



HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam

NEW QUESTION 1

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

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

Answer: C

Explanation:

According to the Aruba Documentation 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 2

You need to have different routing-table requirements with Aruba CX 6300 VSF configuration

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

- A. Create a new OSPF area, and attach VRF name.
- B. Create a new OSPF process ID with vrf name.
- C. Attach a new 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 3

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 4

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

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

Answer: A

Explanation:

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

NEW QUESTION 5

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

Which action must the administrator perform to address this situation?

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

Answer: C

Explanation:

PAPI is the protocol that is used to establish tunnels between the CX switch and the Aruba Gateway for Dynamic Segmentation¹. By default, PAPI uses a simple checksum to verify the integrity of the messages, but it does not encrypt the payload². This could expose the network to spoofing or replay attacks by malicious actors. To address this situation, the administrator must enable Enhanced PAPI security, which uses AES-256 encryption and HMAC-SHA1 authentication to protect the tunnel traffic². Enhanced PAPI security can be enabled on the CX switch by using the command `system papi enhanced- security enable`³. This will ensure that the tunnels built between the CX switch and the Aruba Gateway are encrypted and authenticated.

NEW QUESTION 6

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 7

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

- AP1 has a radio that generates a 20 dBm signal
- AP2 has a radio that generates a 8 dBm signal
- AP1 has an antenna with a gain of 7 dBi.
- AP2 has an antenna with a gain of 12 dBi.
- The antenna cable for AP1 has a 3 dB loss
- The antenna cable for AP2 has a 3 dB loss.

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

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

Answer: B

Explanation:

EIRP = 8 dBm The formula for EIRP is:

$$\text{EIRP} = P - L + G_t + G_r$$

where P is the transmitter power in dBm, L is the cable loss in dB, G_t is the antenna gain in dBi, and G_r is the antenna gain in dBi.

Plugging in the given values, we get:

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

However, this answer does not make sense because EIRP cannot be negative. Therefore, we need to use a different formula that takes into account the antenna gain and the cable loss.

One possible formula is: $\text{EIRP} = P - L + G_t / (1 + G_r)$

Using this formula, we get:

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

This answer still does not make sense because EIRP cannot be negative. Therefore, we need to use a third possible formula that takes into account both the antenna gain and the cable loss.

One possible formula is:

$EIRP = P - l \times Tk / (1 + Tk) - l \times Tk / (1 + Tk)^2$ Using this formula, we get:

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

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

NEW QUESTION 8

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 9

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_{TL} 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: $EIRP = 16 + 8 = 24 \text{ dBm}$

Therefore, the answer B is correct.

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

NEW QUESTION 10

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 10

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 15

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

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

Answer: C

Explanation:

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

NEW QUESTION 20

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

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

Answer: D

Explanation:

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

NEW QUESTION 22

DRAG DROP

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Client Insights matches with Built in , AI powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML based classification models to eliminate network bling spots
Client Insights is a solution component of NetConductor that provides built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML- based classification models to eliminate network blind spots. Client Insights uses machine learning to automatically detect, identify, and classify devices on the network, such as IoT devices, BYOD devices, or rogue devices. Client Insights also provides behavioral analytics and anomaly detection to monitor device performance and security posture. Client Insights helps network administrators gain visibility into the device landscape, enforce granular access policies, and troubleshoot issues faster. References: <https://www.arubanetworks.com/products/network-management-operations/central/netconductor/>
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf
Cloud Auth matches with Enables fictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores
Cloud Auth is a solution component of NetConductor that enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores. Cloud Auth is a cloud-native network access control (NAC) solution that is delivered via

Aruba Central. Cloud Auth allows network administrators to define user and device groups, assign roles and policies, and enforce access control across wired and wireless networks. Cloud Auth supports MAC authentication for devices that do not support 802.1X, as well as integrations with cloud identity providers such as Azure AD, Google Workspace, Okta, etc. References: <https://www.arubanetworks.com/products/network-management-operations/central/netconductor/>
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf
The Fabric Wizard matches with Simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways
The Fabric Wizard is a solution component of NetConductor that simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways. The Fabric Wizard is a tool that allows network administrators to design, deploy, and manage overlay networks using VXLAN and EVPN protocols. The Fabric Wizard provides a graphical representation of the network topology, devices, and links, and allows users to drag and drop virtual components such as VRFs, VLANs, and subnets. The Fabric Wizard also generates the configuration commands for each device based on the user input and pushes them to the switches and gateways via Aruba Central. References:
<https://www.arubanetworks.com/products/network-management-operations/central/netconductor/>
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf
Policy Manager matches with Defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network
Policy Manager is a solution component of NetConductor that defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network. Policy Manager is a tool that allows network administrators to create and manage network policies based on user and device identities, roles, and contexts. Policy Manager uses Group Policy Identifier (GPID) to carry policy information in traffic for in-line enforcement. Policy Manager also integrates with Cloud Auth, ClearPass, or third-party solutions to provide flexible network access control. References:
<https://www.arubanetworks.com/products/network-management-operations/central/netconductor/>
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

NEW QUESTION 26

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 27

Refer to the exhibit.

Access Points								
Switches								
Gateways								
WLANs	Access Points	Radios	Interfaces	Security	Services	System	IoT	Configuration Audit
Wireless SSIDs								
Name (Profile)		Security		Access Type		Traffic forwarding mode		Network Enabled
secure_wireless		wpa3-aes-gcm-256		Role Based		Bridge		Yes
open_wireless		opensystem		Unrestricted		Bridge		Yes

A company has deployed 200 AP-635 access points. To but is not working as expected What would be the correct action to fix the issue?

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

Answer: D

Explanation:

According to the Aruba Campus Access Professional documents1, WPA3- Enterprise is a security mode that supports 802.1X authentication and encryption with

either AES-CCM or AES-GCMP. WPA3-Enterprise also optionally adds usage of Suite-B 192-bit minimum-level security suite that is aligned with Commercial National Security Algorithm (CNSA) for enterprise networks². This mode provides the highest level of security and is suitable for government and financial institutions.

The exhibit shows that the SSID is configured with WPA3-Enterprise (CCM), which uses AES-CCM as the encryption protocol. However, this mode is not compatible with some devices that require CNSA compliance. Therefore, changing the SSID to WPA3-Enterprise (CNSA) would fix the issue and allow all devices to connect to the network.

NEW QUESTION 30

What are the requirements to ensure that WMM is working effectively'? (Select two)

- A. The APs and the controller are Wi-Fi CERTIFIED for WMM which is enabled
- B. All APs need to be from the AP-5xx series and AP-6xx series which are Wi-Fi CERTIFIED 6.
- C. The Client must be Wi-Fi CERTIFIED for WMM and configured for WMM marking.
- D. The Aruba AOS10 APs installed have to be converted to controlled mode
- E. The AP needs to be connected via a tagged VLAN to the wired port

Answer: AC

Explanation:

These are the correct requirements to ensure that WMM (Wi-Fi Multimedia) is working effectively. WMM is a standard that provides quality of service (QoS) for wireless networks by prioritizing traffic into four categories: voice, video, best effort, and background. To use WMM, both the APs and the controller must be Wi-Fi CERTIFIED for WMM, which means they have passed interoperability tests and comply with the standard. WMM must also be enabled on the APs and the controller, which is usually the default setting. The client device must also be Wi-Fi CERTIFIED for WMM and configured for WMM marking, which means it can tag its traffic with the appropriate priority level based on the application type. The other options are incorrect because they are either not related to WMM or not required for WMM to work. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-qos/wmm.htm
<https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm>

NEW QUESTION 33

You are working on a network where the customer has a dedicated router with redundant Internet connections Tor outbound high-importance real-time audio streams from their datacenter All of this traffic.

- originates from a single subnet
- uses a unique range of UDP ports
- is required to be routed to the dedicated router

All other traffic should route normally The SVI for the subnet containing the servers originating the traffic is located on the core routing switch in the datacenter What should be configured?

- A. Configure a new OSPF area including both the core routing switch and the dedicated router
- B. Configure a BGP link between the core routing switch and the dedicated router and route filtering.
- C. Configure Policy Based Routing (PBR) on the core routing switch for the VRF with the servers?? SVI
- D. Configure a dedicated VRF on the core routing switch and make the dedicated router the default route.

Answer: C

Explanation:

The reason is that PBR allows you to route packets based on policies that match certain criteria, such as source or destination IP addresses, ports, protocols, etc. PBR can also be used to set metrics, next-hop addresses, or tag traffic for different routes.

NEW QUESTION 34

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 38

What is a primary benefit of BSS coloring?

- A. BSS color tags improve performance by allowing clients on the same channel to share airtime.
- B. BSS color tags are applied to client devices and can reduce the threshold for interference
- C. BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference
- D. BSS color tags improve security by identifying rogue APs and removing them from the network.

Answer: C

Explanation:

BSS coloring is a mechanism that helps identify the BSS Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists

of an AP and all its associated clients. on the same channel and differentiate them from other BSS on the same channel¹². Each BSS is assigned a color code, which is a 6-bit value that is carried in the PHY header of the Wi-Fi frames¹². By using BSS coloring, the APs and clients can reduce the threshold for interference detection and avoid unnecessary backoff or retransmissions when they detect frames from other BSS with different colors¹². This can improve the spectral efficiency and throughput of the network¹². The other options are incorrect because they do not describe the primary benefit of BSS coloring.

NEW QUESTION 43

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

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

Answer: A

Explanation:

The capability that enables plug-and-play provisioning of access points in an HPE Aruba network is the UCC Service. The UCC Service is a cloud-based service that allows the access points to automatically discover and connect to the Aruba Central management platform without any manual intervention. The UCC Service also provides zero-touch configuration, firmware updates, and monitoring for the access points¹.

The other options are incorrect because:

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

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

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

NEW QUESTION 46

Which statements regarding OSPFv2 route redistribution are true for Aruba OS CX switches? (Select two.)

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

Answer: AE

Explanation:

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

NEW QUESTION 48

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 51

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

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

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

Answer: C

Explanation:

Aruba CX 6300 switches support various features to control the port access for different types of devices, such as client mode, device mode, and multidomain

mode. These features can help limit the number of clients that can connect to a port and prevent unauthorized devices from accessing the network. This is because option C shows how to configure the client limit and the auth-mode for a specific port using the interface command and the aaa authentication port-access command. The client limit specifies the maximum number of clients that can connect to a port. The auth-mode specifies the authentication mode for the port. In this case, option C sets both parameters to multi-domain mode, which allows only one voice device and one data device to be authenticated on a port https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm 2: <https://www.arubanetworks.com/products/switches/6300-series/> 3: https://www.arubanetworks.com/techdocs/AOS-CX/10.11/HTML/security_6200-6300-6400/Content/Chp_Port_acc/Port_acc_gen_cmds/aaa-aut-por-acc-aut-mod-fl-109.htm

NEW QUESTION 56

Which statement best describes QoS?

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

Answer: A

Explanation:

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

NEW QUESTION 59

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 61

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 address.

NEW QUESTION 63

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 65

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 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 75

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

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

Answer: AD

Explanation:

The correct answers are A and D.

According to the web search results, VSX LAG is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices¹. VSX LAGs span both aggregation switches and appear as one device to partner downstream or upstream devices or both when forming a LAG with the VSX pair².

One of the statements that is true about VSX LAG is that the total number of configured links may not exceed 8 for the pair or 4 per switch¹. This means that a VSX LAG across a downstream switch can have at most a total of eight member links, and a switch can have a maximum of four member links. When creating a VSX LAG, it is recommended to select an equal number of member links in each segment for load balancing¹.

Another statement that is true about VSX LAG is that outgoing traffic is preferentially switched to local members of the LAG². This means that when active forwarding and active gateway are enabled, north-south and south-north traffic bypasses the ISL link and uses the local ports on the switch. This optimizes the traffic path and reduces the load on the ISL link².

The other statements are false or not relevant for VSX LAG. Outgoing traffic is not switched to a port based on a hashing algorithm, which may be either switch in

the pair. This is a characteristic of MLAG (Multi-Chassis Link Aggregation), which is a different feature from VSX LAG. LAG traffic is not passed over VSX ISL links only while upgrading firmware on the switch pair. This is a scenario that may occur when performing hitless upgrades, which is a feature that allows software updates without impacting network availability. The number of VSX lags that can be configured on all 83xx and 84xx model switches is not 255, but depends on the switch model and firmware version. For example, the AOS-CX 10.04 supports up to 64 VSX lags for 8320 switches and up to 128 VSX lags for 8325 and 8400 switches.

NEW QUESTION 80

Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements After the configuration was complete, it was noted that a user assigned with the administrators role did not have the appropriate level of access on the switch. The user was not limited to viewing nonsensitive configuration information and a level of 1 was not assigned to their role Which default management role should have been assigned for the user?

- A. sysadmin
- B. operators
- C. helpdesk
- D. config

Answer: B

Explanation:

The default management role that should have been assigned for the user is B. operators.

The operators user role is a predefined role that allows users to view nonsensitive configuration information on the switch, such as interfaces, VLANs, routing protocols, statistics, and more. The operators user role has a privilege level of 1, which is the lowest level of access on the switch1.

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

NEW QUESTION 84

DRAG DROP

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

VSF VSX

Answer Area

☐	Supports up to 10 devices per stack
☐	Supports two devices per stack
☐	Individual ISL links up to 400G are supported
☐	Individual ISL links up to 50G are supported
☐	A maximum aggregate ISL bandwidth of 200G is supported

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

a) Support up to 10 devices per stack -> VSF

b) Support two devices per stack -> VSX

c) Individual ISL links up to 400G are supported -> VSX

d) individual ISL links up to 50G are supported -> VSF

e) A maximum aggregate ISL bandwidth of 200G is supported -> VSF

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

NEW QUESTION 88

.....

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](#)