

HPE7-A01 Dumps

Aruba Certified Campus Access Professional Exam

<https://www.certleader.com/HPE7-A01-dumps.html>



NEW QUESTION 1

The administrator notices that wired guest users that have exceeded their bandwidth limit are not being disconnected. Access Tracker in ClearPass indicates a disconnect CoA message is being sent to the AOS-CX switch.

An administrator has performed the following configuration:

```
Access1(config)# ip dns host cppm.arubatraining.com 10.254.1.23 vrf mgmt
Access1(config)# radius-server host cppm.arubatraining.com key plaintext aruba123 vrf mgmt
Access1(config)# aaa group server radius cppm
Access1(config-sg)# server cppm.arubatraining.com vrf mgmt
Access1(config-sg)# exit
Access1(config)# aaa accounting port-access start-stop interim 5 group cppm
Access1(config)# radius dyn-authorization client cppm.arubatraining.com secret-key plaintext aruba123 vrf mgmt
Access1(config)# radius dyn-authorization enable
```

What is the most likely cause of this issue?

- A. Change of Authorization has not been globally enabled on the switch
- B. The SSL certificate for CPPM has not been added as a trust point on the switch
- C. There is a mismatch between the RADIUS secret on the switch and CPPM.
- D. There is a time difference between the switch and the ClearPass Policy Manager

Answer: D

Explanation:

Change of Authorization (CoA) is a feature that allows ClearPass Policy Manager (CPPM) to send messages to network devices such as switches to change the authorization state of a user session. CoA requires that both CPPM and the network device support this feature and have it enabled. For AOS-CX switches, CoA must be globally enabled using the command `radius-server coa enable`. If CoA is not enabled on the switch, the disconnect CoA message from CPPM will be ignored and the user session will not be terminated. References:

https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/index.htm#CPPM_UserGuide/Admin/ChangeOfAuthorization.htm

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

NEW QUESTION 2

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 3

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

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

Answer: A

Explanation:

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

NEW QUESTION 4

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

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

Answer: A

Explanation:

The standard that is supported by some Aruba APs and can enable a customer to accurately locate wireless client devices within a few meters is A. 802.11mc.

* 802.11mc is an IEEE standard that enables computing devices to measure the distance to nearby Wi-Fi access points using a technique called Fine Timing Measurement (FTM). FTM uses precise timestamps to calculate the round-trip time of Wi-Fi frames between the device and the access point, and then converts it

to a distance estimate. By using multiple access points and triangulation methods, the device can determine its location with high accuracy¹. According to the Aruba document 802.11mc Support, this feature is supported on 500 Series, 510 Series, 530 Series, 550 Series, 560 Series and 570 Series access points. These APs act as FTM responders to time measurement queries sent from a client. To configure the AP to send FTM responses, you need to enable the `ftm-responder-enable` parameter in the WLAN SSID profile¹.

NEW QUESTION 5

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

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

The customer is using Aruba CX 6300s

What is the correct way to implement these requirements?

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 6

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

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

Answer: A

Explanation:

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

NEW QUESTION 7

A customer has a site with 200 AP-515 access points and 75 AP-565 access points installed.

The customer is rolling out new mobile phones with Wi-Fi calling. 802.1X is in use for authentication.

What should be enabled to ensure the best roaming experience?

- A. 802.1X
- B. 802.11r
- C. 802.11W
- D. 802.11h

Answer: A

Explanation:

<https://www.howtogeek.com/794724/what-is-wi-fi-calling/> ²:

<https://www.networkcomputing.com/networking/your-network-optimized-wifi-calling> ³: https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fro-pan-led-630.htm

Wi-Fi calling is a feature that allows you to make or receive voice calls over Wi-Fi instead of cellular network. Wi-Fi calling can provide better voice quality and reliability in areas with poor or no cellular coverage.

NEW QUESTION 8

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 9

By default, Best Effort is higher priority than which priority traffic type?

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

Answer: B

Explanation:

This is because Best Effort traffic is all other kinds of non-detrimental traffic that are not sensitive to Quality of Service metrics (jitter, packet loss, latency). A typical example would be peer-to-peer and email applications². Background traffic is a type of traffic that is used for system maintenance or backup purposes and does not affect the performance or availability of the network³.

Therefore, Best Effort traffic has a higher priority than Background traffic in terms of network resources allocation and management.

1: <https://www.arubanetworks.com/techdocs/ArubaDocPortal/content/docportal.htm> 2: <https://stackoverflow.com/questions/33854306/best-effort-traffic-and-real-time-traffic-difference> 3: <https://www.informit.com/articles/article.aspx?p=25315&seqNum=4>

NEW QUESTION 10

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: $EIRP = 16 + 8 - 4 = 20$ 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 10

What is used to retrieve data stored in a Management Information Base (MIB)?

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

Answer: A

Explanation:

The correct answer is A. SNMPv3.

SNMPv3 is a protocol that is used to retrieve data stored in a Management Information Base (MIB), which is a database of managed objects in a network.

SNMPv3 provides security and access control features that are not available in earlier versions of SNMP. SNMPv3 can also use encryption to protect the data from unauthorized access or modification.

According to the Aruba Certified Professional – Campus Access document¹, one of the skills that this certification validates is:

? Implement and Analyze the output from common network monitoring tools

The document also mentions that the candidate should have a distinguished understanding of different protocols across vendors, which implies that they should be familiar with SNMPv3 and how it can be used to access MIB data.

NEW QUESTION 12

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 13

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 18

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

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

Answer: B

Explanation:

The correct answer is B. sysops.

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

The other options are incorrect because:

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

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

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

NEW QUESTION 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 24

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 26

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 31

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 35

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

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

https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

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 37

What is a primary benefit of BSS coloring?

- A. BSS color tags improve performance by allowing APS on the same channel to be farther apart
- B. BSS color tags improve security by identifying rogue APS and tagging them as threats.
- C. BSS color tags are applied on the wireless controllers and can reduce the threshold for interference_
- D. BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference

Answer: D

Explanation:

The primary benefit of BSS coloring is D. BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference.

BSS coloring is a mechanism that allows Wi-Fi 6 devices to mark each frame with a color code that identifies the BSS (Basic Service Set) it belongs to. This helps differentiate between frames from different BSSs that share the same channel and avoid unnecessary collisions and backoffs. BSS coloring also introduces an adaptive threshold for interference, which means that Wi-Fi 6 devices can adjust the signal strength value that determines whether a channel is busy or not based on the current network environment. This allows for more efficient use of spectrum and higher throughput in dense scenarios¹².

NEW QUESTION 42

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 46

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 48

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.

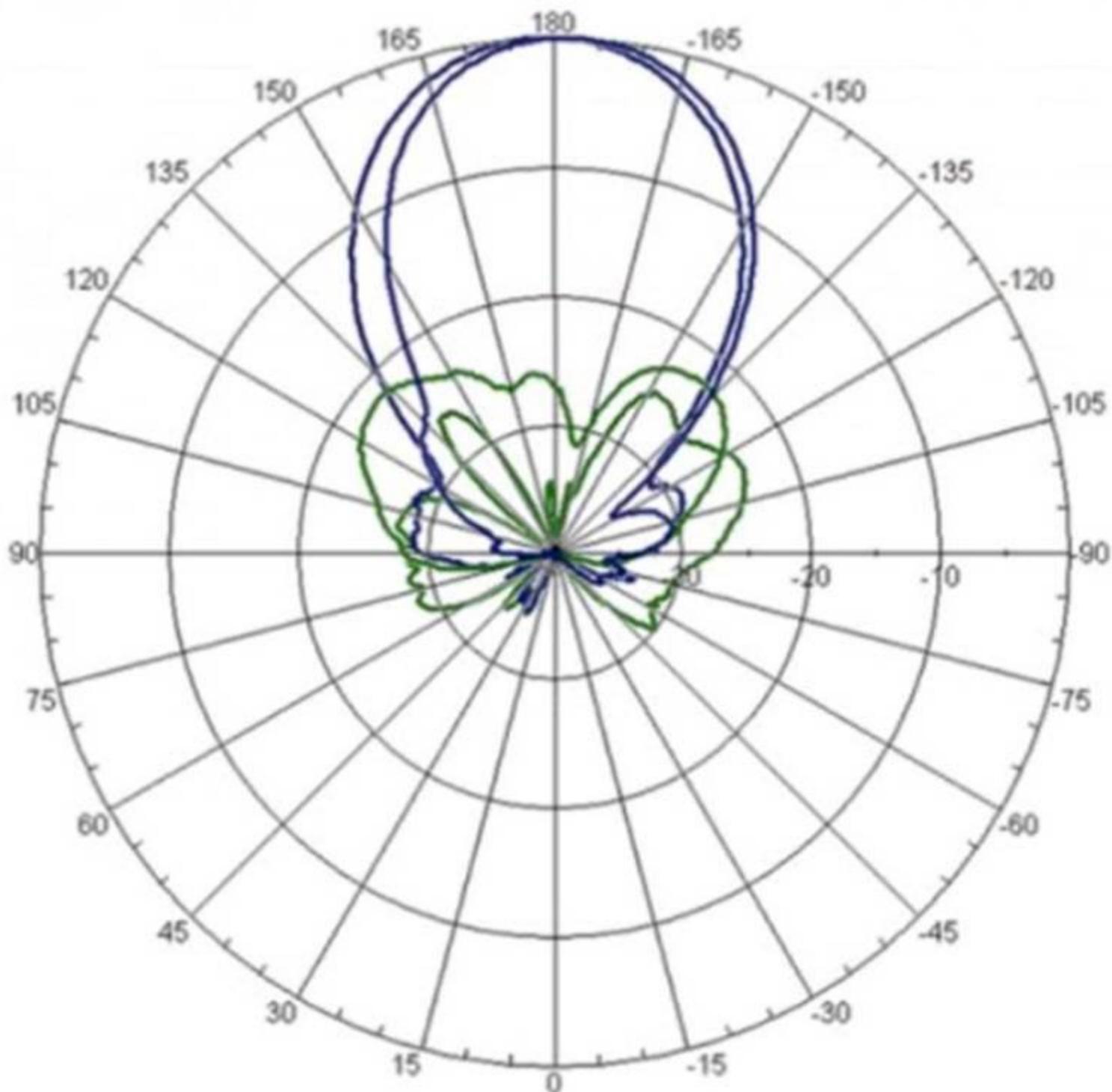
Option A is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify the next hop IP address as 10.1.1.253, which is the new default route that the user wants to use. Instead, it specifies a next hop IP address of 10.1.1.254, which is different 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 49

Refer to the image.



Horizontal Pattern

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

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

Answer: B

Explanation:

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

NEW QUESTION 50

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 51

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 55

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 58

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 61

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 65

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 67

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 71

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 75

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 78

DRAG DROP

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

EVPN-VXLAN User Based Tunneling (UBT)

Answer Area

- Centralized Overlay
- Distributed Overlay
- Encapsulated in UDP
- Generic Routing Encapsulation (GRE)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

EVPN-VXLAN User Based Tunneling (UBT)

Answer Area

- EVPN-VXLAN Centralized Overlay
- EVPN-VXLAN Distributed Overlay
- EVPN-VXLAN Encapsulated in UDP
- User Based Tunneling (UBT) Generic Routing Encapsulation (GRE)

NEW QUESTION 83

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 84

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

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

Answer: B

Explanation:

The difference in the noise floor perceived by a client using a bonded 40 MHz wide channel as compared to an unbonded 20 MHz wide channel is 3 dB. The noise

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

NEW QUESTION 85

Which method is used to onboard a new UXI in an existing environment with 802.1X authentication? (The sensor has no cellular connection)

- A. Use the UXI app on your smartphone and connect the UXI via Bluetooth
- B. Use the Aruba installer app on your smartphone to scan the barcode
- C. Connect the new UXI from an already installed one and adjust the initial configuration.
- D. Use the CLI via the serial cable and adjust the initial configuration.

Answer: A

Explanation:

To onboard a new UXI in an existing environment with 802.1X authentication, you need to use the UXI app on your smartphone and connect the UXI via Bluetooth. The UXI app allows you to scan the QR code on the UXI sensor and configure its network settings, such as SSID, password, IP address, etc. The Bluetooth connection allows you to communicate with the UXI sensor without requiring any network access or cellular connection. The other options are incorrect because they either do not use the UXI app or do not use Bluetooth. References: <https://www.arubanetworks.com/products/network-management-operations/analytics-monitoring/user-experience-insight-sensors/> https://help.centralon-prem.arubanetworks.com/2.5.4/documentation/online_help/content/nms-on-prem/aos-cx/get-started/uxi-sensor.htm

NEW QUESTION 90

You need to create a keepalive network between two Aruba CX 8325 switches for VSX configuration. How should you establish the keepalive connection?

- A. SVI, VLAN trunk allowed all on ISL in default VRF
- B. routed port in custom VRF
- C. loopback 0 and OSPF area 0 in default VRF
- D. SVI, VLAN trunk allowed all on ISL in custom VRF

Answer: B

Explanation:

To establish a keepalive connection between two Aruba CX 8325 switches for VSX configuration, you need to use a routed port in custom VRF. A routed port is a physical port that acts as a layer 3 interface and does not belong to any VLAN. A custom VRF is a virtual routing and forwarding instance that provides logical separation of routing tables. By using a routed port in custom VRF, you can isolate the keepalive traffic from other traffic and prevent routing loops or conflicts. The other options are incorrect because they either do not use a routed port or do not use a custom VRF. 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 93

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 96

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 97

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

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

Answer: BE

Explanation:

These are the correct statements regarding the ERSPAN session that needs to be established on an AOS-CX switch for a network administrator to examine the packets over a period of time from their desktop. ERSPAN (Encapsulated Remote Switched Port Analyzer) is a feature that allows an AOS-CX switch to mirror traffic from one or more source ports or VLANs to a remote destination IP address over a GRE (Generic Routing Encapsulation) tunnel. The destination IP address must be the IP address of the administrator's desktop, which must have a packet capture tool installed to receive and analyze the mirrored traffic. The encapsulation protocol used for ERSPAN is GRE, which adds a header to the mirrored packets with information such as source and destination IP addresses, session ID, etc. The other statements are incorrect because they either do not specify the correct destination IP address or do not use ERSPAN or GRE. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html>

NEW QUESTION 101

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 Manager^{7,8,9}. 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 access^{10,11,12}.

NEW QUESTION 102

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 107

What does the 802.3bz standard describe?

- A. 2.5Gb and 5Gb Ethernet ports
- B. 60 W and 90W PoE
- C. AP directed roaming between APs
- D. 60 GHz P2P Wi-Fi

Answer: A

Explanation:

802.3bz is a standard for Ethernet over twisted pair at speeds of 2.5 and 5 Gbit/s. These use the same cabling as the ubiquitous Gigabit Ethernet, yet offer higher speeds. The resulting standards are named 2.5GBASE-T and 5GBASE-T.

Option A: 2.5Gb and 5Gb Ethernet ports

This is because option A shows how to identify the speed of an Ethernet port based on its name and the standard it supports. A port that supports 2.5GBASE-T or 5GBASE-T is a multi-gigabit port that can operate at speeds of up to 2.5 Gbit/s or 5 Gbit/s over twisted pair cables23.

Therefore, option A is correct.

1: https://en.wikipedia.org/wiki/2.5GBASE-T_and_5GBASE-T 2: <https://kb.netgear.com/000049004/What-is-Multi-Gigabit-Ethernet-and-how-can-I-benefit-from-using-NETGEAR-Multi-Gigabit-Ethernet-Switches-in-my-network> 3: <https://arstechnica.com/gadgets/2016/09/5gbps-ethernet-standard-details-8023bz/>

NEW QUESTION 112

Which statements are true regarding a VXLAN implementation on Aruba Switches? (Select two.)

- A. MTU size must be increased beyond the default
- B. VNIs encapsulate and decapsulate VXLAN traffic
- C. VTEPs encapsulate and decapsulate VXLAN traffic
- D. They are only available for datacenter switches (CX 8k, 9k,10k)
- E. All Aruba CX switches support VXLAN.

Answer: AB

Explanation:

Option A: MTU size must be increased beyond the default

This is because option A shows how to configure the MTU size for VXLAN tunnels on Aruba switches using the interface command and the vxlan command. The MTU size must be increased beyond the default value of 1500 bytes to accommodate the VXLAN header and payload2.

Therefore, option A is true regarding a VXLAN implementation on Aruba switches. Option B: VNIs encapsulate and decapsulate VXLAN traffic

This is also true regarding a VXLAN implementation on Aruba switches. VNIs are used to encapsulate and decapsulate VXLAN traffic between two devices, such as a switch and a server. VNIs are also used to map VXLAN tunnels to overlay networks3.

Therefore, option B is also true regarding a VXLAN implementation on Aruba switches. VXLAN is a Layer 2 encapsulation technology that substitutes the usage of VLAN numbers to label Ethernet broadcast domains with VXLAN numbers. VXLAN supports 224 Ethernet broadcast domains or VXLAN numbers. A VXLAN number ID is referred to as VNI. There is a one-to-one relationship between an Ethernet broadcast domain and a VNI. A single Ethernet broadcast domain can't have more than one VNI.

NEW QUESTION 116

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

b) Support two devices per stack -> VSX

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

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

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

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

NEW QUESTION 120

A customer has a large number of food-producing machines

- All machines are connected via Aruba CX6200 switches in VLANs 100, 110, and 120
- Several external technicians are maintaining this special equipment

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

A)

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

```
interface lag 1
  no shutdown
  description Uplink-to-Core
  no routing
  vlan trunk native 1
  vlan trunk allowed all
  lacp mode active
  dhcp-snooping trust
```

B)

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

C)

```
dhcpv4-snooping all vlans
no dhcpv4-snooping option 82
interface lag 1
  no shutdown
  description Uplink-to-Core
  no routing
  vlan trunk native 1
  vlan trunk allowed all
  lacp mode active
  dhcpv4-snooping trust
```

D)

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

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

Answer: B

Explanation:

configures DHCP snooping on the switch and enables it for VLANs 100, 110, and 120. It also specifies the IP address of the authorized DHCP server and sets the ports connected to the server as trusted. This prevents any unauthorized DHCP server from providing invalid configuration data to the clients on those VLANs. Option B also enables DHCP option-82, which adds information about the switch port and VLAN to the DHCP packets, allowing for more granular control and logging of DHCP transactions.

NEW QUESTION 123

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your HPE7-A01 Exam with Our Prep Materials Via below:

<https://www.certleader.com/HPE7-A01-dumps.html>