



HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam

NEW QUESTION 1

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

- A. stacked data-plane
- B. faster MSTP converge processing
- C. dual Aruba AP LAN port connectivity for PoE redundancy
- D. dual control plane provides better resiliency

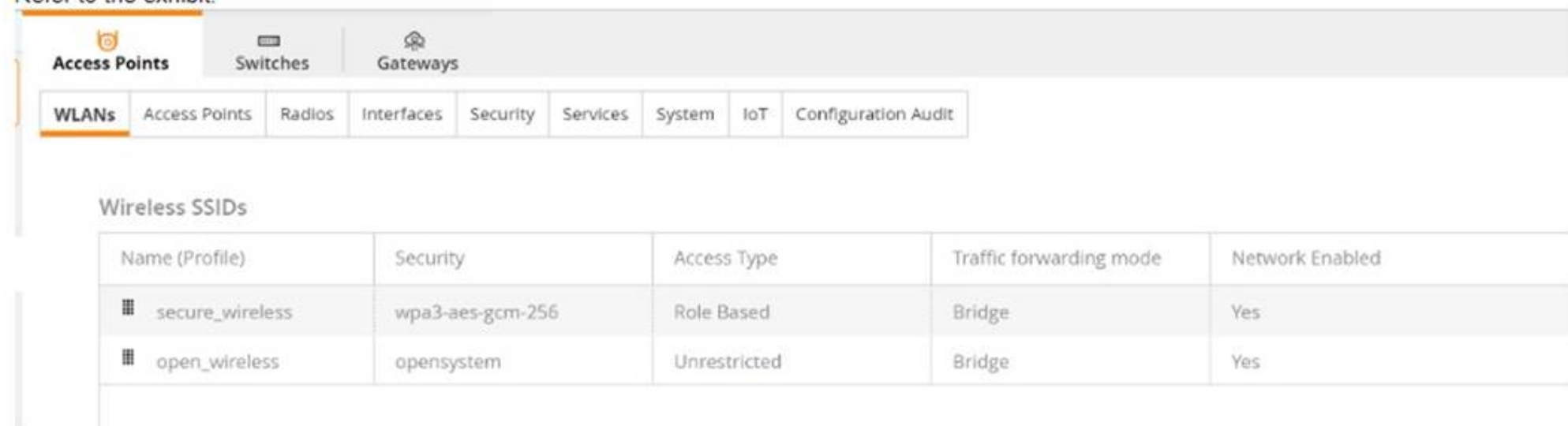
Answer: D

Explanation:

VSX clustering is a feature that allows two Aruba CX switches to operate as a single logical device, providing high availability, scalability, and simplified management. VSX clustering has several benefits over spanning tree configuration, such as:
? Dual control plane provides better resiliency. Unlike stacking, where switches share a single control plane, VSX switches have independent control planes that synchronize their states over an inter-switch link (ISL). This means that if one switch fails or reboots, the other switch can continue to operate without affecting traffic flows or network services.
? Active-active forwarding provides better performance. Unlike spanning tree, where some links are blocked to prevent loops, VSX switches use all available links for forwarding traffic, providing load balancing and increased bandwidth utilization.
? Multichassis LAG provides better redundancy. Unlike single-chassis LAG, where all member ports belong to one switch, VSX switches can form multichassis LAGs with downstream or upstream devices, where member ports are distributed across both switches. This provides link redundancy and seamless failover in case of switch or port failure.
References: https://www.arubanetworks.com/assets/tg/TG_VSX.pdf

NEW QUESTION 2

Refer to Exhibit:



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 3

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 Portal¹, 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 4

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

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

Answer: D

Explanation:

The reason is that the Inter-Switch Link Protocol (ISLP) is a protocol that enables VSX stack join and synchronization between two VSX peer switches. ISLP uses a hello interval to exchange control messages between the switches.

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

NEW QUESTION 5

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 6

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-ch03.html

NEW QUESTION 7

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 icmp 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 VLAN. 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 default. 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 8

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 9

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 10

What steps are part of the Key Management workflow when a wireless device is roaming from AP1 to AP2? (Select two.)

- A. AP1 will cache the client's information and send it to the Key Management service
- B. The Key Management service receives from AirMatch a list of all AP2's neighbors
- C. The Key Management service receives a list of all AP1 s neighbors from AirMatch.
- D. The Key Management service then generates R1 keys for AP2's neighbors.
- E. A client associates and authenticates with the AP2 after roaming from AP1

Answer: AD

Explanation:

The correct steps that are part of the Key Management workflow when a wireless device is roaming from AP1 to AP2 are A and D.

* A. AP1 will cache the client's information and send it to the Key Management service. This is true because when a client associates and authenticates with AP1, AP1 will generate a pairwise master key (PMK) for the client and store it in its cache. AP1 will also send the PMK and other client information, such as MAC address, VLAN, and SSID, to the Key Management service, which is a centralized service that runs on Aruba Mobility Controllers (MCs) or Mobility Master (MM) devices1. The Key Management service will use this information to facilitate fast roaming for the client.

* D. The Key Management service then generates R1 keys for AP2's neighbors. This is true because when the Key Management service receives the client information from AP1, it will use the PMK to derive R0 and R1 keys for the client. R0 keys are used to generate R1 keys, which are used to generate pairwise transient keys (PTKs) for encryption. The Key Management service will distribute the R1 keys to AP2 and its neighboring APs, which are determined by AirMatch based on RF proximity2. This way, when the client roams to AP2 or any of its neighbors, it can skip the 802.1X authentication and use the R1 key to quickly generate a PTK with the new AP3.

* B. The Key Management service receives from AirMatch a list of all AP2's neighbors. This is false because the Key Management service does not receive this information from AirMatch directly. AirMatch is a feature that runs on MCs or MM devices and optimizes the RF performance of Aruba devices by using machine learning algorithms. AirMatch periodically sends neighbor reports to all APs, which contain information about their nearby APs based on signal strength and interference. The APs then send these reports to the Key Management service, which uses them to determine which APs should receive R1 keys for a given client2.

* C. The Key Management service receives a list of all AP1 s neighbors from AirMatch. This is false for the same reason as B. The Key Management service does not receive this information from AirMatch directly, but from the APs that send their neighbor reports.

* E. A client associates and authenticates with the AP2 after roaming from AP1. This is false because a client does not need to authenticate with AP2 after roaming from AP1 if it has already authenticated with AP1 and received R1 keys from the Key Management service. The client only needs to associate with AP2 and perform a four-way handshake using the R1 key to generate a PTK for encryption3. This is called fast roaming or 802.11r roaming, and it reduces the latency and disruption caused by full authentication.

1: ArubaOS 8.7 User Guide 2: ArubaOS 8.7 User Guide 3: ArubaOS 8.7 User Guide : ArubaOS 8.7 User Guide

NEW QUESTION 10

A client is connecting to 802.1X SSID that has been configured in tunnel mode with the default AP-group settings. After receiving Access-Accept from the RADIUS server, the Aruba Gateway will send Access-Accept to the AP through which tunnel?

- A. IPsec tunnel

- B. Split tunnel
- C. GRE tunnel
- D. PAR tunnel

Answer: C

Explanation:

According to the Aruba Documentation Portal¹, 802.1X is a standard for port-based network access control that uses a RADIUS server to authenticate and authorize wireless clients. 802.1X can be configured in different modes, such as bridge mode, tunnel mode, or split tunnel mode.

Option C: GRE tunnel

This is because option C shows how to configure an SSID in tunnel mode with the default AP-group settings on an Aruba switch. In tunnel mode, all client traffic from the access points is tunneled back to the controller and the controller would in turn put the client traffic onto the network². The GRE protocol is used to encapsulate and decapsulate the traffic between the access points and the controller³.

Therefore, option C is correct.

1: <https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html> 2:

<https://community.arubanetworks.com/discussion/bridge-and-tunnel-mode> 3: <https://www.twingate.com/blog/ipsec-tunnel-mode>

NEW QUESTION 11

With the Aruba CX 6200 24G switch with uplinks on 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 14

In an ArubaOS 10 architecture using an AP and a gateway, what happens when a client attempts to join the network and the WLAN is configured with OWE?

- A. Authentication information is not exchanged
- B. The Gateway will not respond.
- C. No encryption is applied.
- D. RADIUS protocol is utilized.

Answer: A

Explanation:

This is the correct statement about what happens when a client attempts to join the network and the WLAN is configured with OWE (Opportunistic Wireless Encryption). OWE is a standard that provides encryption for open networks without requiring any authentication or credentials from the client or the network. OWE uses a Diffie-Hellman key exchange mechanism to establish a secure session between the client and the AP without exchanging any authentication information. The other options are incorrect because they either describe scenarios that require authentication or encryption methods that are not used by OWE. References: https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

NEW QUESTION 16

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 19

You are doing tests in your lab and with the following equipment specifications:

- AP1 has a radio that generates a 16 dBm signal.
- AP2 has a radio that generates a 13 dBm signal.
- AP1 has an antenna with a gain of 8 dBi.
- AP2 has an antenna with a gain of 12 dBi. The antenna cable for AP1 has a 4 dB loss. The antenna cable for AP2 has a 3 dB loss.

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

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

Answer: B

Explanation:

The Equivalent Isotropic Radiated Power (EIRP) is the measured radiated power of an antenna in a specific direction. It is also called Equivalent Isotropic Radiated Power. It is the output power when a signal is concentrated into a smaller area by the Antenna. The EIRP can take into account the losses in transmission line, connectors and includes the gain of the antenna. It is represented in dBm. The formula for EIRP is:

$EIRP = P_{TL} + G_a$ where P_T is the output power of the transmitter in dBm, L_c is the cable and connector loss in dB, and G_a is the antenna gain in dBi.

For AP1, the EIRP can be calculated as: $EIRP = 164 + 8 = 20$ dBm

Therefore, the answer B is correct.

References: 1: Aruba Campus Access documents and learning resources 2: EIRP Calculator - Effective Isotropic Radiated Power

NEW QUESTION 24

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 G0/0/V1 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 default¹. If the gateway is connected to a different port, such as G0/0/V1, it will not be able to communicate with Aruba Activate and Aruba Central, which are required for ZTP². Moreover, port G0/0/V1 is configured as a DHCP server by default, which can cause IP address conflicts with the existing network³. Therefore, the technician should move the cable on the gateway to port G0/0/0, which will allow the gateway to obtain an IP address from the network DHCP server and start the ZTP process. The other options are not correct because they will not solve the issue or enable ZTP. For example, option D will not work because factory defaulting and rebooting the gateway will not change the port configuration or behavior³.

NEW QUESTION 29

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 32

With the Aruba CX switch configuration, what is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation?

- A. Active Gateway
- B. Active-Active VRRP
- C. SVI with vsx-sync
- D. VRRP

Answer: A

Explanation:

Active Gateway is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation. Active Gateway is a feature that allows both VSX peers to act as active gateways for different subnets, eliminating the need for VRRP or other first-hop redundancy protocols. Active Gateway also provides fast failover and load balancing for L3 traffic across the VSX peers. The other options are incorrect because they are either not recommended or not supported by Aruba CX VSX. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html>

<https://www.arubanetworks.com/resource/aruba-virtual-switching-extension-vsx/>

NEW QUESTION 33

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:

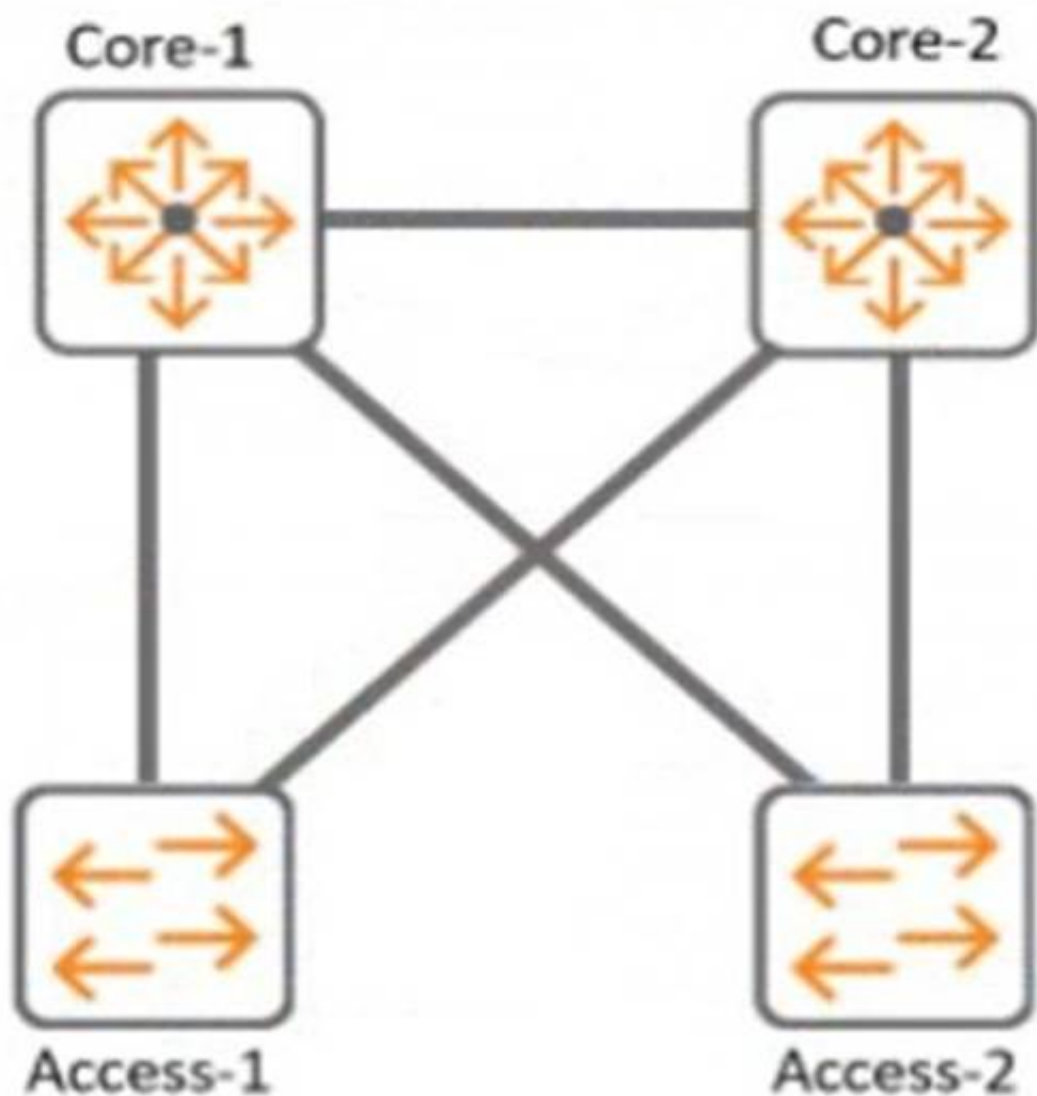
OCSP is a protocol that allows clients to query the CA or a trusted responder for the status of a specific certificate. OCSP requests and responses are smaller and faster than CRLs, and they can provide real-time information about the revocation status of a certificate¹². CRLs are lists of all revoked 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 38

Refer to the exhibit.



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

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

Answer: A

Explanation:

The default value for config-revision on Core-1 is 0. Config-revision is a parameter that indicates the configuration version of a VSX pair. It is used to synchronize the configuration between the VSX peers and to detect any configuration mismatch. The config-revision value is set to 0 by default on both VSX peers and is incremented by 1 every time a configuration change is made on either peer. The other options are incorrect because they do not reflect the default value of config-revision. 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 39

A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working to a remote site connected via layer-3 All legacy devices are connected to a dedicated Aruba CX 6200 switch at each site.

What technology on the Aruba CX 6200 could be used to meet this requirement?

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

Answer: A

Explanation:

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

<https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html>

NEW QUESTION 43

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

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

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

Answer: BC

Explanation:

CoA (Change of Authorization) is a feature that allows ClearPass to dynamically change the authorization and access privileges of a device after it has been authenticated¹. CoA uses RADIUS messages to communicate with the network device and instruct it to perform an action, such as reauthenticating the device, applying a new VLAN or user role, or disconnecting the device².

To enable CoA on a CX switch, the network engineer needs to configure dynamic authorization on the switch, which is a global command that allows the switch to accept RADIUS messages from ClearPass and execute the requested actions³. The network engineer also needs to specify the IP address and shared secret of ClearPass as a dynamic authorization client on the switch³.

To trigger CoA for a specific wired device, the network engineer needs to bounce the switchport, which is an action that temporarily disables and re-enables the port where the device is connected. This forces the device to reauthenticate and receive the new policy from ClearPass. Bouncing the switchport can be done manually by using the interface shutdown and no shutdown commands, or automatically by using ClearPass as a CoA server and sending a RADIUS message with the Port-Bounce-Host AVP (Attribute-Value Pair).

NEW QUESTION 46

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

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

Answer: B

Explanation:

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

NEW QUESTION 50

A new network design is being considered to minimize client latency in a high-density environment. The design needs to do this by eliminating contention overhead by dedicating subcarriers to clients.

Which technology is the best match for this use case?

- A. OFDMA
- B. MU-MIMO
- C. QWMM
- D. Channel Bonding

Answer: A

Explanation:

OFDMA (Orthogonal Frequency Division Multiple Access) is a technology that can minimize client latency in a high-density environment by eliminating contention overhead by dedicating subcarriers to clients. OFDMA allows multiple clients to transmit simultaneously on different subcarriers within the same channel, reducing contention and increasing efficiency. MU-MIMO (Multi-User Multiple Input Multiple Output) is a technology that allows multiple clients to transmit simultaneously on different spatial streams within the same channel, but it does not eliminate contention overhead. QWMM (Quality of Service Wireless Multimedia) is a technology that prioritizes traffic based on four access categories, but it does not eliminate contention overhead. Channel Bonding is a technology that combines two adjacent channels into one wider channel, increasing bandwidth but not eliminating contention overhead. References: https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf
https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf

NEW QUESTION 52

DRAG DROP

Match the topics of an AOS10 Tunneled mode setup between an AP and a Gateway. (Options may be used more than once or not at all.)

Authenticator

Negotiate IPsec Phase1

Negotiate IPsec Phase 2

RADIUS proxy

Answer Area

Access Point

Access Point and Gateway

Device Designated Gateway

Overlay Tunnel Orchestrator

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Authenticator

Negotiate IPsec Phase1

Negotiate IPsec Phase 2

RADIUS proxy

Answer Area

Negotiate IPsec Phase1

Negotiate IPsec Phase 2

Authenticator

RADIUS proxy

Access Point

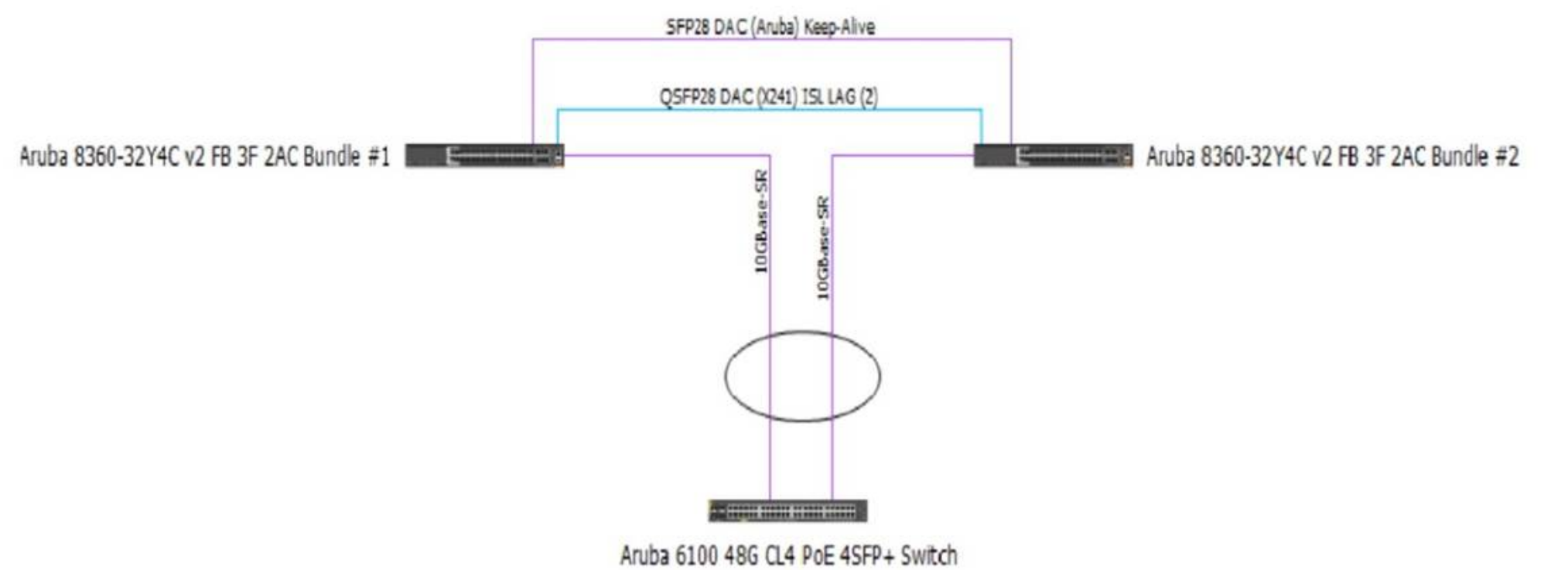
Access Point and Gateway

Device Designated Gateway

Overlay Tunnel Orchestrator

NEW QUESTION 56

Review the exhibit.



You are troubleshooting an issue with a 10 102.39 0/24 subnet which is also VLAN 1000 used Tor wireless clients on a pair of Aruba CX 8360 switches The subnet SVI is configured on the 8360 pair, and the DHCP server is a Microsoft Windows Server 2022 Standard with an IP address of 10 200 1.100. The 10.102.250.0/24 subnet is used for switch management. A large number of DHCP requests are failing You are observing sporadic DHCP behavior across clients attached to the CX 6100 switch. Which action may help fix the issue?

- A)
- Enter the following commands on the VSX primary switch:

```
vsx
vsx-sync dhcp-relay
exit
```
- B)
- Enter the following commands on the VSX secondary switch:

```
vlan 1000
ip relay-address 10.200.1.100
exit
```
- C)
- Add an SVI in the 10.102.39.0/24 subnet on the Aruba CX 6100 switch that the APs are connected to.

D)

Enter the following commands on the Aruba CX 6100 switch:

```
interface vlan 1000
ip helper-address 10.200.1.100
exit
```

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

Answer: C**Explanation:**

Option C is the only action that configures the DHCP relay on the SVI of VLAN 1000 on the CX 8360 switches. DHCP relay is a feature that allows a switch to forward DHCP requests from clients in one subnet to a DHCP server in another subnet. DHCP relay is required when the DHCP server and the clients are not in the same broadcast domain1.

Option C uses the following commands:

? interface vlan 1000: This command enters the interface configuration mode for the SVI of VLAN 1000, which has an IP address of 10.102.39.1/24 and is used for wireless clients.

? ip helper-address vrf default 10.200.1.100: This command configures the IP address of the DHCP server as a helper address for the SVI, which means that the switch will forward DHCP requests from clients on VLAN 1000 to this address. The vrf default parameter indicates that the SVI and the DHCP server are in the same VRF.

NEW QUESTION 58

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 62

You are configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network Traffic originating from 10.2.250.0/24 should use a new default route to 10.1.1.253. Other non-default routes for this subnet should not be affected by this change.

What are two parts of the solution for these requirements? (Select two.)

A)

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

B)

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

C)

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

D)

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

E)

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

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

Answer: CE

Explanation:

Two parts of the solution for these requirements are Option C and Option E. Option C is a part of the solution because it defines a policy-based routing action list named route_test, which specifies the next hop IP address as 10.1.1.253 for the matching traffic. This is the new default route that the user wants to use for the subnet 10.2.250.0/24. The interface null parameter indicates that the traffic will be routed to the next hop without using a specific interface1.

Option E is a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 250, which has an IP address of 10.2.250.1/24. This is the subnet that the user wants to test the new default route for. The apply policy command enables policy-based routing on the interface and associates it with the action list2.

Option A is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify the next hop IP address as 10.1.1.253, which is the new default route that the user wants to use. Instead, it specifies a next hop IP address of 10.1.1.254, which is different from the requirement.

Option B is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify any next hop IP address at all, which is necessary for policy-based routing to work. Instead, it specifies an interface null parameter without any IP address, which is invalid.

Option D is not a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 200, which has an IP address of 10.2.200.1/24. This is not the subnet that the user wants to test the new default route for, but a different subnet that should not be affected by this change.

NEW QUESTION 64

Your customer is interested in hearing more about how roles can help keep consistent policy enforcement in a distributed overlay fabric How would you explain this concept to them"

- A. Group Based Policy ID is applied on egress VTEP after device authentication and policy is enforced on ingress VTEP
- B. Role-based policies are tied to IP addresses which have an advantage over IP-based policies and role names are sent between VTEPs
- C. Group Based Policy ID is applied on ingress VTEP after device authentication and policy is enforced on egress VTEP
- D. Role-based policies enhance User Based Tunneling across the campus network and the policy traffic is protected with IPsec

Answer: C

Explanation:

This is the correct explanation of how roles can help keep consistent policy enforcement in a distributed overlay fabric. Roles are used to assign group based policy IDs (GBPs) to devices after they authenticate with ClearPass or a local database. GBPs are then used to tag the traffic from the devices and send them to the ingress VTEP, which applies the GBP on the VXLAN header. The egress VTEP then enforces the policy based on the GBP and the destination device. The other options are incorrect because they either do not describe the correct sequence of events or do not use the correct terms. References:

<https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html>

NEW QUESTION 65

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 69

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

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

Answer: A

Explanation:

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

References: 1: Aruba Campus Access documents and learning resources 3: Active gateway over VSX - Aruba

NEW QUESTION 70

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 72

You are deploying Aruba CX 6300's with the customer's 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 2aaa authentication port-access auth-mode multi-domain
- D. interface 1/1/1aaa authentication port-access client-limit 1aaa authentication port-access auth-mode device-mode

Answer: C

Explanation:

Aruba CX 6300 switches support various features to control the port access for different types of devices, such as client mode, device mode, and multidomain mode. These features can help limit the number of clients that can connect to a port and prevent unauthorized devices from accessing the network.

This is because option C shows how to configure the client limit and the auth-mode for a specific port using the interface command and the aaa authentication port-access command. The client limit specifies the maximum number of clients that can connect to a port. The auth-mode specifies the authentication mode for the port. In this case, option C sets both parameters to multi-domain mode, which allows only one voice device and one data device to be authenticated on a port.

https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm 2:

<https://www.arubanetworks.com/products/switches/6300-series/> 3: https://www.arubanetworks.com/techdocs/AOS-CX/10.11/HTML/security_6200-6300-6400/Content/Chp_Port_acc/Port_acc_gen_cmds/aaa-aut-por-acc-aut-mod-fl-109.htm

NEW QUESTION 76

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 80

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 changes¹. 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 tasks¹. 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 language¹.

? 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 actions¹.

? 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 language¹.

NEW QUESTION 83

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 84

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

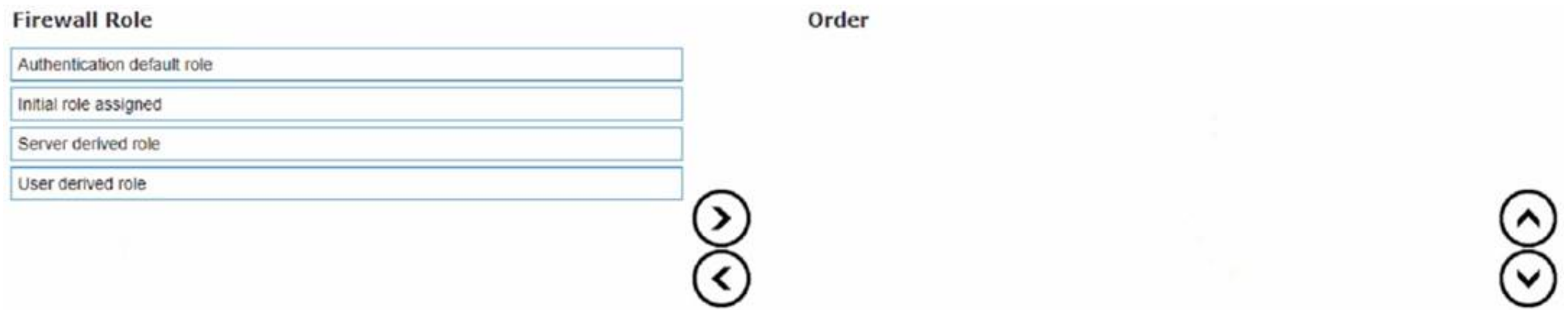
? Class 6 (60W): 802.3bt

? Class 8 (90W): 802.3bt

NEW QUESTION 87

DRAG DROP

List the firewall rule derivation flow in the correct order



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

According to the Aruba Documentation Portal¹, the firewall role derivation flow in the correct order is:

- ? Server derived role
- ? User derived role
- ? Authentication default role
- ? Initiation role assigned

NEW QUESTION 90

you are implementing ClearPass Policy Manager with EAP-TLS for authenticating all corporate-owned devices.

What are two possible solutions to the problem of deploying client certificates to corporate MacBooks that are joined to a Windows domain? (Select two.)

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

Answer: AB

Explanation:

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

Apple Configurator is a tool that allows you to configure and deploy Mac computers using a GPO. This tool can also be used to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate.

NEW QUESTION 91

You are building a configuration in Central that will be used for a standardized network design for small sites for your company, you want to use GUI configuration for gateways and Aps, while template configuration for switches. You need to align with Aruba best practices.

Which set of actions will satisfy these requirements?

- A. Create one group in Central for switches a second group for AP
- B. and a third group for gateways Create a unique site for each location, and assign devices to the appropriate site.
- C. Create one group in Central for switches and a second group for APs and gateway
- D. Create a unique site for each location, and assign devices to the appropriate site.
- E. Create a single group in Centra
- F. Create a unique site for each location, and assign devices to the appropriate site.
- G. Create a single group in Centra
- H. Create a unique site for each type of device, and assign devices to the appropriate site.

Answer: C

Explanation:

This is because option C shows how to create a single group in Central with different configuration methods defined for each device type. For example, you can create a group with the name Group1, and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (Group1). If a device type in the group is marked for template-based configuration method, the group name is prefixed with TG (TG Group1). You can use Group1 as the group ID for workflows such as user management, monitoring, reports, and audit trail².

<https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/abt-groups.htm> 2:

<https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/groups.htm>

NEW QUESTION 93

DRAG DROP

What is the order of operations for Key Management service for a wireless client roaming from AP1 to AP2?

Operation

Cache the client's information

Client associates and authenticates to AP1

Generate Pairwise Master Key keys for AP1's neighbors

Get AP1 neighbor AP list

Share Pairwise Master Key along with VLAN and User Role to target APs

Order

>

<

↑

↓

- A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://www.arubanetworks.com/techdocs/Instant_85_WebHelp/Content/instant-ug/wlan-ssid-conf/conf-fast-roam.htm

NEW QUESTION 95

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 96

DRAG DROP

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

EVPN-VXLAN

User Based Tunneling (UBT)

Answer Area

Centralized Overlay

Distributed Overlay

Encapsulated in UDP

Generic Routing Encapsulation (GRE)

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

EVPN-VXLAN

User Based Tunneling (UBT)

Answer Area

EVPN-VXLAN

EVPN-VXLAN

EVPN-VXLAN

User Based Tunneling (UBT)

Centralized Overlay

Distributed Overlay

Encapsulated in UDP

Generic Routing Encapsulation (GRE)

NEW QUESTION 101

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 104

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 105

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

- A. Sixteen different VMACs are supported total as shared.
- B. Active Gateway can once MSTP instances are created for VLAN load sharing.
- C. Sixteen different VMACs are supported for each IPV4 and IPV6 stack simultaneously
- D. copied over the ISL link for an optimized path.

Answer: C

Explanation:

The active gateway feature is used to provide active-active layer 3 default gateway for hosts on the same subnet. It allows the switch to convert multicast streams into unicast streams over the wireless link, which improves the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. The active gateway feature is unique to VSX configuration because it eliminates the need for VRRP and avoids traffic being pushed over the ISL link, which can cause latency in the network.

The correct answer to the question is C. Sixteen different VMACs are supported for each IPv4 and IPv6 stack simultaneously. This means that you can have a maximum of eight VMACs for IPv4, and a maximum of eight VMACs for IPv6, on a VSX pair. Only 15 VMACs are supported on 6400 switch series.

The other options are incorrect because:

? A. Sixteen different VMACs are not supported total as shared. They are supported for each IPv4 and IPv6 stack separately.

? B. Active gateway can be used without MSTP instances. MSTP is a protocol that allows multiple spanning tree instances to coexist on the same switch, but it

does not affect how active gateway works.

? D. Active gateway does not copy traffic over the ISL link for an optimized path. It avoids using the ISL link for routed traffic and uses the local switch interface MAC instead of the virtual MAC address (VMAC) for source address1.

NEW QUESTION 106

A network administrator is troubleshooting some issues guest users are having when connecting and authenticating to the network. The access switches are AOS-CX switches.

What command should the administrator use to examine information on which role the guest user has been assigned?

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

Answer: A

Explanation:

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

NEW QUESTION 107

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 110

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 111

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-ch02.html

NEW QUESTION 116

A customer is looking for a wireless authentication solution for all of their IoT devices that meet the following requirements

- The wireless traffic between the IoT devices and the Access Points must be encrypted
- Unique passphrase per device
- Use fingerprint information to perform role-based access

Which solutions will address the customer's requirements? (Select two.)

- A. MPSK and an internal RADIUS server
- B. MPSK Local with MAC Authentication
- C. ClearPass Policy Manager
- D. MPSK Local with EAP-TLS
- E. Local User Derivation Rules

Answer: CD

Explanation:

The correct answers are C and D.

MPSK (Multi Pre-Shared Key) is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices¹. MPSK requires MAC authentication against a ClearPass Policy Manager server, which returns the encrypted passphrase for the device in a RADIUS VSA². ClearPass Policy Manager is a platform that provides role-and device-based network access control for any user across any wired, wireless and VPN infrastructure³. ClearPass Policy Manager can also use device profiling and posture assessment to assign roles based on device fingerprint information⁴.

MPSK Local is a variant of MPSK that allows the user to configure up to 24 PSKs per SSID locally on the device, without requiring ClearPass Policy Manager⁵.

MPSK Local can be combined with EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), which is a secure authentication method that uses certificates to encrypt the wireless traffic between the IoT devices and the access points⁶. EAP-TLS can also use device certificates to perform role-based access control⁶.

Therefore, both ClearPass Policy Manager and MPSK Local with EAP-TLS can meet the customer's requirements for wireless authentication, encryption, unique passphrase, and role-based access for their IoT devices.

MPSK and an internal RADIUS server is not a valid solution, because MPSK does not support internal RADIUS servers and requires ClearPass Policy Manager⁷⁸⁹. MPSK Local with MAC Authentication is not a valid solution, because MAC Authentication does not encrypt the wireless traffic or use fingerprint information for role-based access². Local User Derivation Rules are not a valid solution, because they do not provide unique passphrase per device or use fingerprint information for role-based access¹⁰¹¹¹².

NEW QUESTION 119

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 124

What is an OSPF transit network?

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

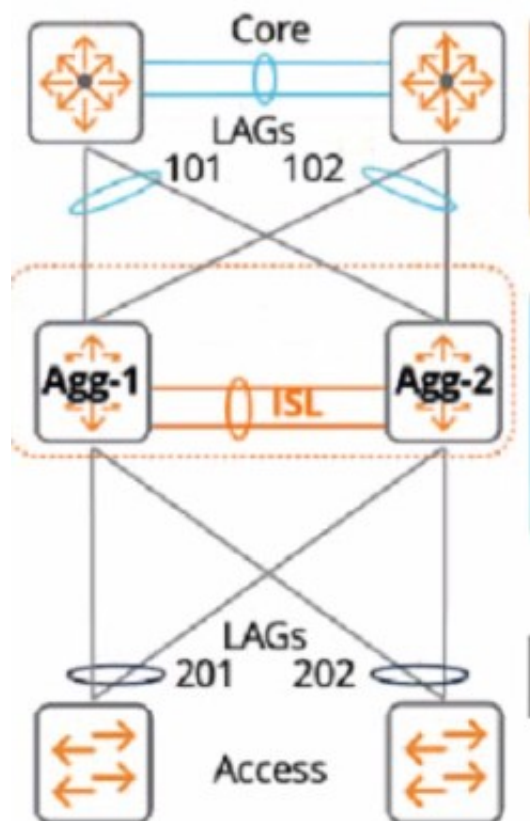
Answer: A

Explanation:

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

NEW QUESTION 125

A customer just upgraded aggregation layer switches and noticed traffic dropping for 120 seconds after the aggregation layer came online again. What is the best way to avoid having this traffic dropped given the topology below?



- A. Configure the linkup delay timer to 240 seconds to double the amount of time for the initial phase to sync
- B. Configure the linkup delay timer to exclude LAGs 101 and 102, which will allow time for routing adjacencies to form and to learn upstream routes
- C. Configure the linkup delay timer to include LAGs 101 and 102, which will allow time for routing adjacencies to form and to learn upstream routes
- D. Configure the linkup delay timer to 120 seconds, which will allow the right amount of time for the initial phase to sync

Answer: C

Explanation:

The reason is that the linkup delay timer is a feature that delays bringing downstream VSX links up, following a VSX device reboot or an ISL flap. The linkup delay timer has two phases: initial synchronization phase and link-up delay phase.

The initial synchronization phase is the download phase where the rebooted node learns all the LACP+MAC+ARP+STP database entries from its VSX peer through ISLP. The initial synchronization timer, which is not configurable, is the required time to download the database information from the peer.

The link-up delay phase is the duration for installing the downloaded entries to the ASIC, establishing router adjacencies with core nodes and learning upstream routes. The link-up delay timer default value is 180 seconds. Depending on the network size, ARP/routing tables size, you might be required to set the timer to a higher value (maximum 600 seconds).

When both VSX devices reboot, the link-up delay timer is not used.

Therefore, by configuring the linkup delay timer to include LAGs 101 and 102, which are part of the same VSX device as LAG 201, you can ensure that both devices have enough time to synchronize their databases and form routing adjacencies before bringing down their downstream links.

NEW QUESTION 127

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 payload.

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 networks.

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 cannot have more than one VNI.

NEW QUESTION 130

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 135

.....

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](#)