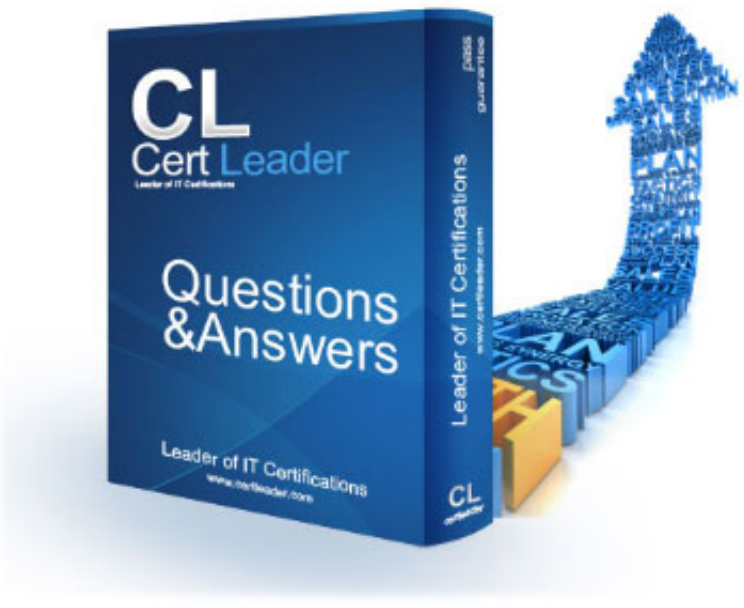
HPE7-A01 Dumps

Aruba Certified Campus Access Professional Exam

https://www.certleader.com/HPE7-A01-dumps.html



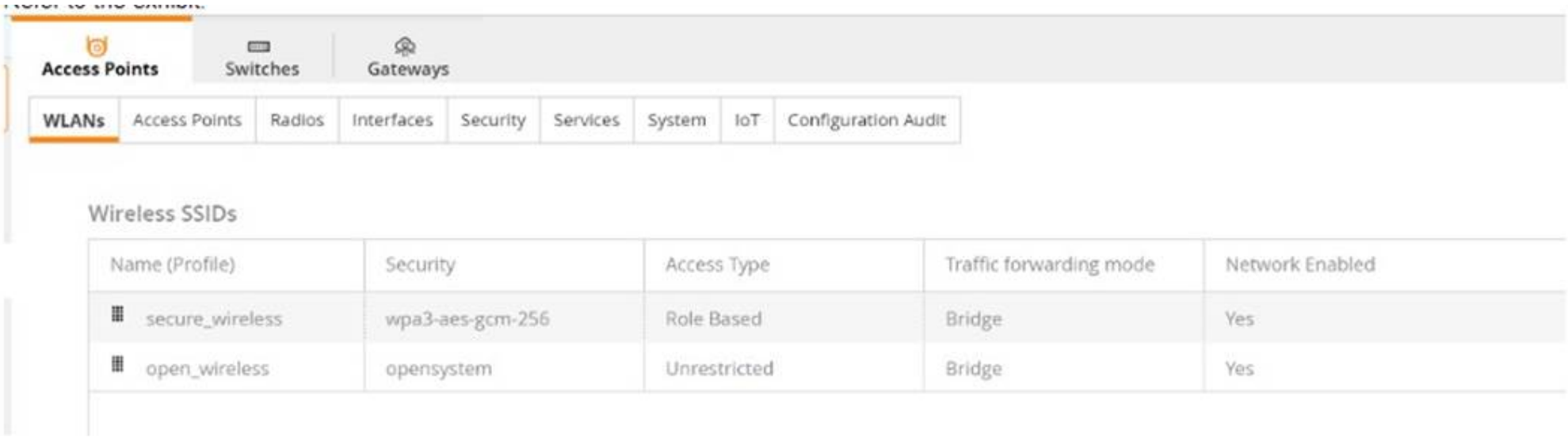
NEW QUESTION 1
The customer needs a network hardware refresh to replace an aging Aruba 5406R core switch pair using spanning tree configuration with Aruba CX 8360-32YC switches What is the benefit of VSX clustering with the new solution?

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
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 3
When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

A. hello interval is disabled by default
B. hello interval is based on the value set by dead interval
C. hello interval 100ms by default
D. hello interval is 1s by default

Answer: D

Explanation:
The reason is that the Inter-Switch Link Protocol (ISLP) is a protocol that enables VSX stack join and synchronization between two VSX peer switches. ISLP uses

a hello interval to exchange control messages between the switches.
The hello interval is a parameter that specifies the time interval between sending hello messages. The default value of the hello interval is 1 second. The hello interval can be configured from 1 second to 10 seconds. https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/index.html

NEW QUESTION 4
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 5
What is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches?

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

Answer: A

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

NEW QUESTION 6
On AOS10 Gateways, which device persona is only available when configuring a Gateway- only group'?

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

Answer: B

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

NEW QUESTION 7
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 8
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 9
With the Aruba CX 6200 24G switch with uplinks or 1/1/25 and 1/1/26, how do you protect client ports from forming layer-2 loops?

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

Answer: A

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

NEW QUESTION 10
You are are doing tests in your lab and with the following equipment specifications:
• AP1 has a radio that generates a 16 dBm signal.
• AP2 has a radio that generates a 13 dBm signal.
• AP1 has an antenna with a gain of 8 dBi.
• AP2 has an antenna with a gain of 12 dBi. The antenna cable for AP1 has a 4 dB loss. The antenna cable for AP2 has a 3 dB loss.
What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?

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

Answer: B

Explanation:
The Equivalent Isotropic Radiated Power (EIRP) is the measured radiated power of an antenna in a specific direction. It is also called Equivalent Isotropic Radiated Power. It is the output power when a signal is concentrated into a smaller area by the Antenna. The EIRP can take into account the losses in transmission line, connectors and includes the gain of the antenna. It is represented in dB2. The formula for EIRP is:
EIRP=PTLc+Ga where PT is the output power of the transmitter in dBm, Lc is the cable and connector loss in dB, and Ga is the antenna gain in dBi.
For AP1, the EIRP can be calculated as: EIRP=164+8=20 dBm
Therefore, the answer B is correct.
References: 1: Aruba Campus Access documents and learning resources 2: EIRP Calculator - Effective Isotropic Radiated Power

NEW QUESTION 10
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

Answer: A

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. References: 1 https://sectigostore.com/blog/ocsp-vs-crl- whats-the-difference/ 2 https://www.keyfactor.com/blog/what-is-a-certificate-revocation-list-crl-vs-ocsp/ 3 https://www.fortinet.com/resources/cyberglossary/ocsp

NEW QUESTION 12
Describe the difference between Class of Service (CoS) and Differentiated Services Code Point (DSCP).

A. CoS has much finer granularity than DSCP

B. CoS is only contained in VLAN Tag fields DSCP is in the IP Header and preserved throughout the IP packet flow
C. They are similar and can be used interchangeably.
D. CoS is only used to determine CLASS of traffic DSCP is only used to differentiate between different Classes.

Answer: B

Explanation:
CoS and DSCP are both methods of marking packets for quality of service (QoS) purposes. QoS is a mechanism that allows network devices to prioritize and differentiate traffic based on certain criteria, such as application type, source, destination, etc. CoS stands for Class of Service and is a 3-bit field in the 802.1Q VLAN tag header. CoS can only be used on Ethernet frames that have a VLAN tag, and it can only be preserved within a single VLAN domain. DSCP stands for Differentiated Services Code Point and is a 6-bit field in the IP header. DSCP can be used on any IP packet, regardless of the underlying layer 2 technology, and it can be preserved throughout the IP packet flow, unless it is modified by intermediate devices. References: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mt-book/qos-overview.html https://www.cisco.com/c/en/us/support/docs/lan- switching/8021q/17056-741-4.html https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html

NEW QUESTION 14
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 19
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 (EolP)
C. Generic Routing Encapsulation (GRE)
D. Static VXLAN

Answer: A

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

NEW QUESTION 24
When configuring UBT on a switch what will happen when a gateway role is not specified?

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

Answer: A

Explanation:
According to the Aruba Documentation Portal1, user-based tunneling (UBT) is a feature that uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. UBT enables a switch to provide a centralized security policy, using per- user authentication and access control to ensure consistent access and permissions.
Option A: The switch will put the client on the access VLAN
This is because option A shows how UBT works on an Aruba switch. When a device connects to the network, it is authenticated using either MAC Authentication or 802.1X and triggers an enforcement policy from ClearPass, which contains an enforcement profile with a user role configuration. The user role can be assigned locally on the switch or on ClearPass as part of an enforcement profile. The user role determines the VLAN that the device belongs to and the access policies that apply to it23.
Therefore, option A is correct.
1: https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-ubt.htm 2: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html 3: https://community.arubanetworks.com/viewdocument/?DocumentKey=c740df4e-3e26-4cc5-9126-355a18709c44&CommunityKey=2fd943a6-8898-4dbe-915f-4f09e4d3c317&tab=librarydocuments

NEW QUESTION 28
A network engineer recently identified that a wired device connected to a CX Switch is misbehaving on the network To address this issue, a new ClearPass policy has been put in place to prevent this device from connecting to the network again.

Which steps need to be implemented to allow ClearPass to perform a CoA and change the access for this wired device? (Select two.)

A. Confirm that NTP is configured on the switch and ClearPass
B. Configure dynamic authorization on the switch.
C. Bounce the switchport
D. Use Dynamic Segmentation.
E. Configure dynamic authorization on the switchport

Answer: BC

Explanation:
CoA (Change of Authorization) is a feature that allows ClearPass to dynamically change the authorization and access privileges of a device after it has been authenticated1. CoA uses RADIUS messages to communicate with the network device and instruct it to perform an action, such as reauthenticating the device, applying a new VLAN or user role, or disconnecting the device2.
To enable CoA on a CX switch, the network engineer needs to configure dynamic authorization on the switch, which is a global command that allows the switch to accept RADIUS messages from ClearPass and execute the requested actions3. The network engineer also needs to specify the IP address and shared secret of ClearPass as a dynamic authorization client on the switch3.
To trigger CoA for a specific wired device, the network engineer needs to bounce the switchport, which is an action that temporarily disables and re-enables the port where the device is connected. This forces the device to reauthenticate and receive the new policy from ClearPass. Bouncing the switchport can be done manually by using the interface shutdown and no shutdown commands, or automatically by using ClearPass as a CoA server and sending a RADIUS message with the Port-Bounce-Host AVP (Attribute-Value Pair).

NEW QUESTION 31
Your manufacturing client is deploying two hundred wireless IP cameras and fifty headless scanners in their warehouse. These new devices do not support 802.1X authentication.
How can HPE Aruba enhance security for these new IP cameras in this environment?

A. Use MPSK Local to automatically provide unique pre-shared Keys for devices.
B. Aruba ClearPass performs the 802.1X authentication and installs a certificate.
C. MPSK provides for each device in the WLAN to have its own unique pre-shared Key.
D. MPSK Local will allow the cameras to share a rey and the scanners to share a different

Answer: C

Explanation:
The best option to enhance security for the new IP cameras and scanners in this environment is C. MPSK provides for each device in the WLAN to have its own unique pre- shared key.
MPSK stands for Multi Pre-Shared Key, and it is a feature that allows different devices to connect to the same SSID with different pre-shared keys. This improves the security and scalability of the network, as each device can have its own key and role without requiring 802.1X authentication or an external policy engine. MPSK can be configured either locally on the AP or centrally on Aruba Central12.
The other options are incorrect because:
? A. MPSK Local is a feature that allows the user to configure 24 PSKs per SSID locally on the device. These local PSKs would serve as an extension of the base MPSK functionality. However, MPSK Local is not suitable for this scenario, as it can only support up to 24 devices per SSID, while the client has 250 devices1.
? B. Aruba ClearPass is a network access control solution that can perform 802.1X authentication and install certificates for devices. However, this option is not feasible for this scenario, as the new IP cameras and scanners do not support 802.1X authentication3.
? D. MPSK Local will not allow the cameras to share a key and the scanners to share a different key. MPSK Local will assign a different key to each device, regardless of their type. Moreover, MPSK Local can only support up to 24 devices per SSID, while the client has 250 devices1.

NEW QUESTION 32
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

Answer: D

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.

NEW QUESTION 35
For an Aruba AOS10 AP in mixed mode, which factors can be used to determine the forwarding role assigned to a client? (Select two.)

A. Client IP address
B. 802.1X authentication result
C. Client MAC address
D. Client SSID
E. Client VLAN

Answer: AD

Explanation:
? Client IP address: This factor can be used to determine if the client is on the same VLAN as the AP or not. If the client IP address is on the same VLAN as the AP, then the client traffic is bridged locally. If the client IP address is on a different VLAN than the AP, then the client traffic is forwarded to the gateway cluster through a secure tunnel 12.

? Client VLAN: This factor can be used to determine if the client belongs to a specific VLAN or not. If the client belongs to a specific VLAN, then the client traffic is forwarded to that VLAN based on its IP address and security profile 12.

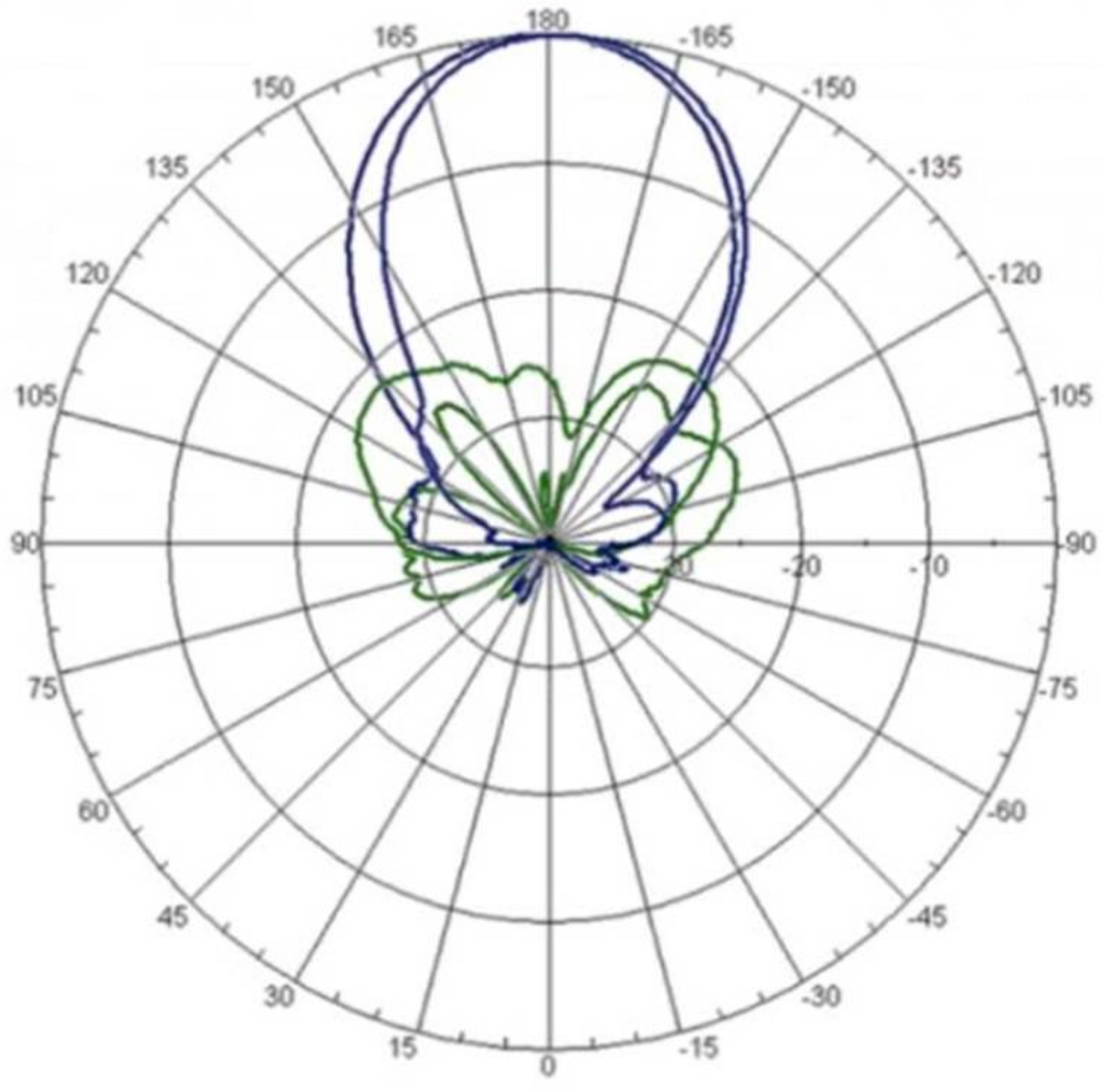
NEW QUESTION 37
You are working on a network where the customer has a dedicated router with redundant Internet connections Tor outbound high-importance real-time audio streams from their datacenter All of this traffic.
• originates from a single subnet
• uses a unique range of UDP ports
• is required 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 38
Refer to the image.



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

A. The AP is a remote access point.
B. The AP is using a directional antenna.

C. The AP is an outdoor access point.
D. The AP is configured in Mesh mode

Answer: B

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

NEW QUESTION 40
Your manufacturing client is having installers deploy seventy headless scanners and fifty IP cameras in their warehouse These new devices do not support 802 1X authentication.
How can HPE Aruba reduce the IT administration overhead associated with this deployment while maintaining a secure environment using MPSK?

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

Answer: C

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

NEW QUESTION 45
With the Aruba CX 6100 48G switch with uplinks of 1/1/47 and 1/1/48. how do you automate the process of resuming the port operational state once a loop on a client port is cleared?

A. Configure int 1/1/1-1/1/52 loop-protect disable timer.
B. Configure global loop-protect disable timer.
C. Configure int 1/1/1-1/1/46 loop-protect re-enable-timer.
D. Configure global loop-protect re-enable-timer.

Answer: C

Explanation:
Loop protection is a feature that detects and prevents loops in layer 2 networks. Loop protection can be enabled on ports, LAGs, or VLANs. When loop protection is enabled, the switch sends periodic loop protection messages on the interface and expects to receive them back. If a loop protection message is received back on the same interface, it indicates a loop and the switch takes an action to disable the interface or block traffic on it3. The loop-protect re-enable-timer command is used to configure the length of time the switch waits before re-enabling an interface that was disabled due to loop detection. The default value is 0, which means that the interface remains disabled until manually re-enabled3. To automate the process of resuming the port operational state once a loop on a client port is cleared, the loop-protect re-enable-timer command can be used with a non-zero value on the interface range that includes the client ports3. Therefore, answer C is correct. References: 1: Aruba Campus Access documents and learning resources 3: Configuring loop protection - Aruba

NEW QUESTION 50
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 54
You are deploying Aruba CX 6300's with the customers requirement to only allow one (1) VoIP phone and one (1) device.

The following local role gets assigned to the phone port-access rote VoIP device-traffic-class voice What set of commands best fits this requirement?

A. interface 1/1/1aaa authentication port-access client-limit 2aaa authentication port-access auth-mode client-mode
B. interface 1/1/1aaa authentication port-access auth-mode multi-domain
C. interface 1/1/1aaa authentication port-access client-limit multi-domain 2 aaa authentication port-access auth-mode multi-domain
D. interface 1/1/1aaa authentication port-access client-limit 1aaa authentication port-access auth-mode device-mode

Answer: C

Explanation:
Aruba CX 6300 switches support various features to control the port access for different types of devices, such as client mode, device mode, and multidomain mode. These features can help limit the number of clients that can connect to a port and prevent unauthorized devices from accessing the network.
This is because option C shows how to configure the client limit and the auth-mode for a specific port using the interface command and the aaa authentication port-access command. The client limit specifies the maximum number of clients that can connect to a port. The auth-mode specifies the authentication mode for the port. In this case, option C sets both parameters to multi-domain mode, which allows only one voice device and one data device to be authenticated on a port
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://www.arubanetworks.com/techdocs/AOS-CX/10.11/HTML/security_6200-6300-6400/Content/Chp_Port_acc/Port_acc_gen_cmds/aaa-aut-por-acc-aut-mod-fl-109.htm

NEW QUESTION 56
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 60
What is enabled by LLDP-MED? (Select two.)

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

Answer: AB

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

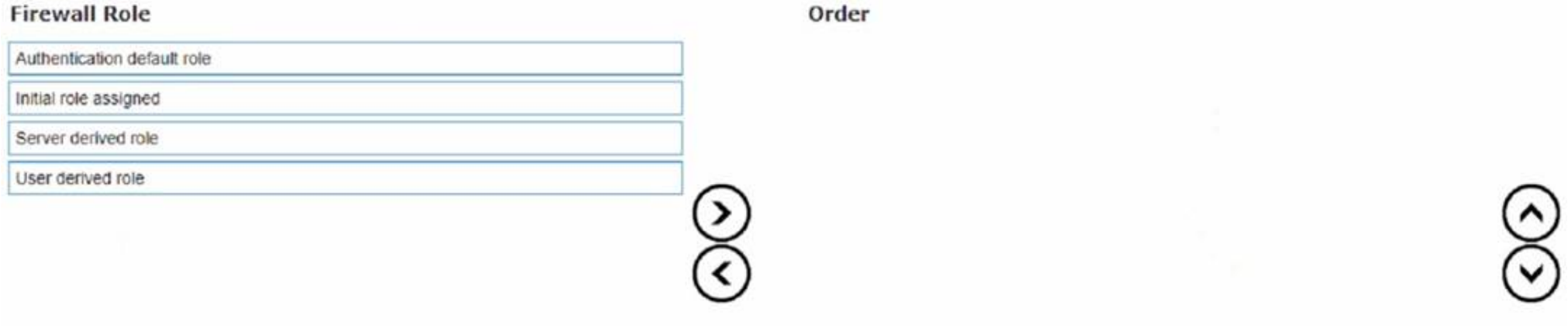
NEW QUESTION 64
Which statement best describes QoS?

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

Answer: A

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

NEW QUESTION 69
DRAG DROP
List the firewall role derivation flow in the correct order



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 73
You are setting up a customer's 15 headless loT 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 76
You are troubleshooting an issue with a pair of Aruba CX 8360 switches configured with VSX Each switch has multiple VRFs. You need to find the IP address of a particular client device with a known MAC address You run the "show arp" command on the primary switch in the pair but do not find a matching entry for the client MAC address.
The client device is connected to an Aruba CX 6100 switch by VSX LAG. Which action can be used to find the IP address successfully?
A)

Run the following command on the CX 6100 switch:
`show mac-address-table`

B)

Run the following command on the VSX primary switch:
`show arp all-vrfs`

C)

Run the following command on the VSX primary switch:
`show mac-address-table`

D)

Run the following command on the CX 6100 switch:
`show arp all-vrfs`

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

Answer: B

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

NEW QUESTION 80
DRAG DROP
List the WPA 4-Way Handshake functions in the correct order.

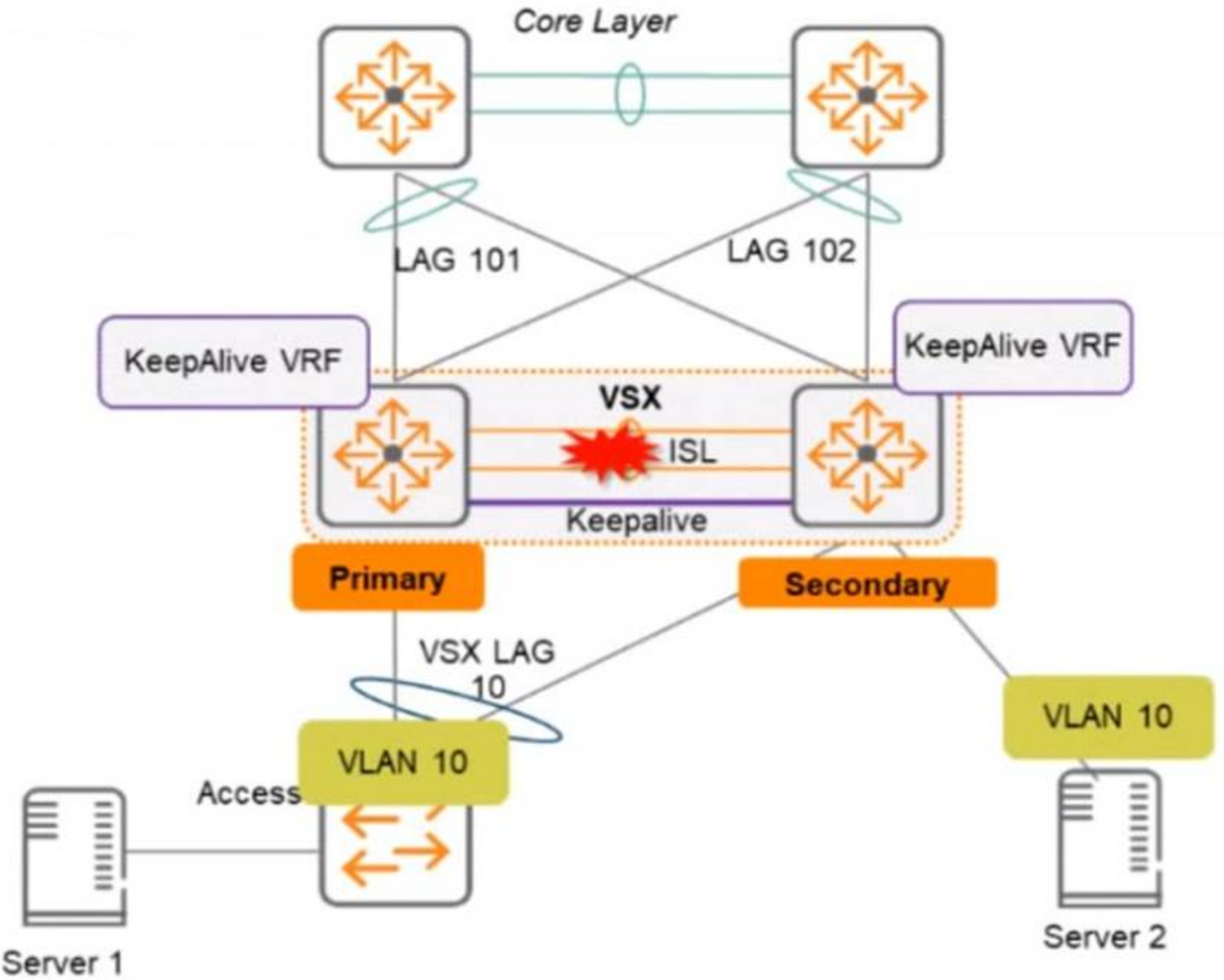
Function	Order
Distributes an encrypted GTK to the client	
Exchanges messages for generating PTK	
Proves knowledge of the PMK	
Sets first initialization vector (IV)	

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 84
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 85
You are deploying a bonded 40 MHz wide channel What is the difference in the noise floor perceived by a client using this bonded channel as compared to an unbonded 20MHz wide channel?

A. 2dB
B. 3dB
C. 8dB
D. 4dB

Answer: B

Explanation:
The difference in the noise floor perceived by a client using a bonded 40 MHz wide channel as compared to an unbonded 20 MHz wide channel is 3 dB. The noise floor is the level of background noise in a given frequency band. When two adjacent channels are bonded, the noise floor increases by 3 dB because the bandwidth is doubled and more noise is captured. The other options are incorrect because they do not reflect the correct relationship between bandwidth and noise floor. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/rf-fundamentals.htm https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/wlan-rf/channel-bonding.htm

NEW QUESTION 86
Which method is used to onboard a new UXI in an existing environment with 802 1X authentication? (The sensor has no cellular connection)

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

Answer: A

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

NEW QUESTION 91
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 93
your customer has asked you to assign a switch management role for a new user The customer requires the user role to View switch configuration information and have access to the PUT and POST meth0ds for REST API.
Which default AOS-CX user role meets these requirements?

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

Answer: C

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

NEW QUESTION 96
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 98
A network administrator is troubleshooting some issues guest users are having when connecting and authenticating to the network The access switches are AOS-CX switches.
What command should the administrator use to examine information on which role the guest user has been assigned?

A. show aaa authentication port-access interface all client-status
B. show port-access captiveportal profile
C. show port-access role
D. diag-dump captiveportal client verbose

Answer: A

Explanation:
The show aaa authentication port-access interface all client-status command displays the status of all clients authenticated by port-based access control on all interfaces. The output includes the MAC address, user role, VLAN ID, and session timeout for each client. This command can be used to examine information on which role the guest user has been assigned by the AOS-CX switch. References: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

NEW QUESTION 102
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.

Answer: A

Explanation:
The correct answer is A. DMO is configured individually for each SSID in use in the network.
DMO is a feature that allows the AP to convert multicast streams into unicast streams over the wireless link. This enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. DMO is configured individually for each SSID in use in the network, as different SSIDs may have different multicast requirements.
According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure DMO is:
? Dynamic multicast optimization: Select Enabled to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients.
The other options are incorrect because:
? B. The AP does not use QoS to provide equal air time for multicast traffic. QoS is a feature that prioritizes different types of traffic based on their importance and latency sensitivity. QoS does not affect how multicast streams are transmitted over the wireless link.
? C. DMO is not configured globally for each SSID in use in the network. DMO is configured individually for each SSID, as different SSIDs may have different multicast requirements.
? D. The controller does not convert multicast streams into unicast streams. The AP does the conversion, as it is closer to the wireless clients and can optimize the transmission based on the client capabilities and channel conditions.

NEW QUESTION 105
A customer is looking Tor a wireless authentication solution for all of their loT devices that meet the following requirements
- The wireless traffic between the IoT devices and the Access Points must be encrypted
- Unique passphrase per device
- Use fingerprint information to perform role-based access
Which solutions will address the customer's requirements? (Select two.)
A. MPSK and an internal RADIUS server
B. MPSK Local with MAC Authentication
C. ClearPass Policy Manager
D. MPSK Local with EAP-TLS
E. Local User Derivation Rules

Answer: CD

Explanation:
The correct answers are C and D.
MPSK (Multi Pre-Shared Key) is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices1. MPSK requires MAC authentication against a ClearPass Policy Manager server, which returns the encrypted passphrase for the device in a RADIUS VSA2. ClearPass Policy Manager is a platform that provides role-and device-based network access control for any user across any wired, wireless and VPN infrastructure3. ClearPass Policy Manager can also use device profiling and posture assessment to assign roles based on device fingerprint information4.
MPSK Local is a variant of MPSK that allows the user to configure up to 24 PSKs per SSID locally on the device, without requiring ClearPass Policy Manager5. MPSK Local can be combined with EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), which is a secure authentication method that uses certificates to encrypt the wireless traffic between the IoT devices and the access points6. EAP-TLS can also use device certificates to perform role-based access control6.
Therefore, both ClearPass Policy Manager and MPSK Local with EAP-TLS can meet the customer??s requirements for wireless authentication, encryption, unique passphrase, and role-based access for their IoT devices.
MPSK and an internal RADIUS server is not a valid solution, because MPSK does not support internal RADIUS servers and requires ClearPass Policy Manager789. MPSK Local with MAC Authentication is not a valid solution, because MAC Authentication does not encrypt the wireless traffic or use fingerprint information for role-based access2. Local User Derivation Rules are not a valid solution, because they do not provide unique passphrase per device or use fingerprint information for role-based access101112.

NEW QUESTION 109
Which statements are true about VSX LAG? (Select two.)

A. The total number of configured links may not exceed 8 for the pair or 4 per switch
B. Outgoing traffic is switched to a port based on a hashing algorithm which may be either switch in the pair
C. LAG traffic is passed over VSX ISL links only while upgrading firmware on the switch pair
D. Outgoing traffic is preferentially switched to local members of the LAG.
E. Up to 255 VSX lags can be configured on all 83xx and 84xx model switches.

Answer: AD

Explanation:
The correct answers are A and D.
According to the web search results, VSX LAG is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices1. VSX LAGs span both aggregation switches and appear as one device to partner downstream or upstream devices or both when forming a LAG with the VSX pair2.
One of the statements that is true about VSX LAG is that the total number of configured links may not exceed 8 for the pair or 4 per switch1. This means that a VSX LAG across a downstream switch can have at most a total of eight member links, and a switch can have a maximum of four member links. When creating a VSX LAG, it is recommended to select an equal number of member links in each segment for load balancing1.
Another statement that is true about VSX LAG is that outgoing traffic is preferentially switched to local members of the LAG2. This means that when active forwarding and active gateway are enabled, north-south and south-north traffic bypasses the ISL link and uses the local ports on the switch. This optimizes the traffic path and reduces the load on the ISL link2.
The other statements are false or not relevant for VSX LAG. Outgoing traffic is not switched to a port based on a hashing algorithm, which may be either switch in the pair. This is a characteristic of MLAG (Multi-Chassis Link Aggregation), which is a different feature from VSX LAG. LAG traffic is not passed over VSX ISL links only while upgrading firmware on the switch pair. This is a scenario that may occur when performing hitless upgrades, which is a feature that allows software updates without impacting network availability. The number of VSX lags that can be configured on all 83xx and 84xx model switches is not 255, but depends on the switch model and firmware version. For example, the AOS-CX 10.04 supports up to 64 VSX lags for 8320 switches and up to 128 VSX lags for 8325 and 8400 switches.

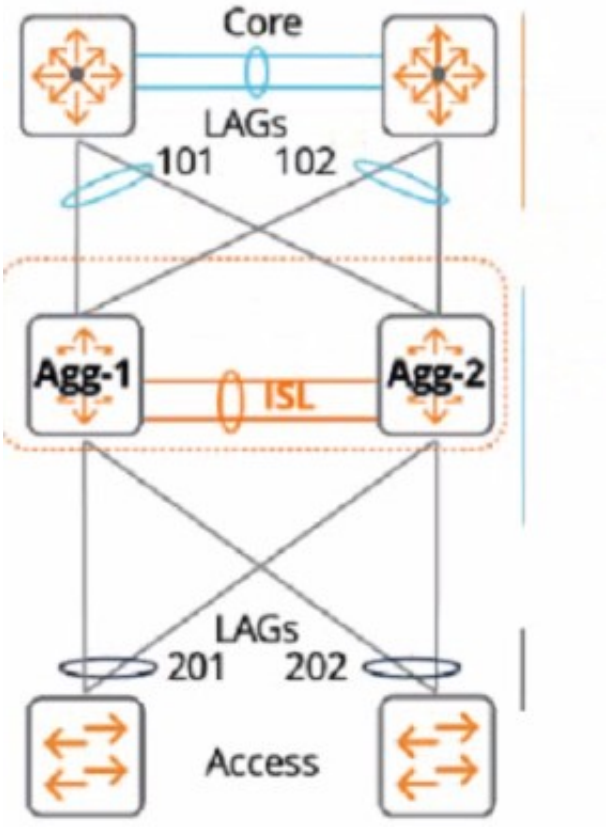
NEW QUESTION 110
Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements After the configuration was complete, it was noted that a user assigned with the administrators role did not have the appropriate level of access on the 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 112
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 115
Which statements are true regarding a VXLAN implementation on Aruba Switches? (Select two.)

A. MTU size must be increased beyond the default
B. VNIs encapsulate and decapsulate VXLAN traffic
C. VTEPs encapsulate and decapsulate VXLAN traffic
D. They are only available for datacenter switches (CX 8k, 9k,10k)
E. All Aruba CX switches support VXLAN.

Answer: AB

Explanation:
Option A: MTU size must be increased beyond the default
This is because option A shows how to configure the MTU size for VXLAN tunnels on Aruba switches using the interface command and the vxlan command. The MTU size must be increased beyond the default value of 1500 bytes to accommodate the VXLAN header and payload2.
Therefore, option A is true regarding a VXLAN implementation on Aruba switches. Option B: VNIs encapsulate and decapsulate VXLAN traffic
This is also true regarding a VXLAN implementation on Aruba switches. VNIs are used to encapsulate and decapsulate VXLAN traffic between two devices, such as a switch and a server. VNIs are also used to map VXLAN tunnels to overlay networks3.
Therefore, option B is also true regarding a VXLAN implementation on Aruba switches. VXLAN is a Layer 2 encapsulation technology that substitutes the usage of VLAN numbers to label Ethernet broadcast domains with VXLAN numbers. VXLAN supports 224 Ethernet broadcast domains or VXLAN numbers. A VXLAN number ID is referred to as VNI. There is a one-to-one relationship between an Ethernet broadcast domain and a VNI. A single Ethernet broadcast domain can??t have more than one VNI.

NEW QUESTION 117
Which Aruba AP mode is sending captured RF data to Aruba Central for waterfall plot?

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

Answer: C

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

NEW QUESTION 121
A customer has a large number of food-producing machines
• All machines are connected via Aruba CX6200 switches in VLANs 100.110. and 120
• Several external technicians are maintaining this special equipment
What are the correct commands to ensure that no rogue DHCP server will impact the network?
A)

```
dhcp-snooping enable
no dhcp-snooping option 82
dhcp-snooping vlan 100-120
vlan 100
    name cornflakes
vlan 110
    name cornmill
vlan 120
    name packaging


interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcp-snooping trust
```

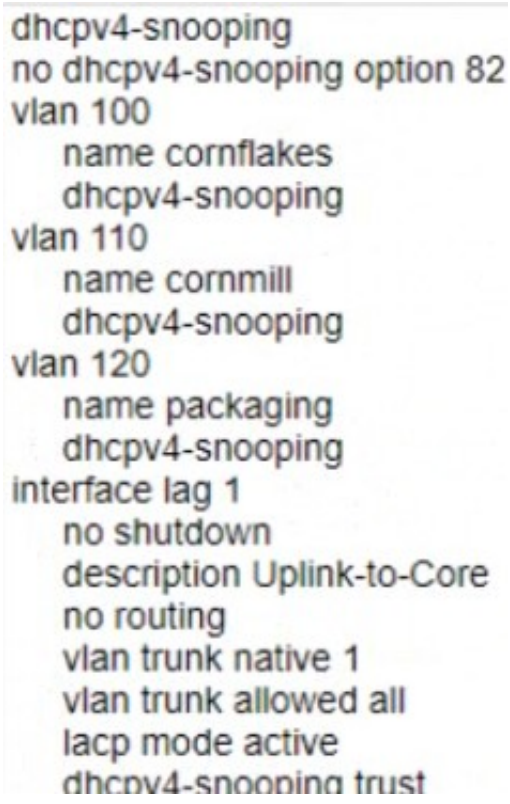
B)

```
dhcp snooping enable
no dhcp-snooping option 82
vlan 100
    name cornflakes
    dhcp-snooping
vlan 110
    name cornmill
    dhcp-snooping
vlan 120
    name packaging
    dhcp-snooping
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcp snooping trust
```

C)

```
dhcpv4-snooping all vlans
no dhcpv4-snooping option 82
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcpv4-snooping trust
```

D)


```
dhcpv4-snooping
no dhcpv4-snooping option 82
vlan 100
    name cornflakes
    dhcpv4-snooping
vlan 110
    name cornmill
    dhcpv4-snooping
vlan 120
    name packaging
    dhcpv4-snooping
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcpv4-snooping trust
```

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

Answer: B

Explanation:
configures DHCP snooping on the switch and enables it for VLANs 100, 110, and 120. It also specifies the IP address of the authorized DHCP server and sets the ports connected to the server as trusted. This prevents any unauthorized DHCP server from providing invalid configuration data to the clients on those VLANs. Option B also enables DHCP option-82, which adds information about the switch port and VLAN to the DHCP packets, allowing for more granular control and logging of DHCP transactions.

NEW QUESTION 123
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your HPE7-A01 Exam with Our Prep Materials Via below:

https://www.certleader.com/HPE7-A01-dumps.html