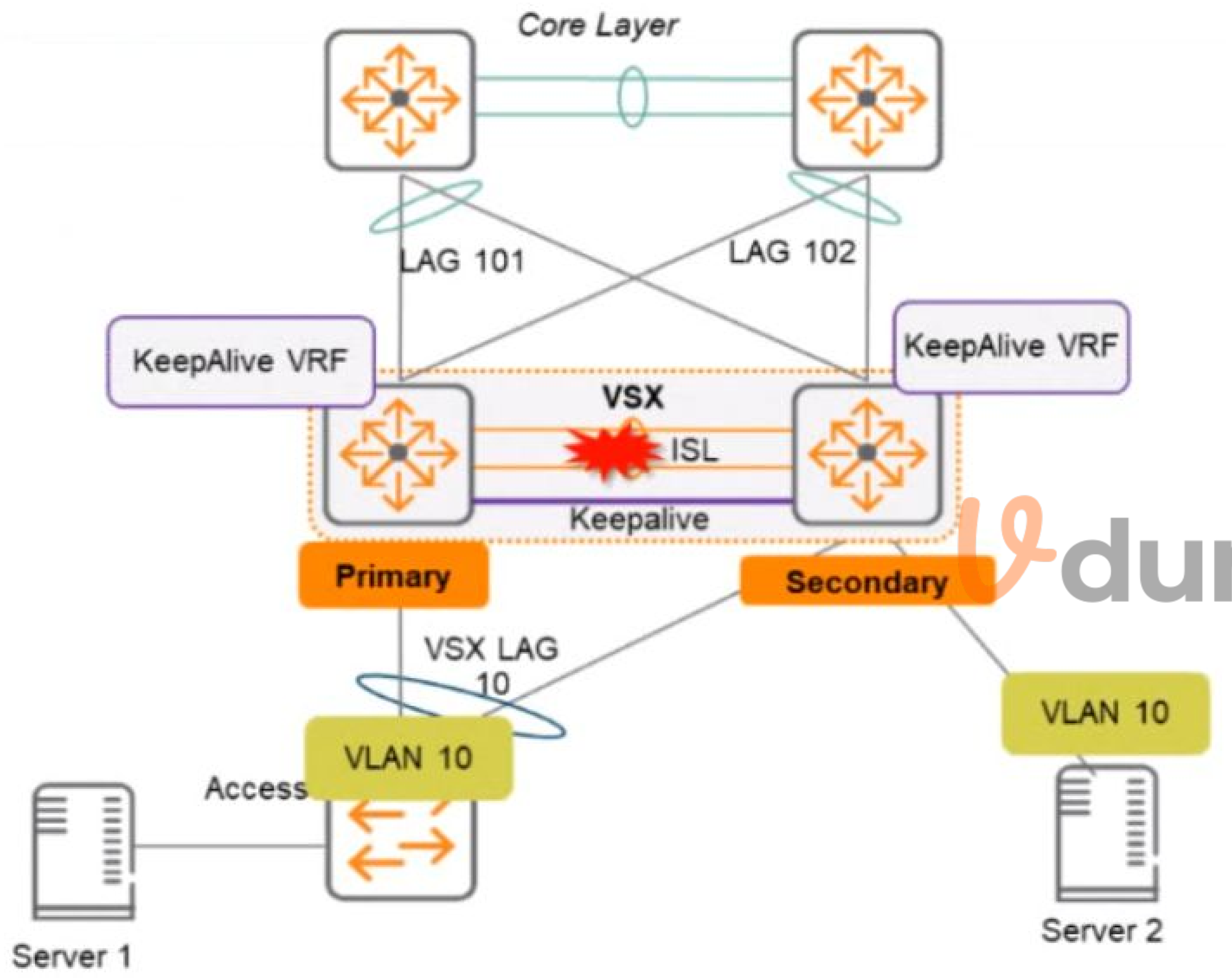
Exam Code: HPE7-A01

Exam Name: Aruba Certified Campus Access Professional

Exam A

QUESTION 1

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

Correct Answer: D, E
Section:

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.
Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-

QUESTION 2
A large retail client is looking to generate a rich set of contextual data based on the location information of wireless clients in their stores Which standard uses Round Trip Time (RTT) and Fine Time Measurements (FTM) to calculate the distance a client is from an AP?

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

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

QUESTION 3
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

Correct Answer: B
Section:
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.
Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html

QUESTION 4
Which method is used to onboard a new UXI in an existing environment with 802 1X authentication? (The sensor has no cellular connection)

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

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

QUESTION 5
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)

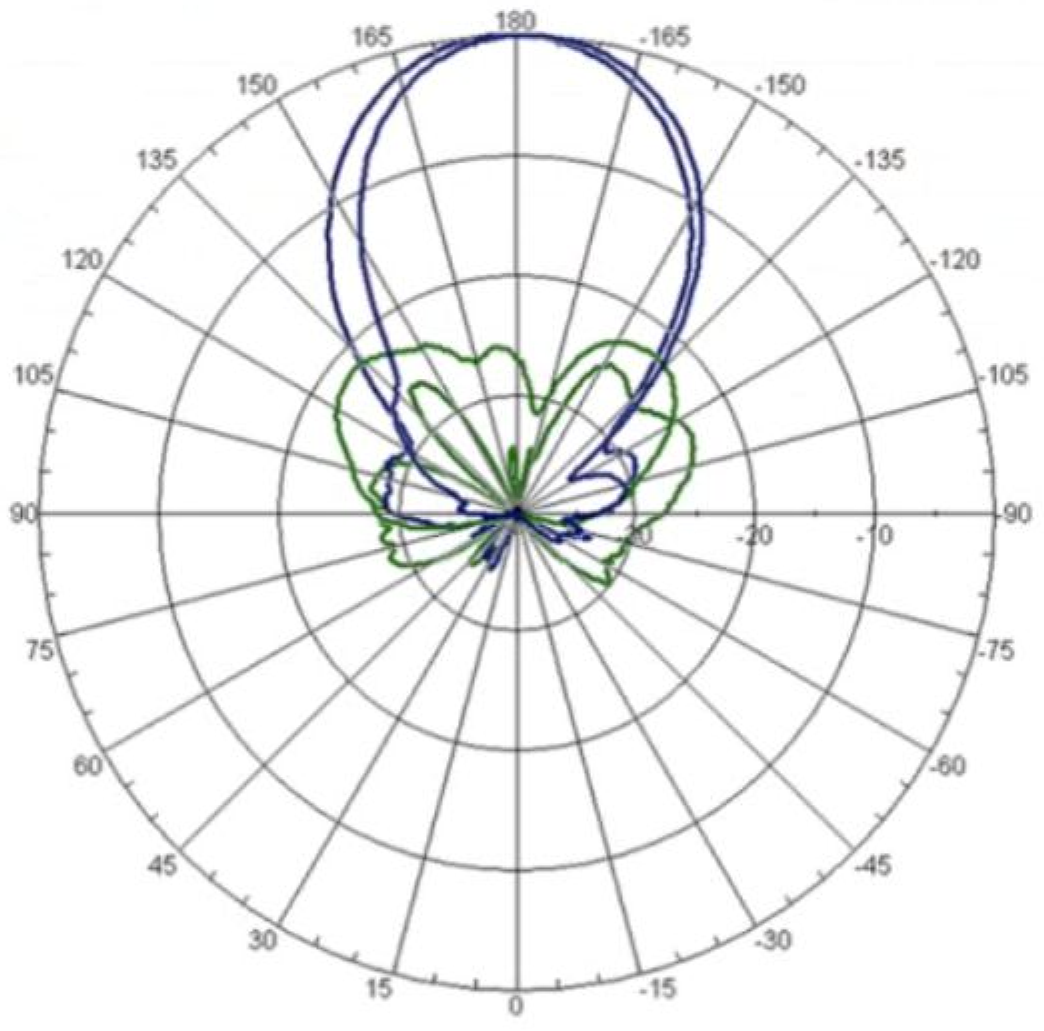
B. Ethernet over IP (EoIP)

C. Generic Routing Encapsulation (GRE)

D. Static VXLAN

Correct Answer: A
Section:
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.
Reference: 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

QUESTION 6
Refer to the image.



Horizontal Pattern

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

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

Correct Answer: B
Section:
Explanation:
The likely cause of the issue of weak Wi-Fi coverage in the office is that the AP is using a directional antenna. A directional antenna is an antenna that radiates or receives radio waves more strongly in one or more directions, creating a focused beam of signal. A directional antenna can provide better coverage and performance for a specific area, but it can also create dead zones or weak spots for other areas. The other options are incorrect because they either do not affect the Wi-Fi coverage or do not match the scenario.
Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/rf-fundamentals.htm
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/antennas.htm

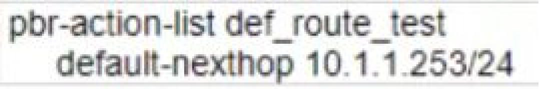
QUESTION 7
Your customer has asked you to assign a switch management role for a new user The customer requires the user role to only have Web Ul access to the System > Log page and only have access to the GET method for REST API for the /logs/event resource
Which default AOS-CX user role meets these requirements?

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

Correct Answer: A
Section:
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.
Reference: 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

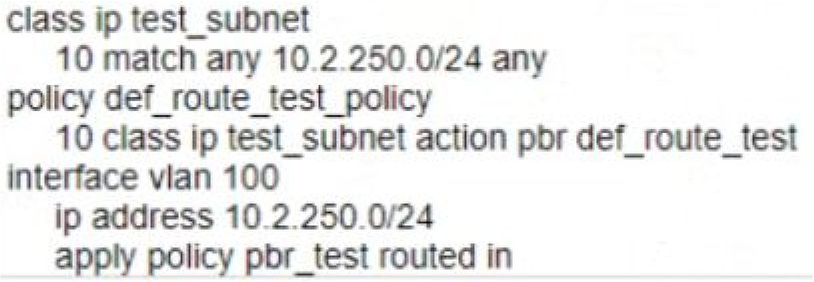
QUESTION 8
You are configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network Traffic originating from 10.2.250.0/24 should use a new default route to 10.1.1.253. Other non-default routes for this subnet should not be affected by this change.
What are two parts of the solution for these requirements? (Select two.)

A)



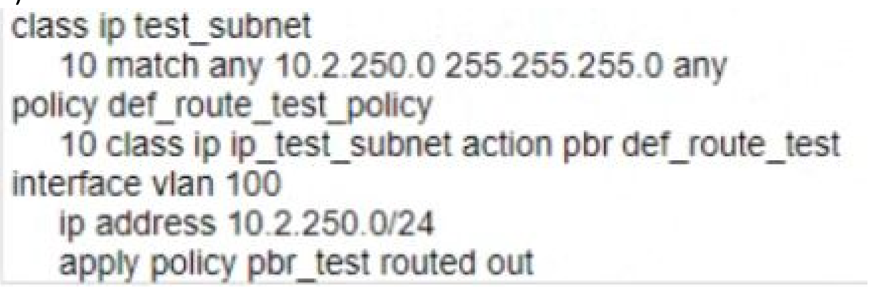
```
pbr-action-list def_route_test
    default-nexthop 10.1.1.253/24
```

B)



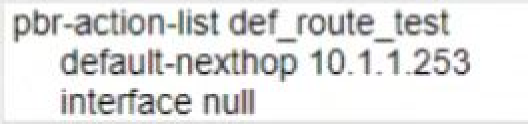
```
class ip test_subnet
    10 match any 10.2.250.0/24 any
policy def_route_test_policy
    10 class ip test_subnet action pbr def_route_test
interface vlan 100
    ip address 10.2.250.0/24
    apply policy pbr_test routed in
```

C)



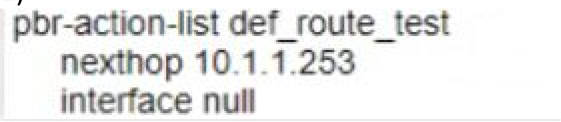
```
class ip test_subnet
    10 match any 10.2.250.0 255.255.255.0 any
policy def_route_test_policy
    10 class ip ip_test_subnet action pbr def_route_test
interface vlan 100
    ip address 10.2.250.0/24
    apply policy pbr_test routed out
```

D)



```
pbr-action-list def_route_test
    default-nexthop 10.1.1.253
    interface null
```

E)



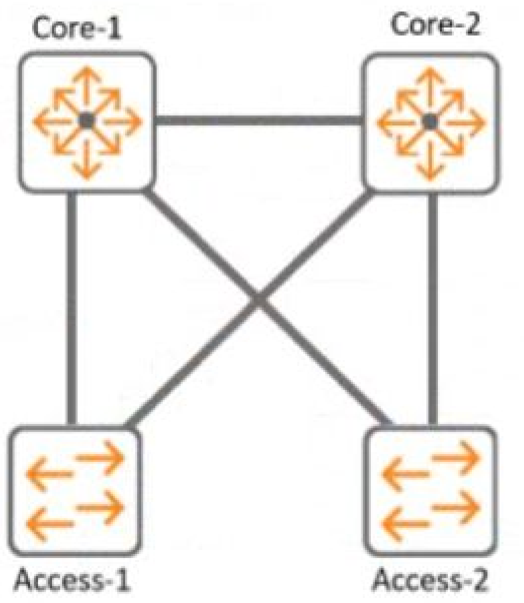
```
pbr-action-list def_route_test
    nexthop 10.1.1.253
    interface null
```

A. Option A
B. Option B

C. Option C
D. Option D
E. Option E

Correct Answer: C, E
Section:
Explanation:
Two parts of the solution for these requirements are Option C and Option E.
Option C is a part of the solution because it defines a policy-based routing action list named route_test, which specifies the next hop IP address as 10.1.1.253 for the matching traffic. This is the new default route that the user wants to use for the subnet 10.2.250.0/24. The interface null parameter indicates that the traffic will be routed to the next hop without using a specific interface1.
Option E is a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 250, which has an IP address of 10.2.250.1/24. This is the subnet that the user wants to test the new default route for. The apply policy command enables policy-based routing on the interface and associates it with the action list2.
Option A is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify the next hop IP address as 10.1.1.253, which is the new default route that the user wants to use. Instead, it specifies a next hop IP address of 10.1.1.254, which is different from the requirement.
Option B is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify any next hop IP address at all, which is necessary for policy-based routing to work. Instead, it specifies an interface null parameter without any IP address, which is invalid.
Option D is not a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 200, which has an IP address of 10.2.200.1/24. This is not the subnet that the user wants to test the new default route for, but a different subnet that should not be affected by this change.

QUESTION 9
Refer to the exhibit.



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

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

Correct Answer: A
Section:
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

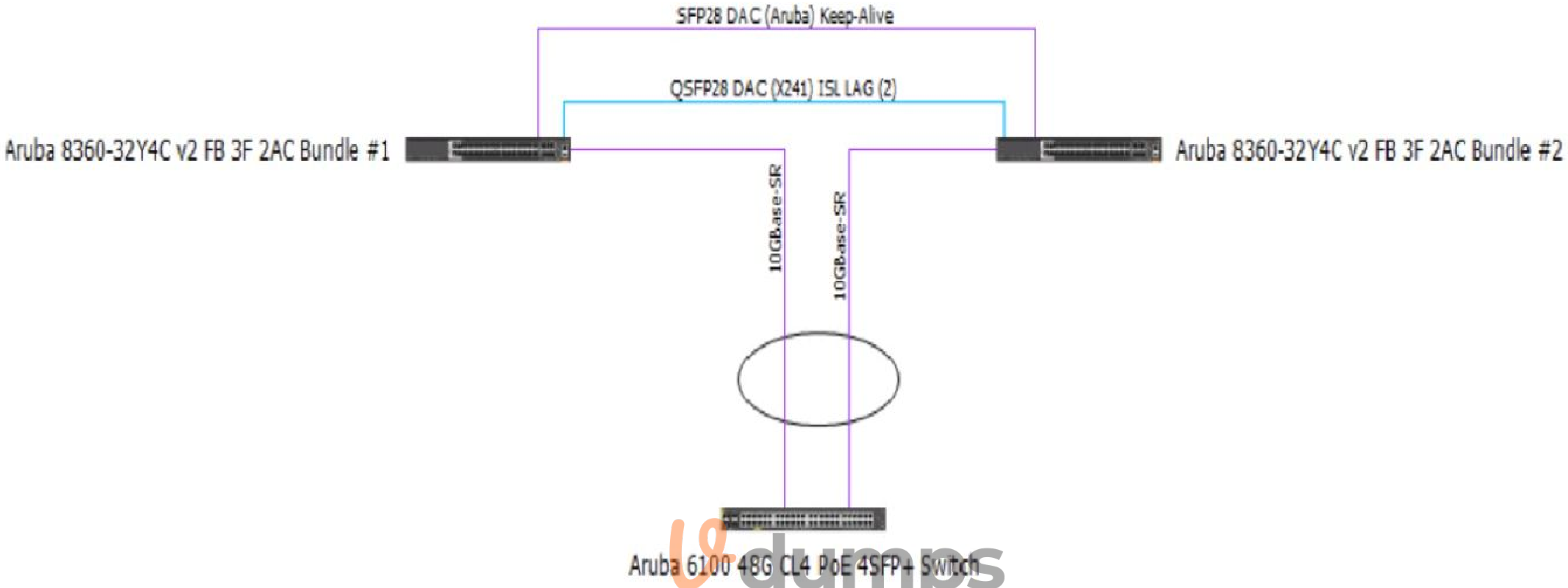
not reflect the default value of config-revision.
Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html

QUESTION 10
What are the requirements to ensure that WMM is working effectively'? (Select two)

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

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

QUESTION 11
Review the exhibit.

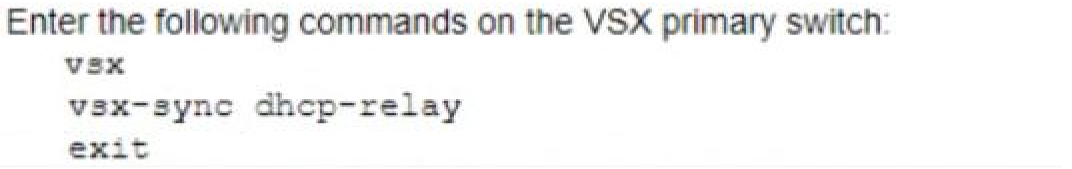

SFP28 DAC (Aruba) Keep-Alive
QSFP28 DAC (X241) ISL LAG (2)
Aruba 8360-32Y4C v2 FB 3F 2AC Bundle #1
Aruba 8360-32Y4C v2 FB 3F 2AC Bundle #2
10GBase-SR
10GBase-SR
Aruba 6100 48G CL4 PoE 4SFP+ Switch

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?

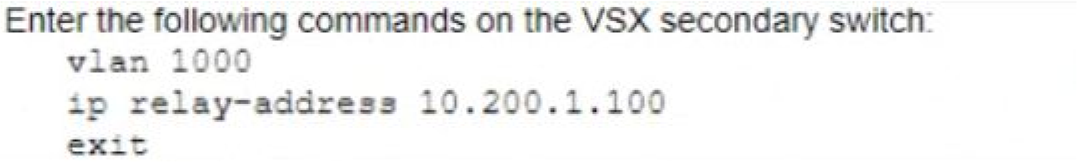
A)



Enter the following commands on the VSX primary switch:

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

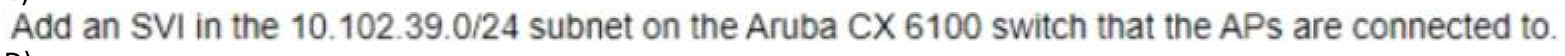
B)



Enter the following commands on the VSX secondary switch:

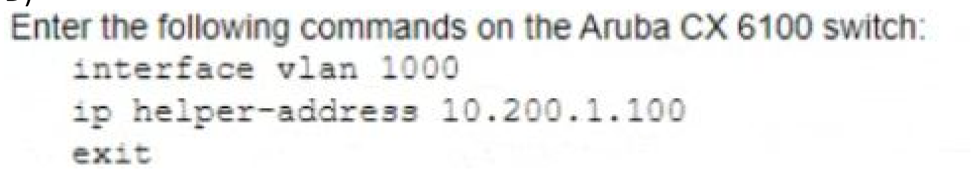
```
   vlan 1000
   ip relay-address 10.200.1.100
   exit
```

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

Correct Answer: C
Section:
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.

QUESTION 12
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.

Correct Answer: A
Section:
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.
Reference: https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

QUESTION 13
Which Aruba AP mode is sending captured RF data to Aruba Central for waterfall plot?

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

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

QUESTION 14
What is a primary benefit of BSS coloring?

A. BSS color tags improve performance by allowing clients on the same channel to share airtime.
B. BSS color tags are applied to client devices and can reduce the threshold for interference
C. BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference
D. BSS color tags improve security by identifying rogue APs and removing them from the network.

Correct Answer: C
Section:
Explanation:
BSS coloring is a mechanism that helps identify the BSS Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.on the same channel and differentiate them from other BSS on the same channel12.Each BSS is assigned a color code, which is a 6-bit value that is carried in the PHY header of the Wi-Fi frames12.By using BSS coloring, the APs and clients can reduce the threshold for interference detection and avoid unnecessary backoff or retransmissions when they detect frames from other BSS with different colors12.This can improve the spectral efficiency and throughput of the network12. The other options are incorrect because they do not describe the primary benefit of BSS coloring.

QUESTION 15
What is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches?

A. Switch authentication and local forwarding of the voice traffic
B. Switch authentication and user-based tunneling of the voice traffic.
C. Central authentication and port-based tunneling of the voice traffic.
D. Controller authentication and port-based tunneling of all traffic

Correct Answer: A
Section:
Explanation:
This is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches. Dynamic segmentation is a feature that allows AOS-CX switches to tunnel user traffic to a controller or another switch based on user roles and policies. For voice traffic, it is recommended to use switch authentication and local forwarding, which means the voice devices are authenticated by the switch and their traffic is forwarded locally without tunneling. This reduces latency and jitter for voice traffic and improves voice quality. The other options are incorrect because they either use central authentication or tunneling, which are not optimal for voice traffic.
Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

QUESTION 16
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

Correct Answer: B, E
Section:
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.
Reference: 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

QUESTION 17
On AOS10 Gateways, which device persona is only available when configuring a Gateway-only group'?

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

Correct Answer: B
Section:
Explanation:
AOS 10 Gateways can have the following personas: Mobility, Branch, and VPN Concentrator1However, the Mobility persona is only available when configuring a Gateway-only group, which is a group that contains only one gateway device2The Mobility persona provides Overlay WLAN and (or) wired LAN functionalities for campus networks1The Branch persona provides the Aruba Instant OS and SD-Branch (LAN + WAN) functionality for branch and microbranch networks1The VPN Concentrator persona provides VPN termination and routing functionality for remote access networks3The Edge persona is not a valid option, as it is not a supported device persona for AOS 10 Gateways.

QUESTION 18
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

Correct Answer: C
Section:
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 commandsystem papi enhanced-security enable3. This will ensure that the tunnels built between the CX switch and the Aruba Gateway are encrypted and authenticated.

QUESTION 19
What is an Aruba-recommended best practice for hardening that only applies to Aruba CX 6300 series switches with dedicated management ports?

A. Implement a control plane ACL to limit access to approved IPs and/or subnets
B. Manually enable Enhanced Security Mode from a console session.
C. Disable all management services on the default VRF.
D. Create a dedicated management VRF, and assign the management port to it.

Correct Answer: D
Section:
Explanation:
This is an Aruba-recommended best practice for hardening that only applies to Aruba CX 6300 series switches with dedicated management ports. A dedicated management port is a physical port that is used exclusively for out-of-band management access to the switch. A dedicated management VRF is a virtual routing and forwarding instance that isolates the management traffic from other traffic on the switch. By creating a dedicated management VRF and assigning the management port to it, the administrator can enhance the security and performance of the management access to the switch. The other options are incorrect because they either do not apply to switches with dedicated management ports or do not follow Aruba-recommended best practices.
Reference: https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

QUESTION 20
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.

Correct Answer: A, B
Section:
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.
Reference: 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

QUESTION 21
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

Correct Answer: A
Section:
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.
Reference: 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

QUESTION 22
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.

Correct Answer: B
Section:
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.

QUESTION 23
A company recently deployed new Aruba Access Points at different branch offices Wireless 802.1X authentication will be against a RADIUS server in the cloud. The security team is concerned that the traffic between the AP and the RADIUS server will be exposed.
What is the appropriate solution for this scenario?

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

Correct Answer: D
Section:
Explanation:
This is the appropriate solution for this scenario where wireless 802.1X authentication will be against a RADIUS server in the cloud and the security team is concerned that the traffic between the AP and the RADIUS server will be exposed. RadSec, also known as RADIUS over TLS, is a protocol that provides encryption and authentication for RADIUS traffic over TCP and TLS. RadSec can be configured on both the AP and the RADIUS server to establish a secure tunnel for exchanging RADIUS packets. The other options are incorrect because they either do not provide encryption or authentication for RADIUS traffic or do not involve RadSec.
Reference: https://www.securew2.com/blog/what-is-radsec/ https://www.cloudradius.com/radsec-vs-radius/
×End Practice TestAre you sure you want to end the test?YesNo

QUESTION 24
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

Correct Answer: C
Section:
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

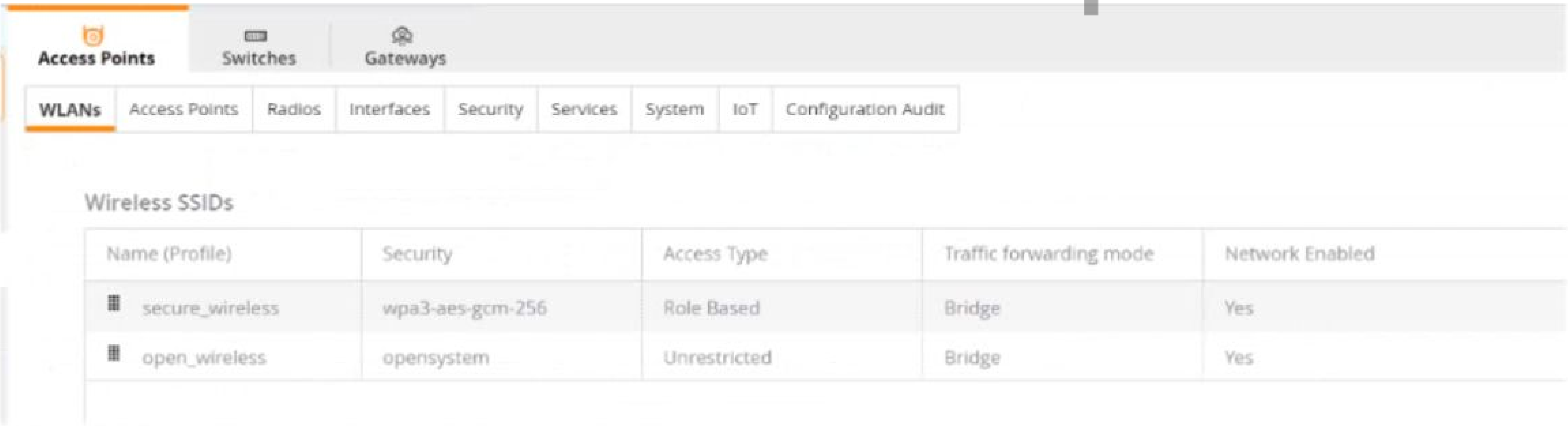
loop protection packets on each port, LAG, or VLAN on which loop protection is enabled. If a loop protection packet is received by the same switch that sent it, it indicates a loop exists and an action is taken based on the configuration. Loop protection should be configured on all edge ports of the 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.
Reference: 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

QUESTION 25
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

Correct Answer: A
Section:
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.
Reference: 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

QUESTION 26
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).

Correct Answer: D
Section:
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.

QUESTION 27
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

Correct Answer: A
Section:
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 address1MAC Caching can be enabled under the splash page settings in Aruba Cloud Guest2MAC Caching can improve the user experience and reduce the network overhead by eliminating the need for repeated authentication.

QUESTION 28
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

Correct Answer: C
Section:
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.
Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/gateways/microbranch.htm https://www.arubanetworks.com/assets/tg/TB_ArubaGateway.pdf

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.

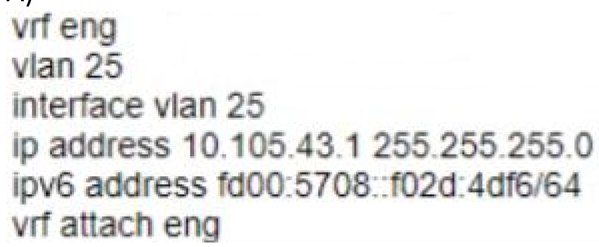
E. The 'redistribute static route-map connected-routes' command will redistribute all static routes with a matching permit in the route map 'connected-routes-

Correct Answer: A, E
Section:
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.
Reference: 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

QUESTION 30

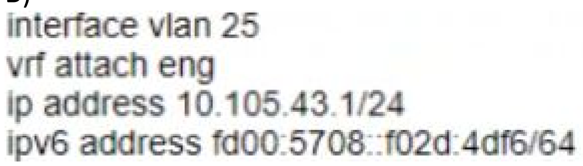
You are configuring an SVI on an Aruba CX switch that needs to have the following characteristics:
* VLANID = 25
. IPv4 address 10 105 43 1 with mask 255 255 255.0
* IPv6 address fd00:5708::f02d:4df6 with a 64 bit prefix length
* member of VRF eng
* VRF eng and VLAN 25 have not yet been created
Which command lists will satisfy the requirements with the least number of commands?

A)



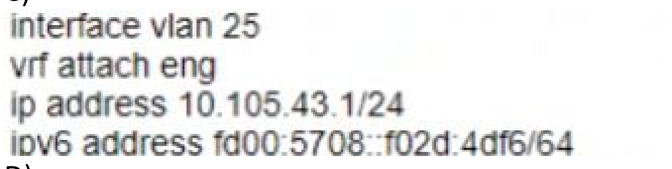
```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43.1 255.255.255.0
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

B)



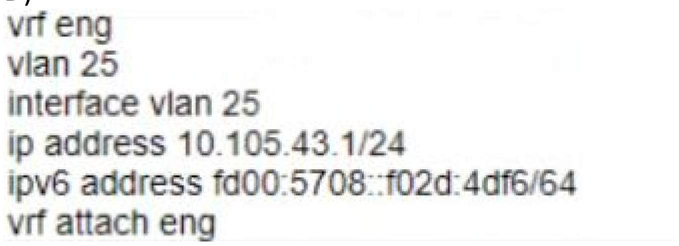
```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
```

C)



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

D)



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

A. Option A

B. Option B

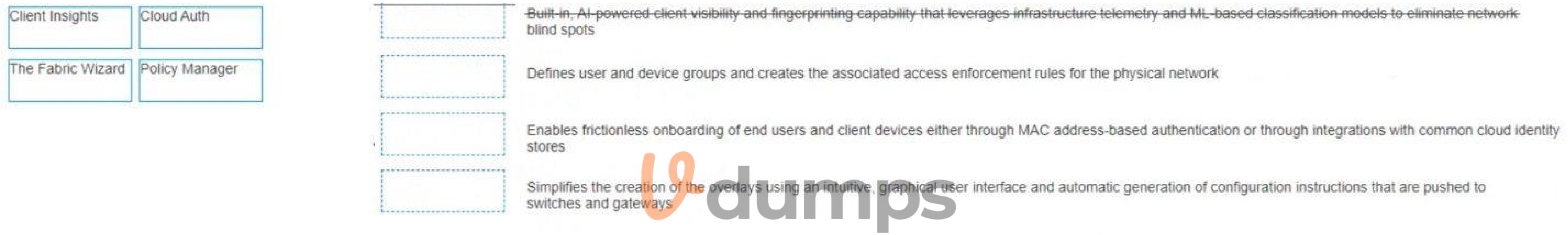
C. Option C

D. Option D

Correct Answer: C
Section:
Explanation:
The other options either use more commands or do not create the VRF or the VLAN.
Option C uses the following commands:
vrf eng: This command creates a VRF named eng and enters the VRF configuration mode1.
vlan 25: This command creates a VLAN with ID 25 and enters the VLAN configuration mode2.
interface vlan 25: This command creates an SVI on VLAN 25 and enters the interface configuration mode3.
ip address 10.105.43.1/24 ipv6 address fd00:5780::102d:4df6/64 vrf attach eng: This command assigns an IPv4 address of 10.105.43.1 with a subnet mask of 255.255.255.0 and an IPv6 address of fd00:5780::102d:4df6 with a prefix length of 64 to the SVI, and attaches it to the VRF eng.

QUESTION 31
DRAG DROP
Match the solution components of NetConductor (Options may be used more than once or not at all.)

Select and Place:



Client Insights
Cloud Auth
The Fabric Wizard
Policy Manager

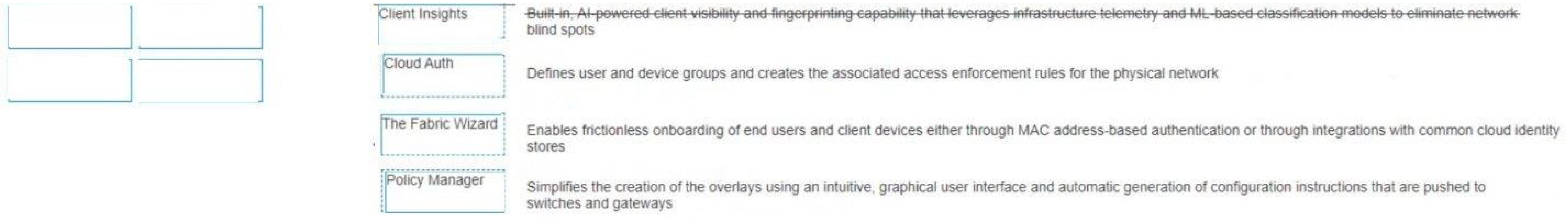
~~Built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network~~ blind spots

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

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

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

Correct Answer:



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

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

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

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

Section:
Explanation:

QUESTION 32
What is one advantage of using OCSP vs CRLs for certificate validation?

A. reduces latency between the time a certificate is revoked and validation reflects this status
B. less complex to implement

C. higher availability for certificate validation
D. supports longer certificate validity periods

Correct Answer: A
Section:
Explanation:
OCSP is a protocol that allows clients to query the CA or a trusted responder for the status of a specific certificate.OCSP requests and responses are smaller and faster than CRLs, and they can provide real-time information about the revocation status of a certificate12. CRLs are lists of all revoked certificates that are downloaded from the CA.CRLs can present issues, as they can become outdated and have to be downloaded frequently13.Therefore, OCSP reduces latency between the time a certificate is revoked and validation reflects this status.
Reference:1https://sectigostore.com/blog/ocsp-vs-crl-whats-the-difference/2https://www.keyfactor.com/blog/what-is-a-certificate-revocation-list-crl-vs-ocsp/3https://www.fortinet.com/resources/cyberglossary/ocsp

QUESTION 33
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

Correct Answer: C
Section:
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.
Reference:4https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html5https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-0C3A9D0F-6E5B-4E1A-AF3C-8D8B2F9C1A7B.html

QUESTION 34
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

Correct Answer: D
Section:
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.
Reference: 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

QUESTION 35

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

A. DMO is configured individually tor each SSID in use in the network.
B. The AP uses OOS to provide equal air time for multicast traffic.
C. DMO is configured globally for each SSID in use in the network.
D. The controller converts multicast streams into unicast streams.

Correct Answer: A
Section:
Explanation:

A. DMO is configured individually for each SSID in use in the network. DMO is a feature that allows the AP to convert multicast streams into unicast streams over the wireless link. This enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. DMO is configured individually for each SSID in use in the network, as different SSIDs may have different multicast requirements. According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure DMO is: Dynamic multicast optimization: Select Enabled to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. The other options are incorrect because:

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

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

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

QUESTION 36
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.

Correct Answer: C
Section:
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.

QUESTION 37
What is a primary benefit of BSS coloring?

A. BSS color tags improve performance by allowing APS on the same channel to be farther apart
B. BSS color tags improve security by identifying rogue APS and tagging them as threats.
C. BSS color tags are applied on the wireless controllers and can reduce the threshold for interference_
D. BSS color tags are applied to WI-Fi channels and can reduce the threshold tor interference

Correct Answer: D
Section:
Explanation:
The primary benefit of BSS coloring is D. BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference.
BSS coloring is a mechanism that allows Wi-Fi 6 devices to mark each frame with a color code that identifies the BSS (Basic Service Set) it belongs to. This helps differentiate between frames from different BSSs that share the same channel and avoid unnecessary collisions and backoffs. BSS coloring also introduces an adaptive threshold for interference, which means that Wi-Fi 6 devices can adjust the signal strength value that determines whether a channel is busy or not based on the current network environment. This allows for more efficient use of spectrum and higher throughput in dense scenarios12.

QUESTION 38
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 auditors role did not have the appropriate level of access on the switch.
The user was not allowed to perform firmware upgrades and a privilege level of 15 was not assigned to their role. Which default management role should have been assigned for the user?

A. sysadmin
B. sysops
C. administrators
D. config

Correct Answer: B
Section:
Explanation:
The correct answer is B. sysops.
The sysops user role is a predefined role that allows users to perform system operations on the switch, such as backup, restore, upgrade, or reboot. The sysops user role also has access to the PUT and POST methods for REST API, which can be used to modify the switch configuration. The sysops user role has a privilege level of 15, which is the highest level of access on the switch1.
The other options are incorrect because:
A) sysadmin: The sysadmin user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The sysadmin user role does not have access to the REST API methods, and cannot perform firmware upgrades1.
C) administrators: 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.
D) config: The config user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The config user role does not have access to the REST API methods, and cannot perform firmware upgrades1.

QUESTION 39
With the Aruba CX 6000 24G switch with uplinks of 1/1/25 and what does the switch do when a client port detects a loop and the do-not-disabie parameter is used?

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

Correct Answer: B
Section:
Explanation:
The correct answer is B. An event log message is created.

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

The other options are incorrect because:

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

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

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