

HP

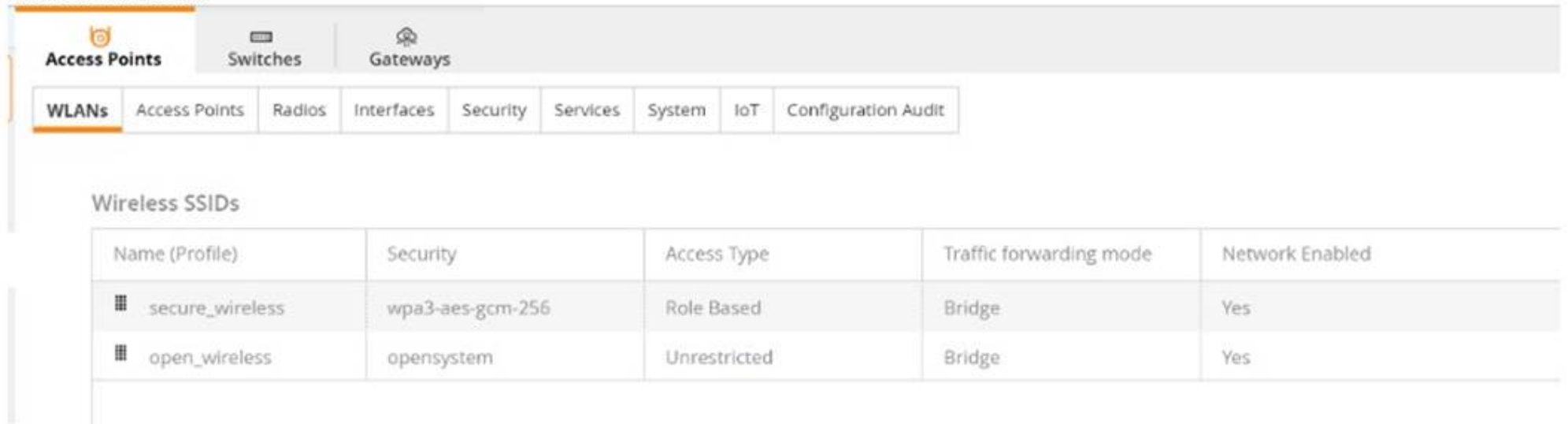
Exam Questions HPE7-A01

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

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

Answer: C

Explanation:

According to the Aruba Documentation Portal¹, the ArubaOS-CX switch supports various features to control the ingress traffic on specific ports, such as rate limiting, QoS shaping, and access control. These features can help reduce the impact of excessive broadcast traffic on the network performance and availability.

This is because rate limiting is a feature that allows you to limit the inbound or outbound traffic on a port based on a percentage of the port capacity or a fixed amount of bytes per second. Rate limiting can help prevent broadcast storms by reducing the amount of broadcast packets that enter or leave a port

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

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

https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8160_ssw_mcg/content/ch05.html

NEW QUESTION 3

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 OSPF 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 4

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 conditions².

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 5

A customer wants to provide wired security as close to the source as possible The wired security must meet the following requirements:

- allow ping from the IT management VLAN to the user VLAN
- deny ping sourcing from the user VLAN to the IT management VLAN

The customer is using Aruba CX 6300s

What is the correct way to implement these requirements?

- A. Apply an outbound ACL on the user VLAN allowing temp echo-reply traffic toward the IT management VLAN
- B. Apply an inbound ACL on the user VLAN allowing icmp echo-reply traffic toward the IT management VLAN
- C. Apply an inbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN
- D. Apply an outbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN

Answer: C

Explanation:

An inbound ACL is applied to traffic entering a port or VLAN. An outbound ACL is applied to traffic leaving a port or VLAN⁴. To deny ping sourcing from the user VLAN to the IT management VLAN, an inbound ACL on the user VLAN should be used to filter icmp echo traffic toward the IT management VLAN. Icmp echo-reply traffic is not needed to be allowed because it is already permitted by default⁵. References: 4

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html 5

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-0C3A9D0F-6E5B-4E1A-AF3C-8D8B2F9C1A7B.html

NEW QUESTION 6

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 7

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 8

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 9

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 10

you need to have different routing-table requirements With Aruba CX 6300 VSF configuration.

Assuming the correct layer-2 VLAN already exists, how would you create a new SVI for a separate routing table?

- A. create a new VLAN, and attach the VRF to it.
- B. Create a new routing table, and attach VLANs to it
- C. Create a new SVI and use attach command.
- D. Create a new VLA
- E. and attach the routing table to it

Answer: C

Explanation:

The correct answer is C. Create a new SVI and use attach command.

To create a new SVI for a separate routing table, you need to use the attach command to associate the SVI with a VRF (Virtual Routing and Forwarding) instance. A VRF is a logical entity that allows multiple routing tables to coexist on the same switch. Each VRF has its own set of interfaces, routing protocols, and routes that are isolated from other VRFs. According to the AOS-CX Virtual Switching Framework (VSF) Guide¹, one of the steps to configure VRF-aware VSF is:

? Configure the VRFs on each member switch and assign the SVIs to the respective

VRFs using the attach command. For example: switch(config)# vrf red

switch(config-vrf)# exit switch(config)# interface vlan 10

switch(config-if-vlan)# ip address 10.1.1.1/24 switch(config-if-vlan)# attach vrf red

The above commands create a VRF named red and assign VLAN 10 SVI to it. The SVI has an IP address of 10.1.1.1/24.

The other options are incorrect because:

? A. You cannot attach a VRF to a VLAN directly. You need to create an SVI for the VLAN and then attach the VRF to the SVI.

? B. You cannot create a new routing table manually. You need to create a VRF and then use routing protocols or static routes to populate the routing table for the VRF.

? D. You cannot attach a routing table to a VLAN directly. You need to create an SVI for the VLAN and then attach a VRF that has a routing table associated with it.

NEW QUESTION 10

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

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

Answer: AD

Explanation:

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

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

NEW QUESTION 12

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 14

A customer is concerned about me unprotected traffic between an AOS-CX switch and a gateway, running on AOS10. What is a feasible option to protect this traffic?

- A. Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway
- B. Implement an MD5 HMAC function to protect PAPI between the AOS-CX switches and the gateway
- C. Implement a GRE tunnel to protect PAPI between the AOS-CX switches and the gateway
- D. no action is needed, an RSA certificate already encrypts the traffic

Answer: A

Explanation:

According to the Aruba Documentation Portal¹, PAPI (Port Aggregation Protocol) is a protocol that allows multiple physical ports to be aggregated into a single logical port for increased bandwidth and performance. PAPI can be used between AOS-CX switches and gateways, or between AOS-CX switches and other devices.

Option A: Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway

This is because option A shows how to implement an IPSec tunnel between two devices using the interface command and the ipsec command. An IPSec tunnel can provide encryption and authentication for PAPI traffic between two devices, such as an AOS-CX switch and a gateway².

Therefore, option A is a feasible option to protect this traffic.

I hope this helps you. If you need more information, please let me know. 1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7727/Content/Chp_prev_traf_loss/Act_gtw_act_fwd/act-gat-ove-vsx-10.htm 2: <https://community.arubanetworks.com/blogviewer?blogkey=989fc43a-e0df-42db-9c0b-f96d6565a1fa>

NEW QUESTION 17

You are working on a network where the customer has a dedicated router with redundant Internet connections. For 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.

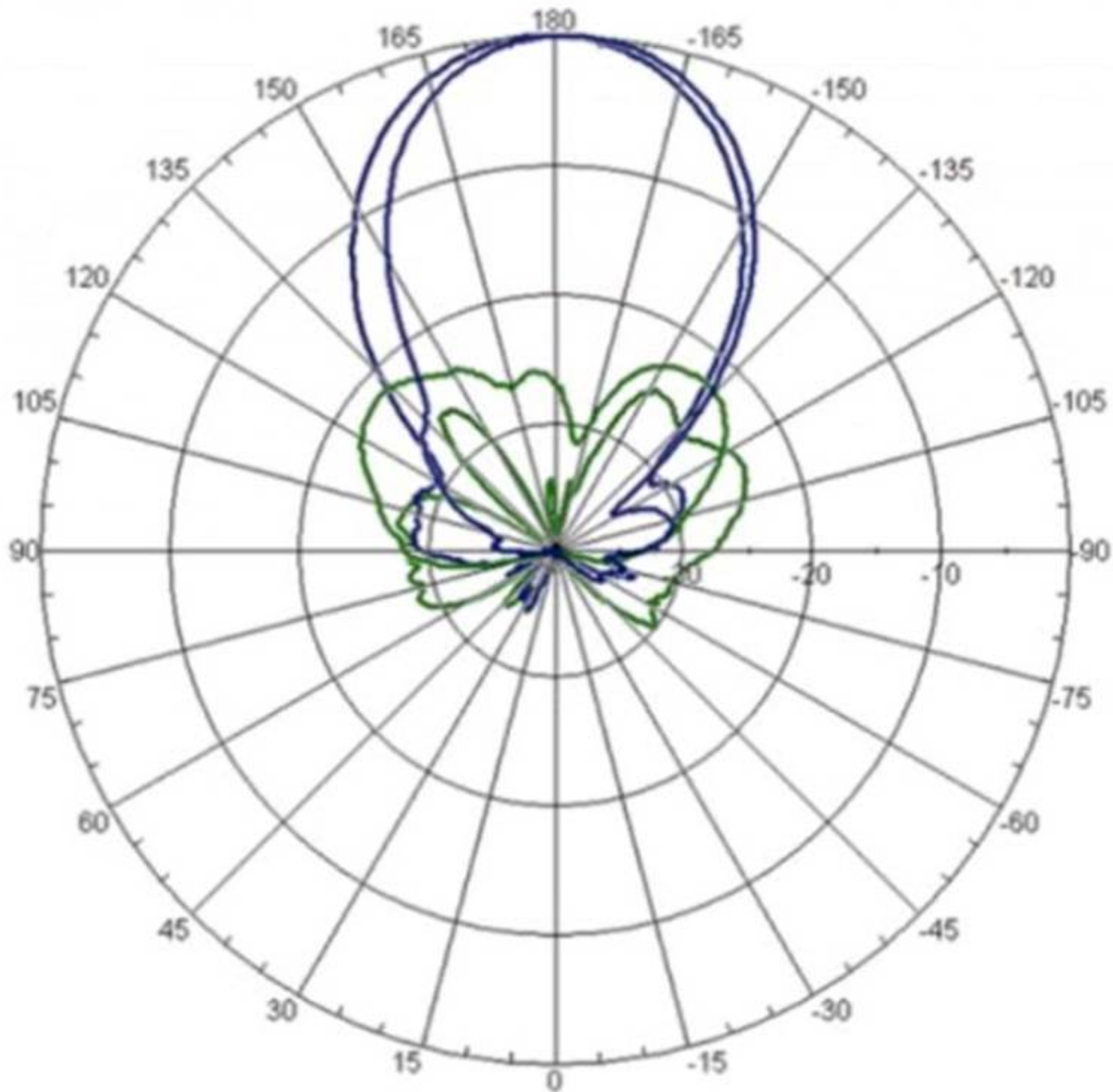
Answer: C

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 18

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/antennas.htm

NEW QUESTION 21

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 22

Your manufacturing client is having installers deploy seventy headless scanners and fifty IP cameras in their warehouse. These new devices do not support 802.1X authentication.

How can HPE Aruba reduce the IT administration overhead associated with this deployment while maintaining a secure environment using MPSK?

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

Answer: C

Explanation:

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

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch05.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch06.html

NEW QUESTION 25

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

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

Answer: D

Explanation:

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

<https://techhub.hpe.com/eginfolib/networking/docs/arubaos-switch/security/GUID-EA0A5B3C-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html>

NEW QUESTION 27

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 29

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 30

Your customer has four (4) Aruba 7200 Series Gateways and two (2) 7000 Series Gateways. The customer wants to form a cluster with these Gateways. What design consideration would prevent you from using all of those Gateways?

- A. Multiple versions between Gateways in the same cluster profile are not allowed AOS 10.x.
- B. A heterogeneous cluster is not supported in AOS 10.x.
- C. The AP load should be lowest value of worst-case scenario load.
- D. A combination of 7200 series and 7000 series gateways supports up to 4 nodes

Answer: A

Explanation:

The reason is that AOS 10.x does not support clustering gateways with different versions in the same cluster profile. A cluster profile defines the configuration settings for a group of gateways that are managed by Aruba Central.

According to the Aruba documentation², ??You can combine 7200 Series and 7000 Series gateways in the same cluster with a maximum size of four devices with reduced AP client capacity on 7000 Series gateways.??

NEW QUESTION 34

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-rf/poe.htm

NEW QUESTION 37

DRAG DROP

Match each PoE power class to its corresponding 802.3 standard. (Options may be used more than once or not at all)

802.3at

802.3bt

802.3af

Answer Area

Class 3 (15.4W)

Class 4 (30W)

Class 6 (60W)

Class 8 (90W)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

? Class 3 (15.4W): 802.3af

? Class 4 (30W): 802.3at

? Class 6 (60W): 802.3bt

? Class 8 (90W): 802.3bt

NEW QUESTION 41

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 MacBook 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 43

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

The client device is connected to an Aruba CX 6100 switch by VSX LAG. Which action can be used to find the IP address successfully?

A)

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

B)

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

C)

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

D)

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

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

Answer: B

Explanation:

The show arp command displays the ARP table for a specific VRF or all VRFs on the switch. The ARP table contains the IP address to MAC address mappings for hosts that are directly connected to the switch or reachable through a gateway. If the client device is connected to another switch by VSX LAG, the ARP entry for the client device will not be present on the primary switch unless it has communicated with it recently. Therefore, to find the IP address of the client device, the administrator should run the show arp command on the secondary switch in the VSX pair, specifying the VRF name that contains the client device's subnet.

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

NEW QUESTION 45

Your customer has asked you to assign a switch management role for a new user. The customer requires the user role to only have Web UI access to the System > Log page and only have access to the GET method for REST API for the /logs/event resource.

Which default AOS-CX user role meets these requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 49

DRAG DROP

List the WPA 4-Way Handshake functions in the correct order.

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

>

<

↑

↓

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 52

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

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

Answer: B

Explanation:

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

NEW QUESTION 57

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 62

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

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

Answer: AC

Explanation:

The statements that are true regarding Aruba NAE agents are A and C.

* A. A single NAE script can be used by multiple NAE agents. This means that you can create different instances of the same script with different parameters or settings. For example, you can use the same script to monitor different VLANs or interfaces on the switch1.

* C. NAE agents will never consume more than 10% of switch processor resources. This is a built-in safeguard that prevents the agents from affecting the switch performance or stability. If an agent exceeds the 10% limit, it will be automatically disabled and an alert will be generated2.

The other options are incorrect because:

? B. NAE agents are not active at all times. They can be enabled or disabled by the user, either manually or based on a schedule. They can also be disabled

automatically if they encounter an error or exceed the resource limit1.

? D. NAE scripts do not need to be reviewed and signed by Aruba before being used. You can create your own custom scripts using Python and upload them to the switch or Aruba Central. You can also use the scripts provided by Aruba or other sources, as long as they are compatible with the switch firmware version1.

? E. A single NAE agent cannot be used by multiple NAE scripts. An agent is an instance of a script that runs on the switch. Each agent can only run one script at a time1.

NEW QUESTION 66

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 70

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

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

Answer: D

Explanation:

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

References: 1: Aruba Campus Access documents and learning resources 2: system-mac - Aruba

NEW QUESTION 71

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 76

.....

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](#)