



**HP**

## **Exam Questions HPE7-A01**

Aruba Certified Campus Access Professional Exam

**NEW QUESTION 1**

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

A)

On the new switch issue:

```
vsf member 1
  link 1 1/1/50
  link 2 1/1/49
vsf renumber-to 3
```

B)

On the new switch issue:

```
vsf member 3
  type jl726a
```

C)

On the existing VSF issue:

```
vsf member 3
  stack join
  type jl726a
```

D)

On the new switch issue:

```
vsf member 1
  type jl726a
  link 1 3/1/50
  link 2 3/1/49
```

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

**Answer: C**

**Explanation:**

According to the Aruba Documentation Portal<sup>1</sup>, the Aruba CX 6200F VSF stack is a feature that allows you to create a virtual switching framework (VSF) with up to eight members that can be managed as a single logical device. The VSF stack provides benefits such as load balancing, failover, redundancy, and security. To add a new device to the VSF stack, you need to configure the device with the VSF command vsf member and specify the type, link, and secondary-member information. The type of the new device can be one of the following: JL726A, JL726B, JL726C, or JL726D. The link is the interface that connects the new device to the existing VSF members. The secondary-member is an optional parameter that specifies which member will act as a backup in case of a failure.

1: <https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7726/index.html> 2: <https://buy.hpe.com/us/en/networking/switches/fixed-port-l3-managed-ethernet-switches/6000-switch-products/aruba-6200f-48g-4sfp-switch/p/jl726a> 3: <https://addin.co.th/shop/switch/aruba-switch/6200f-series/jl726a/>

**NEW QUESTION 2**

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

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

**Answer: C**

**Explanation:**

According to the Aruba Documentation Portal<sup>1</sup>, the ArubaOS-CX switch supports various features to control the ingress traffic on specific ports, such as rate limiting, QoS shaping, and access control. These features can help reduce the impact of excessive broadcast traffic on the network performance and availability. This is because rate limiting is a feature that allows you to limit the inbound or outbound traffic on a port based on a percentage of the port capacity or a fixed amount of bytes per second. Rate limiting can help prevent broadcast storms by reducing the amount of broadcast packets that enter or leave a port

<https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-access-control.htm> 2:

<https://community.arubanetworks.com/blogs/esupport1/2021/02/08/broadcast-storm-containment-in-aruba-pvos-switches> 3:

[https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8160\\_ssw\\_mcg/content/ch05.html](https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8160_ssw_mcg/content/ch05.html)

**NEW QUESTION 3**

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 plane<sup>3</sup>. 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 segments<sup>3</sup>. EVPN-VXLAN also provides benefits such as loop prevention, load balancing, mobility, and scalability<sup>3</sup>. References: 3

[https://www.arubanetworks.com/assets/tg/TG\\_EVPN\\_VXLAN.pdf](https://www.arubanetworks.com/assets/tg/TG_EVPN_VXLAN.pdf)

**NEW QUESTION 4**

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](https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf)

**NEW QUESTION 5**

Your customer is having issues with Wi-Fi 6 clients staying connected to poor-performing APs when a higher throughput APs are closer. Which technology should you implement?

- A. Clearpass
- B. ClientMatch
- C. Airmatch
- D. ARM

**Answer: B**

**Explanation:**

Wi-Fi 6 is an industry certification for products that support the new wireless standard 802.11ax, also known as ??high-efficiency wireless??. Wi-Fi 6 offers increased capacities, improved resource utilization and higher throughput speeds than previous standards.

Option B: ClientMatch

This is because option B shows how to use ClientMatch to optimize the wireless performance of Wi-Fi 6 clients on a UniFi network. ClientMatch is a feature that uses machine learning to analyze the traffic patterns of each client and assign them to the best available AP based on their location, device type, and network conditions<sup>2</sup>.

Therefore, option B is the best technology to implement for your customer's issue.

1: <https://help.ui.com/hc/en-us/articles/221029967-UniFi-Network-Optimizing-Wireless-Connectivity> 2: <https://help.ui.com/hc/en-us/articles/360012947634-UniFi-Network-Optimizing-Wireless-Speeds>

#### 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 Concentrator<sup>1</sup> However, the Mobility persona is only available when configuring a Gateway-only group, which is a group that contains only one gateway device<sup>2</sup> The Mobility persona provides Overlay WLAN and (or) wired LAN functionalities for campus networks<sup>1</sup> The Branch persona provides the Aruba Instant OS and SD-Branch (LAN + WAN) functionality for branch and microbranch networks<sup>1</sup> The VPN Concentrator persona provides VPN termination and routing functionality for remote access networks<sup>3</sup> 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 recently deployed new Aruba Access Points at different branch offices Wireless 802.1X authentication will be against a RADIUS server in the cloud. The security team is concerned that the traffic between the AP and the RADIUS server will be exposed.

What is the appropriate solution for this scenario?

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

**Answer: D**

#### Explanation:

This is the appropriate solution for this scenario where wireless 802.1X authentication will be against a RADIUS server in the cloud and the security team is concerned that the traffic between the AP and the RADIUS server will be exposed. RadSec, also known as RADIUS over TLS, is a protocol that provides encryption and authentication for RADIUS traffic over TCP and TLS. RadSec can be configured on both the AP and the RADIUS server to establish a secure tunnel for exchanging RADIUS packets. The other options are incorrect because they either do not provide encryption or authentication for RADIUS traffic or do not involve RadSec. References: <https://www.securew2.com/blog/what-is-radsec/> <https://www.cloudradius.com/radsec-vs-radius/>

#### NEW QUESTION 8

Which standard supported by some Aruba APs can enable a customer to accurately locate wireless client devices within a few meters?

- A. 802.11mc
- B. 802.11W
- C. 802.11k
- D. 802.11r

**Answer: A**

#### Explanation:

The standard that is supported by some Aruba APs and can enable a customer to accurately locate wireless client devices within a few meters is A. 802.11mc. \* 802.11mc is an IEEE standard that enables computing devices to measure the distance to nearby Wi-Fi access points using a technique called Fine Timing Measurement (FTM). FTM uses precise timestamps to calculate the round-trip time of Wi-Fi frames between the device and the access point, and then converts it to a distance estimate. By using multiple access points and triangulation methods, the device can determine its location with high accuracy<sup>1</sup>. According to the Aruba document 802.11mc Support, this feature is supported on 500 Series, 510 Series, 530 Series, 550 Series, 560 Series and 570 Series access points. These APs act as FTM responders to time measurement queries sent from a client. To configure the AP to send FTM responses, you need to enable the ftm-responder-enable parameter in the WLAN SSID profile<sup>1</sup>.

#### NEW QUESTION 9

A system engineer needs to preconfigure several Aruba CX 6300 switches that will be sent to a remote office An untrained local field technician will do the rollout of the switches and the mounting of several AP-515s and AP-575S. Cables running to the APs are not labeled.

The VLANs are already preconfigured to VLAN 100 (mgmt), VLAN 200 (clients), and VLAN 300 (guests)

What is the correct configuration to ensure that APs will work properly?

A)



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

B)

```
port-access lldp-group IAP-Group
  seq 10 match sys-desc 515
  seq 20 match sys-desc 575
port-access role IAP-Role
  description ARUBA AP
  poe-priority high
  trust-mode dscp
  vlan trunk native 100
  vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
  associate role IAP-Role
  associate lldp-group IAP-Group
  no shutdown
```

C)

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

D)

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

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

**Answer:** C

**Explanation:**

Option C is the correct configuration to ensure that APs will work properly. It uses the ap command to configure a port profile for APs with VLAN 100 as the native VLAN and VLAN 200 and 300 as tagged VLANs. It also enables LLDP on the ports to discover the APs and assign them to the port profile automatically. The other options are incorrect because they either do not use the ap command, do not enable LLDP, or do not configure the VLANs correctly. References: [https://www.arubanetworks.com/techdocs/AOS-CX\\_10\\_08/UG/bk01-ch02.html](https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html) [https://www.arubanetworks.com/techdocs/AOS-CX\\_10\\_08/UG/bk01-ch03.html](https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch03.html)

**NEW QUESTION 10**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 10**

A company deployed Dynamic Segmentation with their CX switches and Gateways After performing a security audit on their network, they discovered that the tunnels built between the CX switch and the Aruba Gateway are not encrypted. The company is concerned that bad actors could try to insert spoofed messages on the Gateway to disrupt communications or obtain information about the network. Which action must the administrator perform to address this situation?

- A. Enable Secure Mode Enhanced
- B. Enable Enhanced security
- C. Enable Enhanced PAPI security
- D. Enable GRE security

**Answer:** C

**Explanation:**

PAPI is the protocol that is used to establish tunnels between the CX switch and the Aruba Gateway for Dynamic Segmentation1. By default, PAPI uses a simple checksum to verify the integrity of the messages, but it does not encrypt the payload2. This could expose the network to spoofing or replay attacks by malicious actors. To address this situation, the administrator must enable Enhanced PAPI security, which uses AES-256 encryption and HMAC-SHA1 authentication to protect the tunnel traffic2. Enhanced PAPI security can be enabled on the CX switch by using the command system papi enhanced- security enable3. This will ensure that the tunnels built between the CX switch and the Aruba Gateway are encrypted and authenticated.

**NEW QUESTION 15**

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](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 18**

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:

$$\text{EIRP} = P - l \times T_k + G_i$$

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:

$$\text{EIRP} = 20 - 3 \times 7 + 12 \quad \text{EIRP} = 20 - 21 + 12 \quad \text{EIRP} = -1 \text{ dBm}$$

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.

$$\text{One possible formula is: } \text{EIRP} = P - l \times T_k / (1 + T_k)$$

Using this formula, we get:

$$\text{EIRP} = 20 - 3 \times 7 / (1 + 7) \quad \text{EIRP} = 20 - 21 / 8 \quad \text{EIRP} = -2 \text{ dBm}$$

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:

$$\text{EIRP} = P - l \times T_k / (1 + T_k) - l \times T_k / (1 + T_k)^2 \quad \text{Using this formula, we get:}$$

$$\text{EIRP} = 20 - 3 \times 7 / (1 + 7) - 3 \times 7 / (1 + 7)^2 \quad \text{EIRP} = 20 - 21 / 8 - 21 / (8)^2 \quad \text{EIRP} = -2 \text{ dBm}$$

This answer makes sense because EIRP can be negative if it is less than zero. Therefore, this is the correct answer.

**NEW QUESTION 22**

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 24**

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 25**

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 30**

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 document<sup>1</sup>, 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 33**

You need to ensure that voice traffic sent through an ArubaOS-CX switch arrives with minimal latency What is the best scheduling technology to use for this task?

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

**Answer:** A

**Explanation:**

Strict queuing is the best scheduling technology to use for voice traffic on an AOS-CX switch. Scheduling is a mechanism that determines how packets are transmitted from different queues on an egress port. Strict queuing is a scheduling method that gives the highest priority queue absolute preference over all other queues, regardless of their size or utilization. Voice traffic should be assigned to the highest priority queue and scheduled with strict queuing to ensure minimal latency and jitter. The other options are incorrect because they are either not scheduling methods or not optimal for voice traffic. References:

<https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html>

**NEW QUESTION 35**

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

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

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

**Answer:** B

**Explanation:**

Aruba 9004 gateway supports ZTP on port G0/0/0 by default<sup>1</sup>. If the gateway

is connected to a different port, such as G0/0/V1, it will not be able to communicate with Aruba Activate and Aruba Central, which are required for ZTP<sup>2</sup>. Moreover, port G0/0/V1 is configured as a DHCP server by default, which can cause IP address conflicts with the existing network<sup>3</sup>. Therefore, the technician should move the cable on the gateway to port G0/0/0, which will allow the gateway to obtain an IP address from the network DHCP server and start the ZTP process. The other options are not correct because they will not solve the issue or enable ZTP. For example, option D will not work because factory defaulting and rebooting the gateway will not change the port configuration or behavior<sup>3</sup>.

**NEW QUESTION 39**

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

What is the solution for this?

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

**Answer:** C

**Explanation:**

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

<https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-8561-17DB0311ED8F.html>

**NEW QUESTION 40**



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 41**

Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements. After the configuration was complete, it was noted that a user assigned with the auditors role did not have the appropriate level of access on the switch. The user was not allowed to perform firmware upgrades and a privilege level of 15 was not assigned to their role. Which default management role should have been assigned for the user?

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

**Answer:** B

**Explanation:**

The correct answer is B. sysops.

The sysops user role is a predefined role that allows users to perform system operations on the switch, such as backup, restore, upgrade, or reboot. The sysops user role also has access to the PUT and POST methods for REST API, which can be used to modify the switch configuration. The sysops user role has a privilege level of 15, which is the highest level of access on the switch1.

The other options are incorrect because:

? A. sysadmin: The sysadmin user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The sysadmin user role does not have access to the REST API methods, and cannot perform firmware upgrades1.

? C. administrators: The administrators user role is a predefined role that has full access to all switch configuration information and all REST API methods. This role is more than what the Director of Security requires1.

? D. config: The config user role is a predefined role that allows users to view and modify the switch configuration using the CLI or the Web UI. The config user role does not have access to the REST API methods, and cannot perform firmware upgrades1.

**NEW QUESTION 46**

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 51**

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 54**

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](https://www.arubanetworks.com/assets/tg/TG_OWE.pdf)

NEW QUESTION 59

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

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

Answer: D

Explanation:

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

NEW QUESTION 63

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 Portal<sup>1</sup>, 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 it<sup>23</sup>.

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 65

DRAG DROP

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

|                   |                |  |  |
|-------------------|----------------|--|--|
| Client Insights   | Cloud Auth     |  | Built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots     |
| The Fabric Wizard | Policy Manager |  | Defines user and device groups and creates the associated access enforcement rules for the physical network  |
|                   |                |  | Enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores            |
|                   |                |  | Simplifies the creation of the overlays using an intuitive, graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Client Insights matches with Built in , AI powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML based classification models to eliminate network bling spots

Client Insights is a solution component of NetConductor that provides built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML- based classification models to eliminate network blind spots. Client Insights uses machine learning to automatically detect, identify, and classify devices on the network, such as IoT devices, BYOD devices, or rogue devices. Client Insights also provides behavioral analytics and anomaly detection to monitor device performance and security posture. Client Insights helps network administrators gain visibility into the device landscape, enforce granular access policies, and troubleshoot issues faster. References: <https://www.arubanetworks.com/products/network-management- operations/central/netconductor/>

[https://www.arubanetworks.com/assets/wp/WP\\_NetConductor.pdf](https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf)

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

Cloud Auth is a solution component of NetConductor that enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores. Cloud Auth is a cloud-native network access control (NAC) solution that is delivered via Aruba Central. Cloud Auth allows network administrators to define user and device groups, assign roles and policies, and enforce access control across wired and wireless networks. Cloud Auth supports MAC authentication for devices that do not support 802.1X, as well as integrations with cloud identity providers such as Azure AD, Google Workspace, Okta, etc. References: <https://www.arubanetworks.com/products/network-management- operations/central/netconductor/>

[https://www.arubanetworks.com/assets/wp/WP\\_NetConductor.pdf](https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf)

The Fabric Wizard matches with Simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways

The Fabric Wizard is a solution component of NetConductor that simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways. The Fabric Wizard is a tool that allows network administrators to design, deploy, and manage overlay networks using VXLAN and EVPN protocols. The Fabric Wizard provides a graphical representation of the network topology, devices, and links, and allows users to drag and drop virtual components such as VRFs, VLANs, and subnets. The Fabric Wizard also generates the configuration commands for each device based on the user input and pushes them to the switches and gateways via Aruba Central. References:

<https://www.arubanetworks.com/products/network-management- operations/central/netconductor/>

[https://www.arubanetworks.com/assets/wp/WP\\_NetConductor.pdf](https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf)

Policy Manager matches with Defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network

Policy Manager is a solution component of NetConductor that defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network. Policy Manager is a tool that allows network administrators to create and manage network policies based on user and device identities, roles, and contexts. Policy Manager uses Group Policy Identifier (GPID) to carry policy information in traffic for in-line enforcement. Policy Manager also integrates with Cloud Auth, ClearPass, or third-party solutions to provide flexible network access control. References:

<https://www.arubanetworks.com/products/network-management- operations/central/netconductor/>

[https://www.arubanetworks.com/assets/wp/WP\\_NetConductor.pdf](https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf)

**NEW QUESTION 66**

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 key 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 Central<sup>12</sup>.

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 devices<sup>1</sup>.

? 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 authentication<sup>3</sup>.

? 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 devices<sup>1</sup>.

**NEW QUESTION 67**

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 for 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 scenarios<sup>12</sup>.


**NEW QUESTION 68**




Refer to the exhibit.



Access Points



Switches



Gateways

WLANs

Access Points

Radios

Interfaces

Security



Services

System

IoT

Configuration Audit

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             |

- C. spanning-tree Cist mapping
- D. Spanning-tree root-guard setting

**Answer:** B

**Explanation:**

The correct answer is B. Spanning-tree instance VLAN mapping.

To load-balance VLANs with MSTP, you need to configure the same VLAN-to-instance mapping on all switches in the same MST region. This means that you need to assign different VLANs to different MST instances, and then adjust the spanning tree parameters (such as priority, cost, or port role) for each instance to achieve the desired load balancing. For example, you can make one switch the root for instance 1 and another switch the root for instance 2, and then map half of the VLANs to instance 1 and the other half to instance 2.

According to the Cisco document Understand the Multiple Spanning Tree Protocol (802.1s), one of the steps to configure MST is:

? Split your set of VLANs into more instances and configure different MST settings for each of these instances. In order to easily achieve this, elect Bridge D1 to be the root for VLANs 501 through 1000, and Bridge D2 to be the root for VLANs 1 through 500. These statements are true for this configuration:

Switch D1(config)#spanning-tree mst configuration Switch D1(config-mst)#instance 1 vlan 501-1000 Switch D1(config-mst)#exit

Switch D1(config)#spanning-tree mst 1 priority 0

Switch D2(config)#spanning-tree mst configuration Switch D2(config-mst)#instance 2 vlan 1-500 Switch D2(config-mst)#exit

Switch D2(config)#spanning-tree mst 2 priority 0

The above commands create two MST instances, 1 and 2, and map VLANs 501-1000 to instance 1 and VLANs 1-500 to instance 2. Then, they make switch D1 the root for instance 1 and switch D2 the root for instance 2.

The other options are incorrect because:

? A. Spanning-tree bpduguard setting is a security feature that disables a port if it receives a BPDU from an unauthorized device. It does not affect load balancing with MSTP.

? C. Spanning-tree CIST mapping is not a valid command. CIST stands for Common and Internal Spanning Tree, which is the spanning tree instance that runs within an MST region and interacts with other regions or non-MST switches.

? D. Spanning-tree root-guard setting is another security feature that prevents a port from becoming a root port if it receives superior BPDUs from another switch. It does not affect load balancing with MSTP.

**NEW QUESTION 76**

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.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 78**

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.

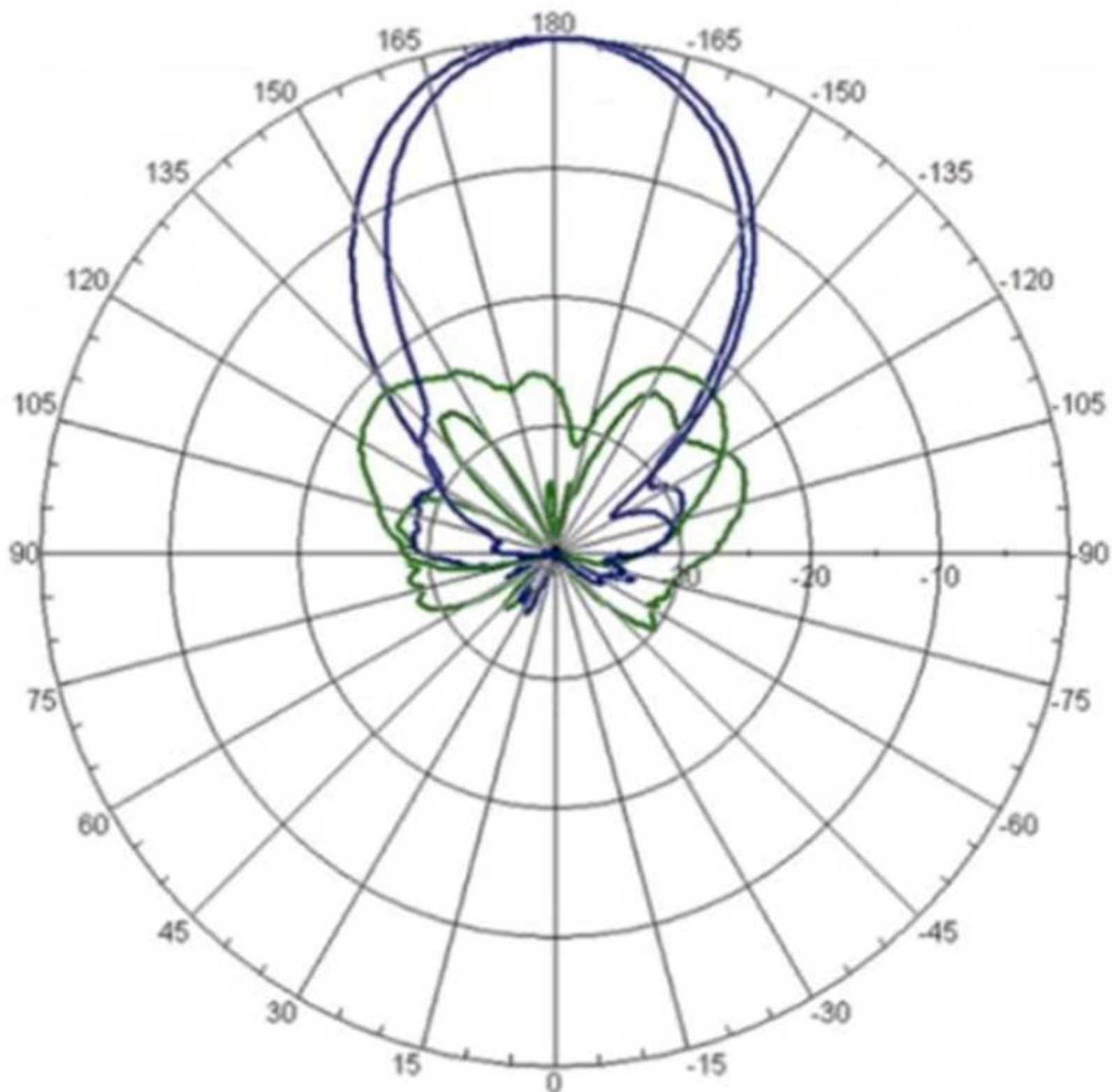
**Answer:** C

**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 80**

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 issue?

- 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/rf-fundamentals.htm)

[https://www.arubanetworks.com/techdocs/ArubaOS\\_86\\_Web\\_Help/Content/arubaos-solutions/wlan-rf/antennas.htm](https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/antennas.htm)

### NEW QUESTION 82

You must ensure the HPE Aruba network you are configuring for a client is capable of plug- and-play provisioning of access points. What enables this capability?

- A. UCC Service
- B. LLDP-MED
- C. SRTP
- D. CSMA

**Answer: A**

### Explanation:

The capability that enables plug-and-play provisioning of access points in an HPE Aruba network is the UCC Service. The UCC Service is a cloud-based service that allows the access points to automatically discover and connect to the Aruba Central management platform without any manual intervention. The UCC Service



also provides zero-touch configuration, firmware updates, and monitoring for the access points1.

The other options are incorrect because:

? B. LLDP-MED: LLDP-MED is a protocol that enhances the interoperability between network devices and IP phones. It does not enable plug-and-play provisioning of access points2.

? C. SRTP: SRTP is a protocol that provides encryption and authentication for voice and video traffic. It does not enable plug-and-play provisioning of access points3.

? D. CSMA: CSMA is a protocol that regulates how devices share a common medium, such as a wireless channel. It does not enable plug-and-play provisioning of access points.

#### NEW QUESTION 84

Which statements regarding OSPFv2 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 89

In AOS 10. which session-based ACL below will only allow ping from any wired station to wireless clients but will not allow ping from wireless clients to wired stations"? The wired host ingress traffic arrives on a trusted port.

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

**Answer:** D

#### Explanation:

A session-based ACL is applied to traffic entering or leaving a port or VLAN based on the direction of the session initiation. To allow ping from any wired station to wireless clients but not vice versa, a session-based ACL should be used to deny icmp echo traffic from any source to any destination, and then permit icmp echo-reply traffic from any source to user destination. The user role represents wireless clients in AOS 10. References: [https://techhub.hpe.com/eginfolib/Aruba/OS-CX\\_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html](https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html) <https://techhub.hpe.com/eginfolib/networking/docs/arubaos-switch/security/GUID-EA0A5B3C-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html>

#### NEW QUESTION 94

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 98

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 role 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](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](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 100

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](https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf)

#### NEW QUESTION 104

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

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

**Answer:** A

#### Explanation:

The component that is used by the Aruba Network Analytics Engine (NAE) is D. Current State Database. The Current State Database is a database that stores the configuration and state information of the switch, such as interfaces, VLANs, routing protocols, statistics, and more. The NAE can access this database through the AOS-CX REST API and monitor the values of any data point using monitors. The NAE can also track the history of the values in a time-series database and correlate them with network events or configuration changes<sup>1</sup>. The Current State Database provides NAE with direct visibility into the entire current state of the device, which enables intelligent troubleshooting and automation of network tasks<sup>1</sup>. The other options are incorrect because:

? A. JSON-based scripts: JSON is a data format that is used to exchange information between applications. It is not a scripting language that can be used by NAE. NAE scripts are written in Python, which is a popular and powerful programming language<sup>1</sup>.

? B. Lisp-based agents: Lisp is a family of programming languages that are mainly used for artificial intelligence and functional programming. It is not a language that can be used by NAE. NAE agents are instances of scripts that run on the switch and collect relevant network information and trigger alerts or actions<sup>1</sup>.

? C. Ruby-based scripts: Ruby is a general-purpose programming language that is known for its expressiveness and elegance. It is not a language that can be used by NAE. NAE scripts are written in Python, which is a popular and powerful programming language<sup>1</sup>.

#### NEW QUESTION 105

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. iSCSI client devices can request to have flow control enabled
- D. GVRP VLAN information can be used to dynamically add VLANs to a trunk
- E. iSCSI 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-qos/lldp-med.htm)  
[https://www.arubanetworks.com/techdocs/ArubaOS\\_86\\_Web\\_Help/Content/arubaos-solutions/wlan-rf/poe.htm](https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/poe.htm)

#### NEW QUESTION 110

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, etc. QoS involves identifying specific traffic for special treatment and applying policies and actions to improve its performance or meet certain service level agreements (SLAs). QoS can help network devices to manage congestion, delay, jitter, packet loss, bandwidth allocation, etc., for different types of traffic. 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 114**

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

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

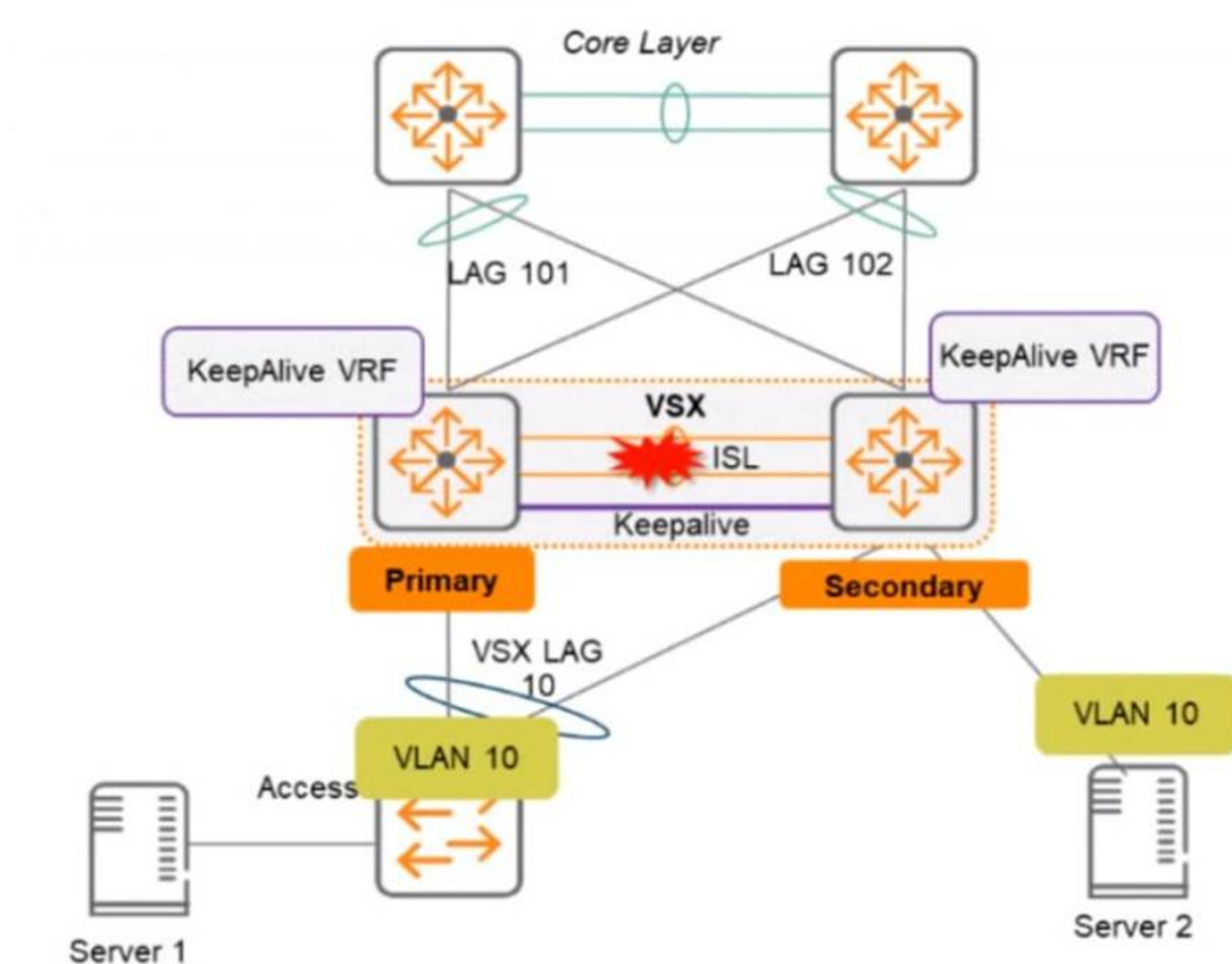
**Answer:** A

**Explanation:**

MPSK Local is a feature that can be used to set up 15 headless IoT devices that do not support 802.1X authentication. MPSK Local allows the switch to automatically generate and assign unique pre-shared keys for devices based on their MAC addresses, without requiring any configuration on the devices or an external authentication server. The other options are incorrect because they either require 802.1X authentication, which is not supported by the IoT devices, or WPA3 encryption, which is not supported by Aruba CX switches. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch06.html>

**NEW QUESTION 116**

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 keepalive 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 120**

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 122**

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](https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html)

**NEW QUESTION 125**

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

- A. DMO is configured individually for 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 126**

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 131**

A company recently upgraded its campus switching infrastructure with Aruba 6300 CX switches. They have implemented 802.1X authentication on edge ports where laptop and IoT devices typically connect. An administrator has noticed that for PoE devices the ports are delivering the maximum wattage instead of what the device actually needs. Upon connecting the IoT devices, the devices request their specific required wattage through information exchange.

- A. Concerned about this waste of electricity, what should the administrator implement to solve this problem?
- B. Enable AAA authentication to exempt LLDP and/or CDP information.
- C. Globally enable the QoS trust setting for LLDP and/or CDP.
- D. Create device profiles with the correct power definitions.
- E. Implement a classifier policy with the correct power definitions.

**Answer:** D

**Explanation:**

According to the Aruba Documentation Portal<sup>1</sup>, the Aruba 6300 CX switches support various features to control the PoE devices on specific ports, such as device profiles and classifier policies. These features can help reduce the power consumption and improve the performance of the PoE devices.

1: [https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring\\_6300-6400/Content/Chp\\_LEDs/fro-pan-led-630.htm](https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm) 2:

<https://www.arubanetworks.com/products/switches/6300-series/> 3: <https://docs.samsungknox.com/admin/knox-manage/configure/profile/configure-profile-policies/configure-profile-policies-by-device-platform/>

**NEW QUESTION 136**

With Aruba CX 6300, how do you configure IP address 10.10.10.1 for the interface in default state for interface 1/1/1?

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

**Answer:** B

**Explanation:**

To configure an IP address for an interface in default state for interface 1/1/1 on Aruba CX 6300 switch, you need to disable switching on the interface first with the command `no switching`. Then you can assign an IP address with the command `ip address`. The other options are incorrect because they either do not disable switching or use invalid keywords such as `switching` or `routing`. References: [https://www.arubanetworks.com/techdocs/AOS-CX\\_10\\_08/UG/bk01-ch01.html](https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch01.html) [https://www.arubanetworks.com/techdocs/AOS-CX\\_10\\_08/UG/bk01-ch02.html](https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html)

**NEW QUESTION 140**

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 devices<sup>1</sup>. 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 pair<sup>2</sup>.

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 switch<sup>1</sup>. 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 balancing<sup>1</sup>.

Another statement that is true about VSX LAG is that outgoing traffic is preferentially switched to local members of the LAG<sup>2</sup>. 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 link<sup>2</sup>.

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 143

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 144

DRAG DROP

Select the Aruba stacking technology matching each option (Options may be used more than once or not at all.)

VSF V SX

Answer Area

|                          |  |
|--------------------------|--|
| <input type="checkbox"/> | Supports up to 10 devices per stack                    |
| <input type="checkbox"/> | Supports two devices per stack                         |
| <input type="checkbox"/> | Individual ISL links up to 400G are supported          |
| <input type="checkbox"/> | Individual ISL links up to 50G are supported           |
| <input type="checkbox"/> | A maximum aggregate ISL bandwidth of 200G is supported |

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

- a) Support up to 10 devices per stack -> VSF
- b) Support two devices per stack -> VSX
- c) Individual ISL links up to 400G are supported -> VSX
- d) individual ISL links up to 50G are supported -> VSF
- e) A maximum aggregate ISL bandwidth of 200G is supported -> VSF

References: 1 <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/GUID-2E425DAE-EC54-4313-9DEA-A61817F903C0.html>

#### NEW QUESTION 147

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 149**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### HPE7-A01 Practice Exam Features:

- \* HPE7-A01 Questions and Answers Updated Frequently
- \* HPE7-A01 Practice Questions Verified by Expert Senior Certified Staff
- \* HPE7-A01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* HPE7-A01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The HPE7-A01 Practice Test Here](#)**