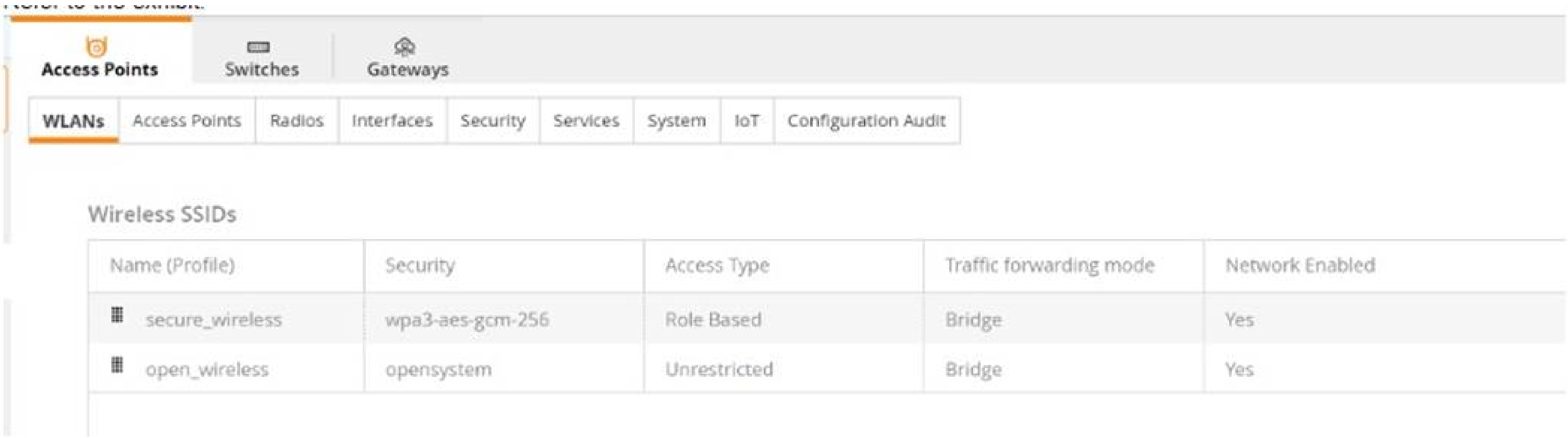
HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam

NEW QUESTION 1
Refer to Exhibit:



Wireless SSIDs

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

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

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

Answer: C

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

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

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

Answer: B

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

NEW QUESTION 3
For the Aruba CX 6400 switch, what does virtual output queueing (VOQ) implement that is different from most typical campus switches?

A. large ingress packet buffers
B. large egress packet buffers
C. per port ASICs
D. VSX

Answer: A

Explanation:
The Aruba CX 6400 switch is a modular switch that supports high- performance and high-density Ethernet switching for campus and data center networks. One of the features that distinguishes the Aruba CX 6400 switch from most typical campus switches is virtual output queueing (VOQ). VOQ is a technique that implements large ingress packet buffers on each port to prevent head-of-line blocking and packet loss due to congestion2. VOQ allows each port to have multiple queues for different output ports and prioritize packets based on their destination and QoS class2. VOQ enables the Aruba CX 6400 switch to achieve high throughput and low latency for various traffic types and
scenarios. References: 2 https://www.arubanetworks.com/assets/ds/DS_CX6400Series.pdf

NEW QUESTION 4
A customer is using Aruba Cloud Guest, but visitors keep complaining that the captive portal page keeps coming up after devices go to sleep Which solution should be enabled to deal with this issue?

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

Answer: A

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

NEW QUESTION 5
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 6
You are doing tests in your lab and with the following equipment specifications:
- AP1 has a radio that generates a 20 dBm signal
- AP2 has a radio that generates a 8 dBm signal
- AP1 has an antenna with a gain of 7 dBI.
- AP2 has an antenna with a gain of 12 dBI.
- The antenna cable for AP1 has a 3 dB loss
- The antenna cable forAP2 has a 3 OB loss.

What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?

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

Answer: B

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

NEW QUESTION 7
When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

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

Answer: B

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

NEW QUESTION 8
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 9
By default, Best Effort is higher priority than which priority traffic type?

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

Answer: B

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

NEW QUESTION 10
What is used to retrieve data stored in a Management Information Base (MIS)?

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

Answer: A

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

NEW QUESTION 10
How do you allow a new VLAN 100 between VSX pair inter-switch-link 256 for port 1/45 and 2/45?

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

Answer: C

Explanation:
To allow a new VLAN 100 between VSX pair inter-switch-link 256 for port 1/45 and 2/45, you need to use the command vlan trunk allowed 100 in LAG256. This will add VLAN 100 to the list of allowed VLANs on the trunk port LAG256, which is part of the inter-switch-link between VSX peers. The other options are incorrect because they either do not use the correct command or do not specify the correct port or VLAN. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch07.html https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6728/bk01-ch02.html

NEW QUESTION 13

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

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

Answer: C

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

NEW QUESTION 18
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 19
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 22
A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working to a remote site connected via layer-3 All legacy devices are connected to a dedicated Aruba CX 6200 switch at each site.
What technology on the Aruba CX 6200 could be used to meet this requirement?

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

Answer: A

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

NEW QUESTION 24
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 25
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 28
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

Answer: AC

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. References: 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

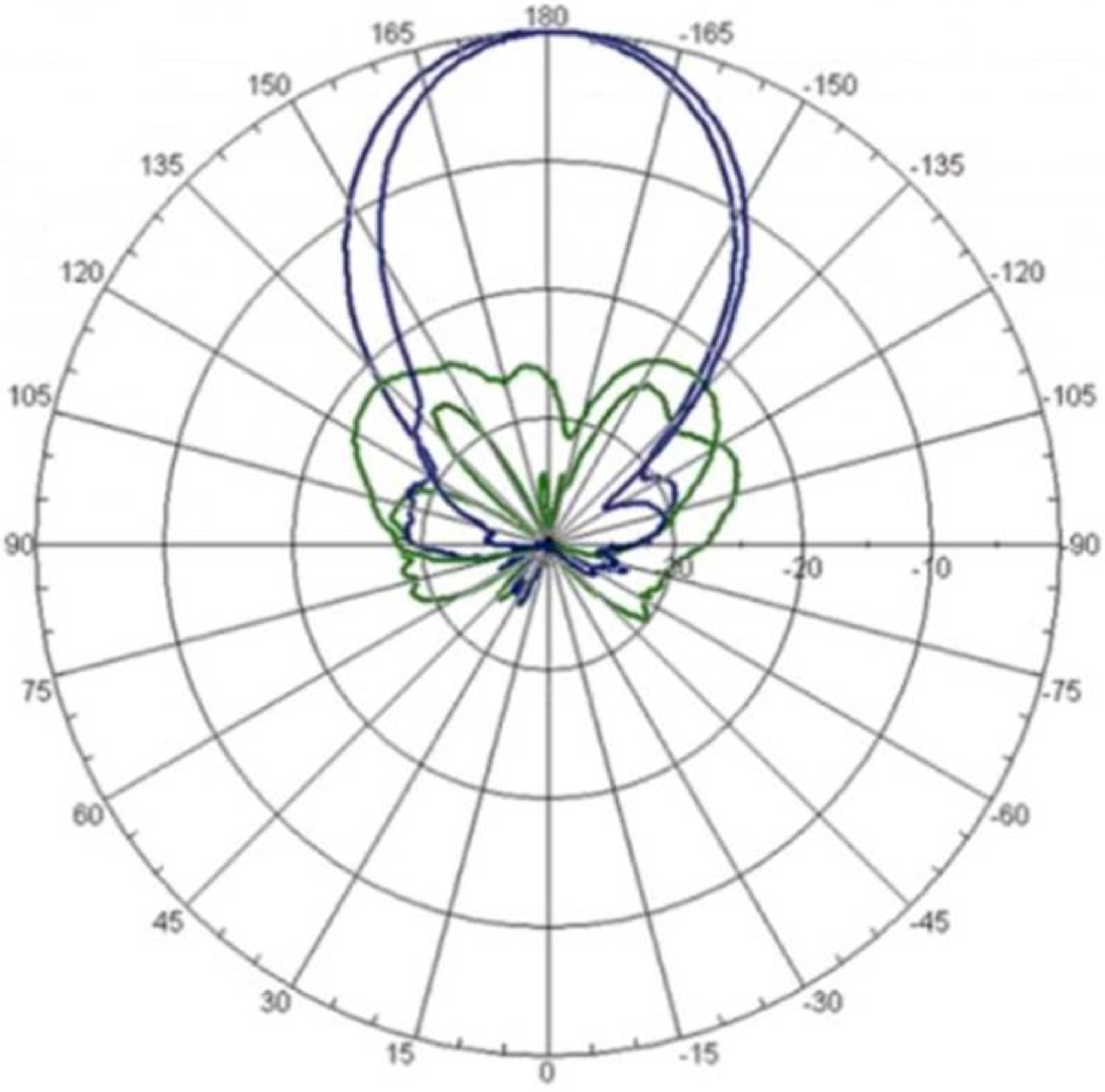
NEW QUESTION 33
You are working on a network where the customer has a dedicated router with redundant Internet connections Tor outbound high-importance real-time audio streams from their datacenter All of this traffic.
• originates from a single subnet
• uses a unique range of UDP ports
• is required 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 36
Refer to the image.



Horizontal Pattern

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

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

Answer: B

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

NEW QUESTION 38
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.

Answer: C

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.

NEW QUESTION 42
With the Aruba CX switch configuration, what is the Active Gateway feature that is used for and is unique to VSX configuration?

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

Answer: A

Explanation:
Active gateway is a first hop redundancy protocol that eliminates a single point of failure. The active gateway feature is used to increase the availability of the default gateway servicing hosts on the same subnet. An active gateway improves the reliability and performance of the host network by enabling a virtual router to act as the default gateway for that network. If you have enabled active gateway, VRRP is not required3. Active gateway is similar to VRRP in that routed traffic from the VSX node is sourced from the switch interface MAC and not the virtual MAC address (VMAC). Each active gateway sends a periodic broadcast hello packet to avoid VMAC aging on the access switches. The switch views the active gateway IP as a self IP address3. Active gateway is preferable over VRRP because with VRRP traffic is still pushed over the ISL link, resulting in latency in the network3. Therefore, VRRP and active gateway are mutually exclusive on a VLAN, and answer A is correct.
References: 1: Aruba Campus Access documents and learning resources 3: Active gateway over VSX - Aruba

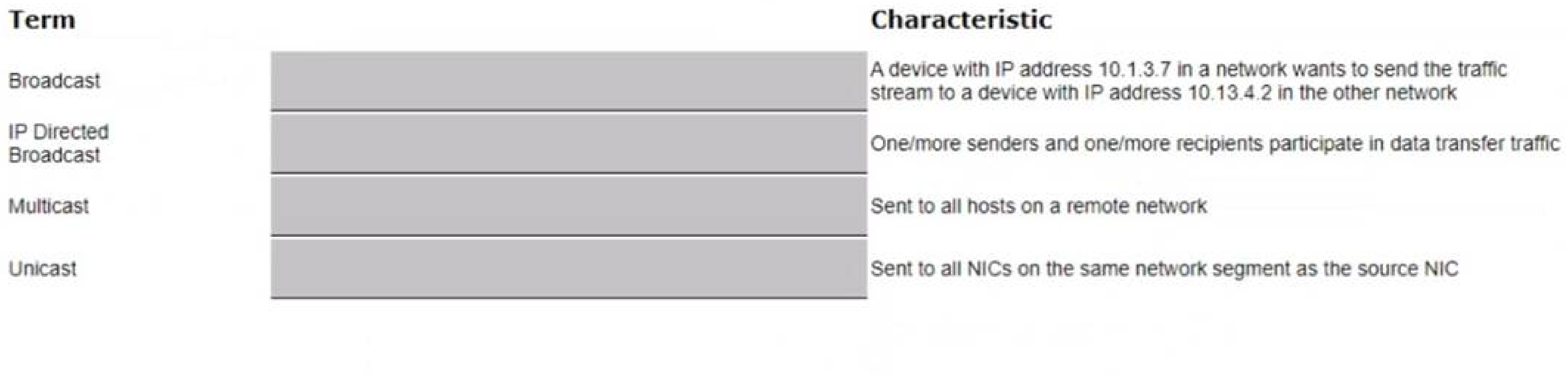
NEW QUESTION 44
Which statements regarding 0SPFv2 route redistribution are true for Aruba OS CX switches? (Select two.)

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

Answer: AE

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

NEW QUESTION 46
DRAG DROP
Match the terms below to their characteristics (Options may be used more than once or not at all.)

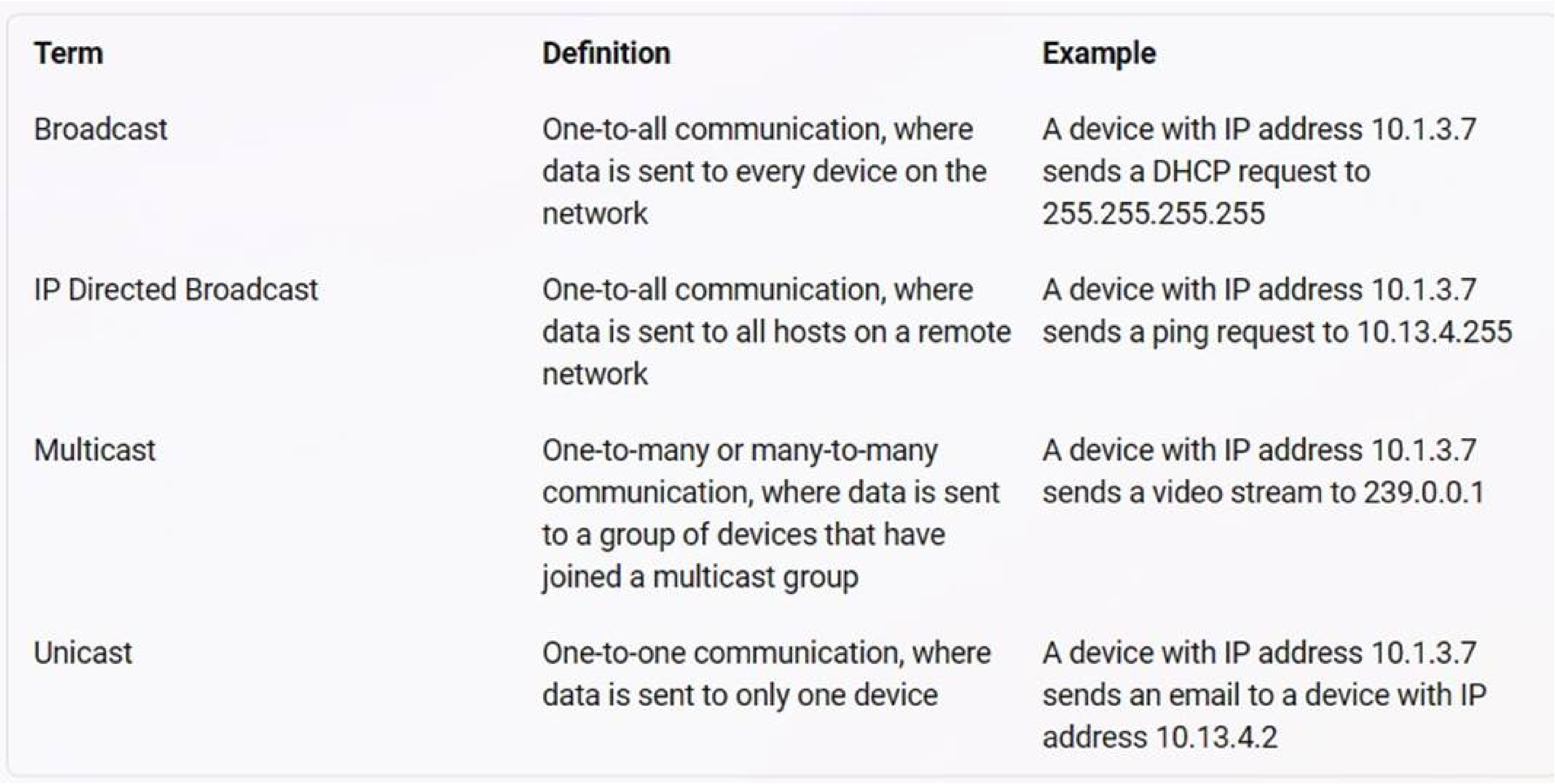


Term		Characteristic
Broadcast		A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address 10.13.4.2 in the other network
IP Directed Broadcast		One/more senders and one/more recipients participate in data transfer traffic
Multicast		Sent to all hosts 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 50
A customer wants to enable wired authentication across all their CX switches One of the requirements is that the switch must be able to authenticate a single computer connected through a VoIP phone.
Which feature should be enabled to support this requirement?

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

Answer: A

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

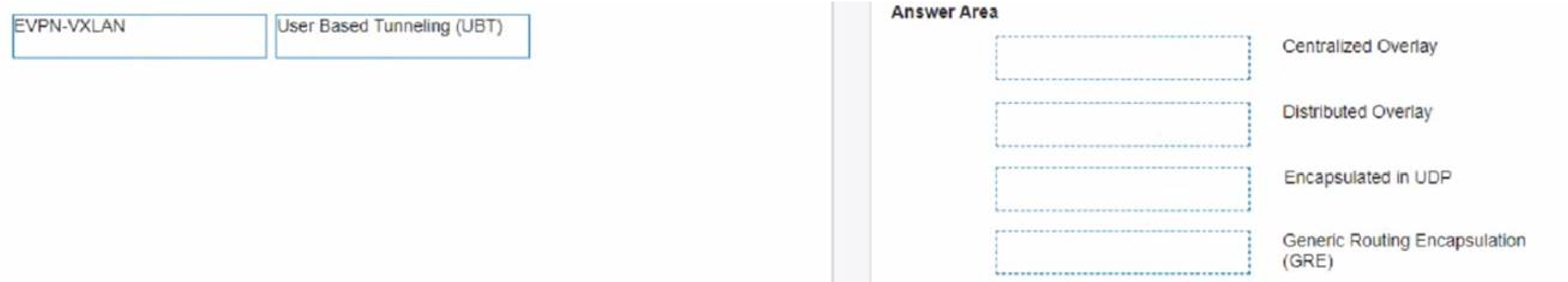
NEW QUESTION 51
you are implementing ClearPass Policy Manager with EAP-TLS for authenticating all corporate-owned devices.
What are two possible solutions to the problem of deploying client certificates to corporate MacBooks that are joined to a Windows domain? (Select two.)

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

Answer: AB

Explanation:
The reason is that ClearPass OnBoard is a tool that allows you to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate. This certificate can be obtained from Apple or from a third-party PKI provider.
Apple Configurator is a tool that allows you to configure and deploy Mac computers using a GPO. This tool can also be used to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate.

NEW QUESTION 52
DRAG DROP
Match the topics with the underlying technologies (Options may be used more than once or not at all.)



EVPN-VXLAN

User Based Tunneling (UBT)

Answer Area

Centralized Overlay

Distributed Overlay

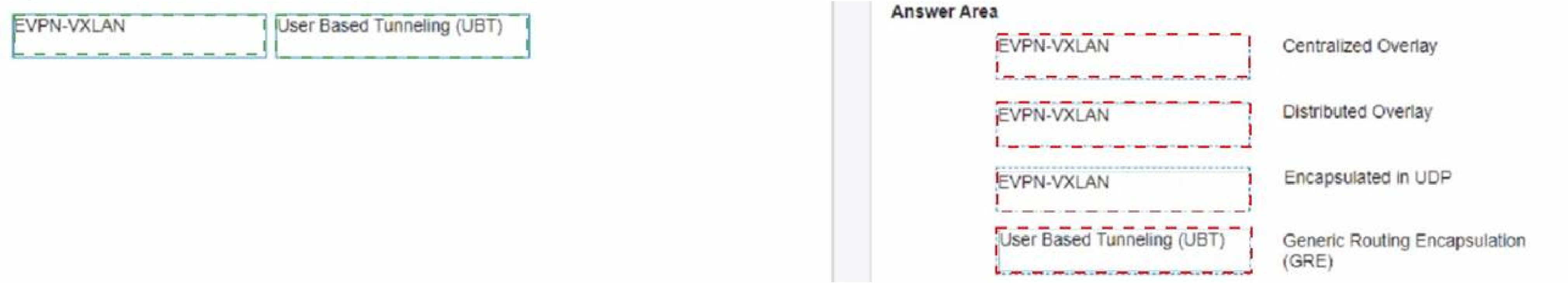
Encapsulated in UDP

Generic Routing Encapsulation (GRE)

A. Mastered
B. Not Mastered

Answer: A

Explanation:



EVPN-VXLAN

User Based Tunneling (UBT)

Answer Area

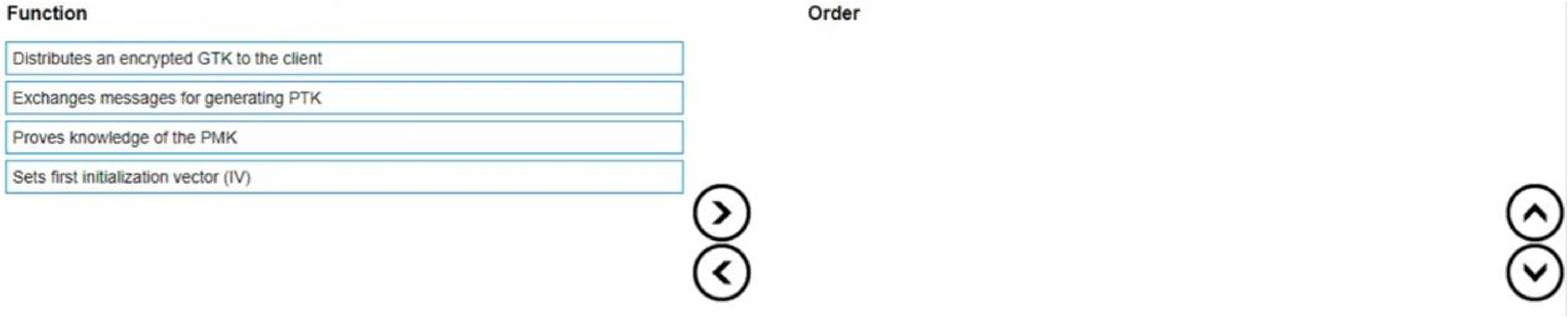
EVPN-VXLAN Centralized Overlay

EVPN-VXLAN Distributed Overlay

EVPN-VXLAN Encapsulated in UDP

User Based Tunneling (UBT) Generic Routing Encapsulation (GRE)

NEW QUESTION 57
DRAG DROP
List the WPA 4-Way Handshake functions in the correct order.



Function

Distributes an encrypted GTK to the client

Exchanges messages for generating PTK

Proves knowledge of the PMK

Sets first initialization vector (IV)

Order

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 60
Which feature supported by SNMPv3 provides an advantage over SNMPv2c?

A. Transport mapping
B. Community strings
C. GetBulk
D. Encryption

Answer: D

Explanation:
Encryption is a feature supported by SNMPv3 that provides an advantage over SNMPv2c. Encryption protects the confidentiality and integrity of SNMP messages by encrypting them with a secret key. SNMPv2c does not support encryption and relies on community strings for authentication and authorization, which are transmitted in clear text and can be easily intercepted or spoofed. Transport mapping, community strings, and GetBulk are features that are common to both SNMPv2c and SNMPv3. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/snmp/snmp.htm https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmpv3.htm

NEW QUESTION 61
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 65
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 67
A customer wants to deploy a Gateway and take advantage of all the SD-WAN features. Which persona role option should be selected?

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

Answer: A

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

NEW QUESTION 70
A network administrator is attempting to troubleshoot a connectivity issue between a group of users and a particular server The administrator needs to examine the packets over a period of time from their desktop; however, the administrator is not directly connected to the AOS-CX switch involved with the traffic flow.
What statements are correct regarding the ERSPAN session that needs to be established on an AOS-CX switch'? (Select two)

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

Answer: BE

Explanation:
These are the correct statements regarding the ERSPAN session that needs to be established on an AOS-CX switch for a network administrator to examine the packets over a period of time from their desktop. ERSPAN (Encapsulated Remote Switched Port Analyzer) is a feature that allows an AOS-CX switch to mirror traffic from one or more source ports or VLANs to a remote destination IP address over a GRE (Generic Routing Encapsulation) tunnel. The destination IP address must be the IP address of the administrator??s desktop, which must have a packet capture tool installed to receive and analyze the mirrored traffic. The encapsulation protocol used for ERSPAN is GRE, which adds a header to the mirrored packets with information such as source and destination IP addresses,

session ID, etc. The other statements are incorrect because they either do not specify the correct destination IP address or do not use ERSPAN or GRE.
References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch02.html https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6728/bk01-ch03.html

NEW QUESTION 72
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 75
What is an OSPF transit network?

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

Answer: A

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

NEW QUESTION 80
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

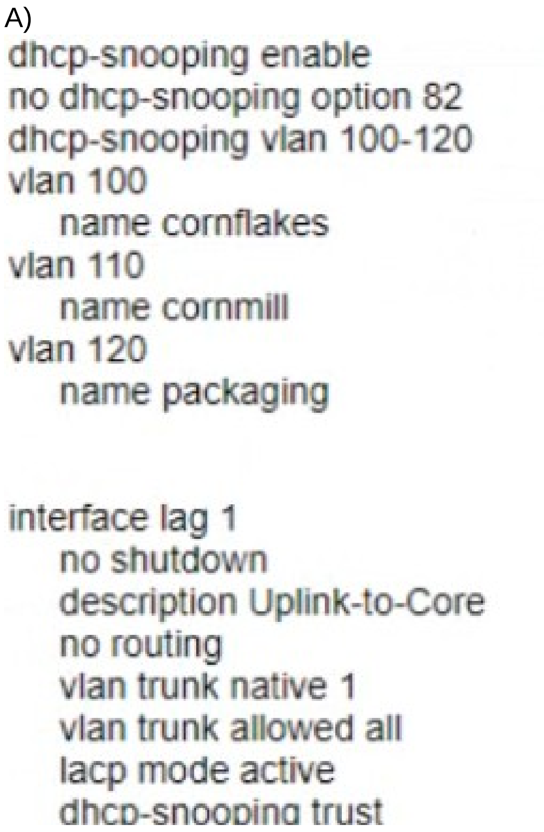
Answer: B

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 82
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

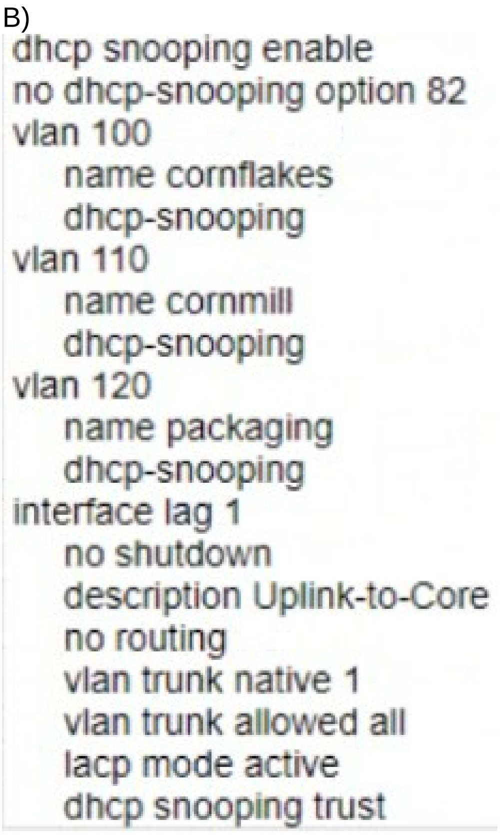
What are the correct commands to ensure that no rogue DHCP server will impact the network?

A)



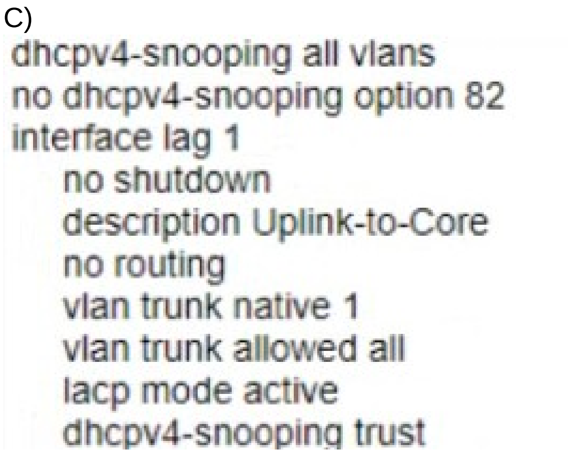
```
dhcp-snooping enable
no dhcp-snooping option 82
dhcp-snooping vlan 100-120
vlan 100
    name cornflakes
vlan 110
    name cornmill
vlan 120
    name packaging


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)



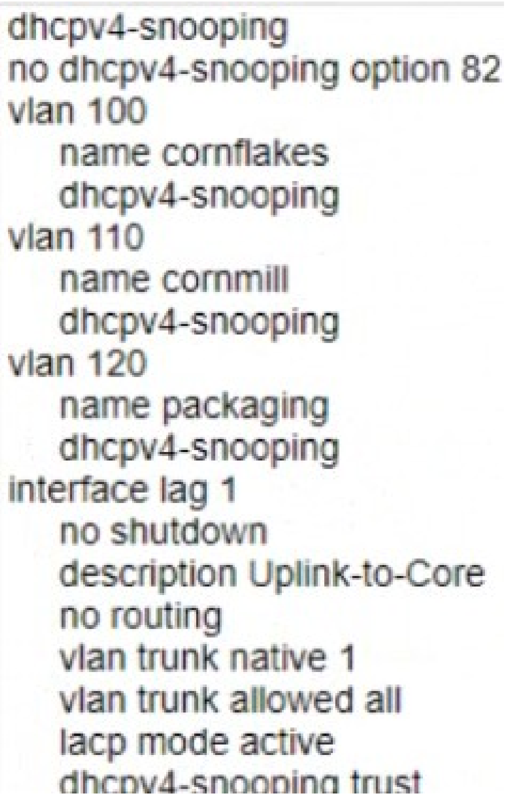
```
dhcp snooping enable
no dhcp-snooping option 82
vlan 100
    name cornflakes
    dhcp-snooping
vlan 110
    name cornmill
    dhcp-snooping
vlan 120
    name packaging
    dhcp-snooping
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan 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)



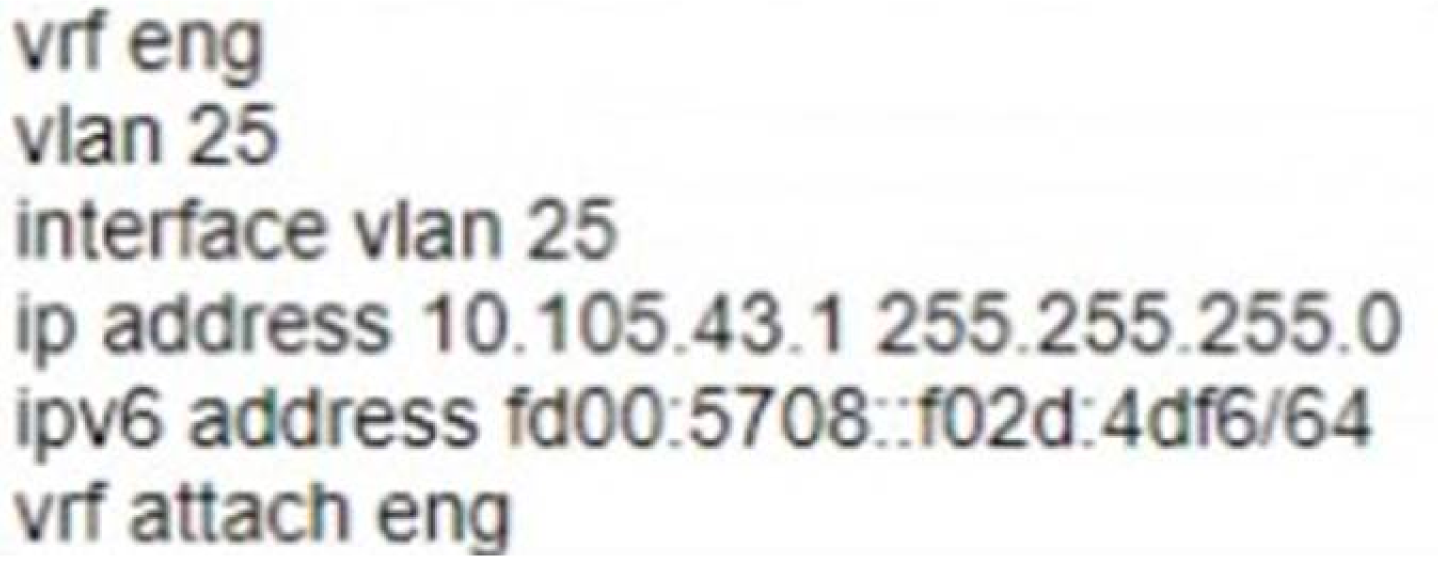
```
dhcpv4-snooping
no dhcpv4-snooping option 82
vlan 100
    name cornflakes
    dhcpv4-snooping
vlan 110
    name cornmill
    dhcpv4-snooping
vlan 120
    name packaging
    dhcpv4-snooping
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan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

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

Answer: B

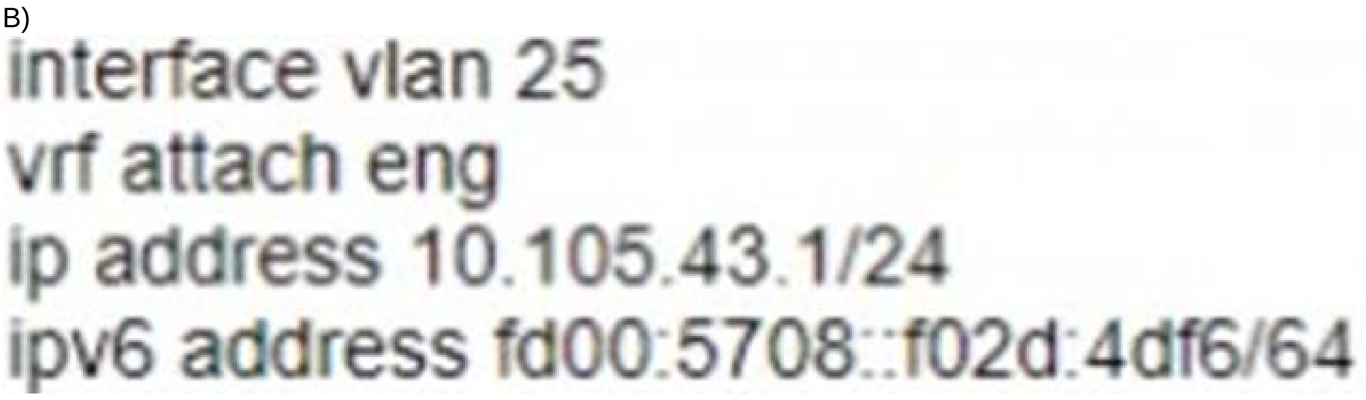
Explanation:
configures DHCP snooping on the switch and enables it for VLANs 100, 110, and 120. It also specifies the IP address of the authorized DHCP server and sets the ports connected to the server as trusted. This prevents any unauthorized DHCP server from providing invalid configuration data to 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 86
You are configuring an SVI on an Aruba CX switch that needs to have the following characteristics:
• VLANID = 25
. IPv4 address 10 105 43 1 with mask 255 255 255.0
• IPv6 address fd00:5708::f02d:4df6 with a 64 bit prefix length
• member of VRF eng
• VRF eng and VLAN 25 have not yet been created
Which command lists will satisfy the requirements with the least number of commands?
A)



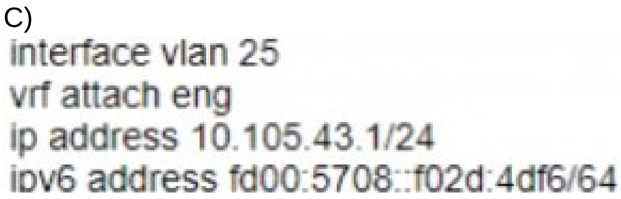
```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43.1 255.255.255.0
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

B)



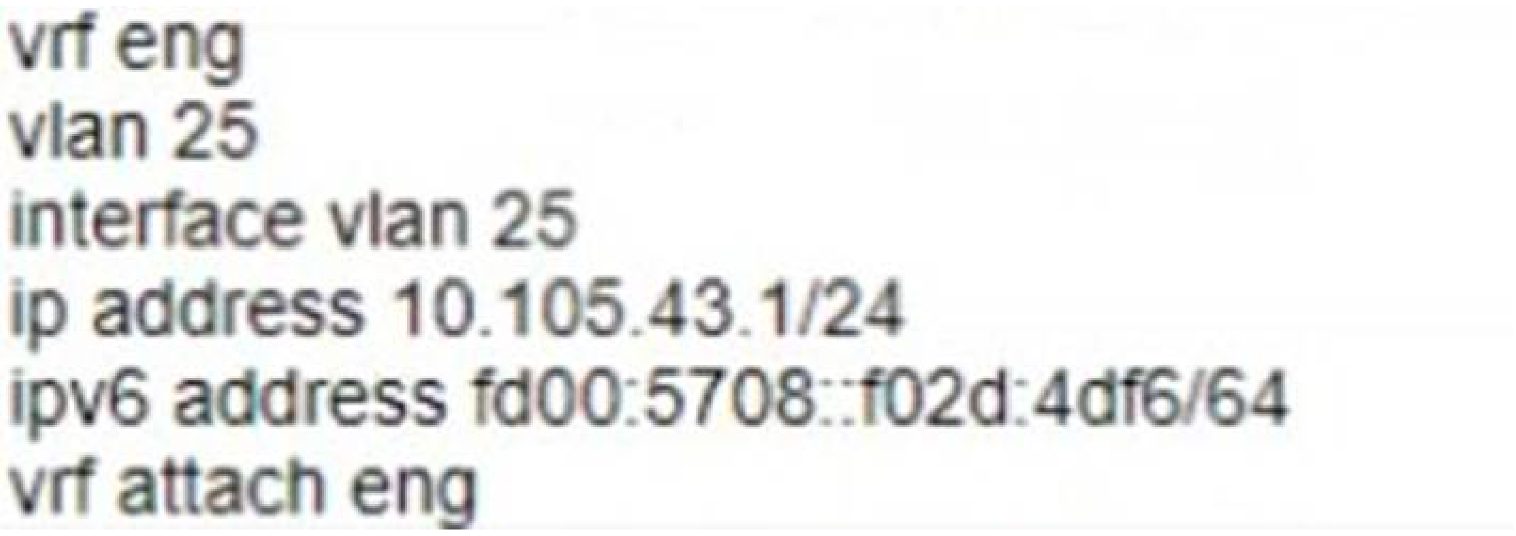
```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
```

C)



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

D)



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

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

Answer: C

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

NEW QUESTION 89
......