HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam

NEW QUESTION 1
Your customer has an Aruba CX 6200F VSF stack with two switches. A third member (JL726A) needs to be added to the VSF configuration. What e the configuration that enables the new devices to join the VSF?
A)

```
On the new switch issue:

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

B)

```
On the new switch issue:

vsf member 3
    type jl726a
```

C)

```
On the existing VSF issue:

vsf member 3
    stack join
    type jl726a
```

D)

```
On the new switch issue:

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

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

Answer: C

Explanation:
According to the Aruba Documentation Portal1, the Aruba CX 6200F VSF stack is a feature that allows you to create a virtual switching framework (VSF) with up to eight members that can be managed as a single logical device. The VSF stack provides benefits such as load balancing, failover, redundancy, and security.
To add a new device to the VSF stack, you need to configure the device with the VSF command vsf member and specify the type, link, and secondary-member information. The type of the new device can be one of the following: JL726A, JL726B, JL726C, or JL726D. The link is the interface that connects the new device to the existing VSF members. The secondary-member is an optional parameter that specifies which member will act as a backup in case of a failure.
1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7726/index.html 2: https://buy.hpe.com/us/en/networking/switches/fixed-port-l3-managed-ethernet-switches/6000-switch-products/aruba-6200f-48g-4sfp-switch/p/jl726a 3: https://addin.co.th/shop/switch/aruba-switch/6200f-series/jl726a/

NEW QUESTION 2
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.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.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 congestion2. VOQ allows each port to have multiple queues for different output ports and prioritize packets based on their destination and QoS class2. VOQ enables the Aruba CX 6400 switch to achieve high throughput and low latency for various traffic types and
scenarios. References: 2 https://www.arubanetworks.com/assets/ds/DS_CX6400Series.pdf

NEW QUESTION 4
A company recently deployed new Aruba Access Points at different branch offices Wireless 802.1X authentication will be against a RADIUS server in the cloud. The security team is concerned that the traffic between the AP and the RADIUS server will be exposed.
What is the appropriate solution for this scenario?

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

Answer: D

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

NEW QUESTION 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 enable3. This will ensure that the tunnels built between the CX switch and the Aruba Gateway are encrypted and authenticated.

NEW QUESTION 6
A client is connecting to 802.1X SSID that has been configured in tunnel mode with the default AP-group settings.
After receiving Access-Accept from the RADIUS server, the Aruba Gateway will send Access-Accept to the AP through which tunnel?

A. IPsec tunnel
B. Split tunnel
C. GRE tunnel
D. PAR tunnel

Answer: C

Explanation:
According to the Aruba Documentation Portal1, 802.1X is a standard for port- based network access control that uses a RADIUS server to authenticate and authorize wireless clients. 802.1X can be configured in different modes, such as bridge mode, tunnel mode, or split tunnel mode.
Option C: GRE tunnel
This is because option C shows how to configure an SSID in tunnel mode with the default AP-group settings on an Aruba switch. In tunnel mode, all client traffic from the access points is tunneled back to the controller and the controller would in turn put the client traffic onto the network2. The GRE protocol is used to encapsulate and decapsulate the traffic between the access points and the controller3.
Therefore, option C is correct.
1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html 2: https://community.arubanetworks.com/discussion/bridge-and-tunnel-mode 3: https://www.twingate.com/blog/ipsec-tunnel-mode

NEW QUESTION 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 forAP2 has a 3 OB loss.
What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?

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

Answer: B

Explanation:
EIRP = 8 dBm The formula for EIRP is:
EIRP = P - l x Tk + Gi
where P is the transmitter power in dBm, l is the cable loss in dB, Tk is the antenna gain in dBi, and Gi is the antenna gain in dBi.
Plugging in the given values, we get:
EIRP = 20 - 3 x 7 + 12 EIRP = 20 - 21 + 12 EIRP = -1 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: EIRP = P - l x Tk / (1 + Tk)
Using this formula, we get:
EIRP = 20 - 3 x 7 / (1 + 7) EIRP = 20 - 21 / 8 EIRP = -2 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 x Tk / (1 + Tk) - l x Tk / (1 + Tk)^2 Using this formula, we get:
EIRP = 20 - 3 x 7 / (1 + 7) - 3 x 7 / (1 + 7)^2 EIRP = 20 - 21 / 8 - 21 / (8)^2 EIRP = -2 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
When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

A. QSVI
B. MAC tables
C. UDLD

D. RPVST+

Answer: B

Explanation:
The information that the Inter-Switch Link Protocol configuration uses in the configuration created is B. MAC tables.
The Inter-Switch Link Protocol (ISL) is a protocol that enables the synchronization of data and state information between two VSX peer switches. The ISL uses a version control mechanism and provides backward compatibility regarding VSX synchronization capabilities. The ISL can span long distances (transceiver dependent) and supports different speeds, such as 10G, 25G, 40G, or 100G1.
One of the data components that the ISL synchronizes is the MAC table, which is a database that stores the MAC addresses of the devices connected to the switch and the corresponding ports or VLANs. The ISL ensures that both VSX peers have the same MAC table entries and can forward traffic to the correct destination2. The ISL also synchronizes other data components, such as ARP table, LACP states for VSX LAGs, and MSTP states2.

NEW QUESTION 9
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 10
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 10
What is one advantage of using OCSP vs CRLs for certificate validation?

A. reduces latency between the time a certificate is revoked and validation reflects this status
B. less complex to implement
C. higher availability for certificate validation
D. supports longer certificate validity periods

Answer: A

Explanation:
OCSP is a protocol that allows clients to query the CA or a trusted responder for the status of a specific certificate. OCSP requests and responses are smaller and faster than CRLs, and they can provide real-time information about the revocation status of a certificate12. CRLs are lists of all revoked certificates that are downloaded from the
CA. CRLs can present issues, as they can become outdated and have to be downloaded frequently13. Therefore, OCSP reduces latency between the time a certificate is revoked and validation reflects this status. References: 1 https://sectigostore.com/blog/ocsp-vs-crl- whats-the-difference/ 2 https://www.keyfactor.com/blog/what-is-a-certificate-revocation-list-crl-vs-ocsp/ 3 https://www.fortinet.com/resources/cyberglossary/ocsp

NEW QUESTION 11
Your customer is having connectivity issues with a newly-deployed Microbranch group The access points in this group are online in Aruba Central, but no VPN tunnels are forming.
What is the most likely cause of this issue?

A. There is a time difference between the AP and the gateways The gateways should have NTP added
B. The SSL certificate on the gateway used to encrypt the connection has not been added to the APs trust list
C. There may be a firewall blocking GRE tunneling between the AP and the gateway
D. The gateway group is running in automatic cluster mode and should be in manual cluster mode

Answer: C

Explanation:
This is the most likely cause of the issue where the access points in a Microbranch group are online in Aruba Central, but no VPN tunnels are forming. A Microbranch group is a group that contains both APs and Gateways and allows them to form VPN tunnels for secure communication. The VPN tunnels use GRE (Generic Routing Encapsulation) as the encapsulation protocol and IPSec as the encryption protocol. If there is a firewall blocking GRE traffic between the AP and the gateway, the VPN tunnels cannot be established. The other options are incorrect because they either do not affect the VPN tunnel formation or do not apply to a Microbranch group. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/gateways/microbranch.htm https://www.arubanetworks.com/assets/tg/TB_ArubaGateway.pdf

NEW QUESTION 12
Describe the difference between Class of Service (CoS) and Differentiated Services Code Point (DSCP).

A. CoS has much finer granularity than DSCP
B. CoS is only contained in VLAN Tag fields DSCP is in the IP Header and preserved throughout the IP packet flow
C. They are similar and can be used interchangeably.
D. CoS is only used to determine CLASS of traffic DSCP is only used to differentiate between different Classes.

Answer: B

Explanation:
CoS and DSCP are both methods of marking packets for quality of service (QoS) purposes. QoS is a mechanism that allows network devices to prioritize and differentiate traffic based on certain criteria, such as application type, source, destination, etc. CoS stands for Class of Service and is a 3-bit field in the 802.1Q VLAN tag header. CoS can only be used on Ethernet frames that have a VLAN tag, and it can only be preserved within a single VLAN domain. DSCP stands for Differentiated Services Code Point and is a 6-bit field in the IP header. DSCP can be used on any IP packet, regardless of the underlying layer 2 technology, and it can be preserved throughout the IP packet flow, unless it is modified by intermediate devices. References: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mt-book/qos-overview.html https://www.cisco.com/c/en/us/support/docs/lan- switching/8021q/17056-741-4.html https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html

NEW QUESTION 13
Using Aruba best practices what should be enabled for visitor networks where encryption is needed but authentication is not required?

A. Wi-Fi Protected Access 3 Enterprise
B. Opportunistic Wireless Encryption
C. Wired Equivalent Privacy
D. Open Network Access

Answer: B

Explanation:
Opportunistic Wireless Encryption (OWE) is a feature that provides encryption for open wireless networks without requiring authentication. OWE uses an enhanced version of the 4-way handshake to establish a pairwise key between the client and the AP, which is then used to encrypt the wireless traffic using WPA2 or WPA3 protocols. OWE can be used for visitor networks where encryption is needed but authentication is not required. References: https://www.arubanetworks.com/assets/tg/TG_OWE.pdf

NEW QUESTION 17
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 22
When configuring UBT on a switch what will happen when a gateway role is not specified?

A. The switch will put the client on the access VLAN
B. The gateway will assign a default role to the client
C. The switch will assign the default deny role to the client.
D. The gateway will send back the deny role to the client.

Answer: A

Explanation:
According to the Aruba Documentation Portal1, user-based tunneling (UBT) is a feature that uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. UBT enables a switch to provide a centralized security policy, using per- user authentication and access control to ensure consistent access and permissions.
Option A: The switch will put the client on the access VLAN
This is because option A shows how UBT works on an Aruba switch. When a device connects to the network, it is authenticated using either MAC Authentication or 802.1X and triggers an enforcement policy from ClearPass, which contains an enforcement profile with a user role configuration. The user role can be assigned locally on the switch or on ClearPass as part of an enforcement profile. The user role determines the VLAN that the device belongs to and the access policies that apply to it23.
Therefore, option A is correct.
1: https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-ubt.htm 2: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html 3: https://community.arubanetworks.com/viewdocument/?DocumentKey=c740df4e-3e26-4cc5-9126-355a18709c44&CommunityKey=2fd943a6-8898-4dbe-915f-4f09e4d3c317&tab=librarydocuments

NEW QUESTION 25
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).

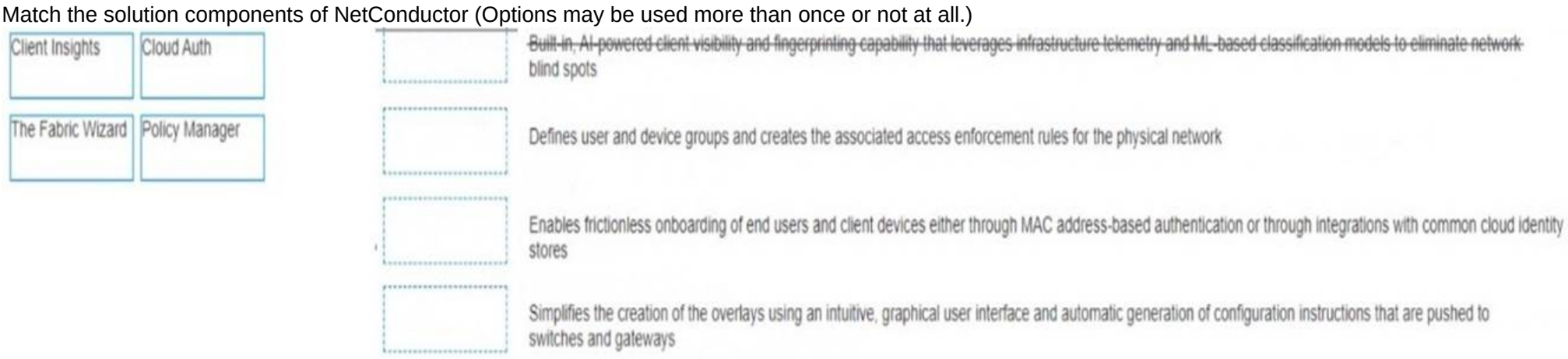
NEW QUESTION 27
A large retail client is looking to generate a rich set of contextual data based on the location information of wireless clients in their stores Which standard uses Round Trip Time (RTT) and Fine Time Measurements (FTM) to calculate the distance a client is from an AP?

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 29
DRAG DROP
Match the solution components of NetConductor (Options may be used more than once or not at all.)



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 30
Your manufacturing client is deploying two hundred wireless IP cameras and fifty headless scanners in their warehouse. These new devices do not support 802.1X authentication.
How can HPE Aruba enhance security for these new IP cameras in this environment?

A. Use MPSK Local to automatically provide unique pre-shared Keys for devices.
B. Aruba ClearPass performs the 802.1X authentication and installs a certificate.
C. MPSK provides for each device in the WLAN to have its own unique pre-shared Key.
D. MPSK Local will allow the cameras to share a rey and the scanners to share a different

Answer: C

Explanation:
The best option to enhance security for the new IP cameras and scanners in this environment is C. MPSK provides for each device in the WLAN to have its own unique pre- shared key.
MPSK stands for Multi Pre-Shared Key, and it is a feature that allows different devices to connect to the same SSID with different pre-shared keys. This improves the security and scalability of the network, as each device can have its own key and role without requiring 802.1X authentication or an external policy engine. MPSK can be configured either locally on the AP or centrally on Aruba Central12.
The other options are incorrect because:
? A. MPSK Local is a feature that allows the user to configure 24 PSKs per SSID locally on the device. These local PSKs would serve as an extension of the base MPSK functionality. However, MPSK Local is not suitable for this scenario, as it can only support up to 24 devices per SSID, while the client has 250 devices1.
? B. Aruba ClearPass is a network access control solution that can perform 802.1X authentication and install certificates for devices. However, this option is not feasible for this scenario, as the new IP cameras and scanners do not support 802.1X authentication3.
? D. MPSK Local will not allow the cameras to share a key and the scanners to share a different key. MPSK Local will assign a different key to each device, regardless of their type. Moreover, MPSK Local can only support up to 24 devices per SSID, while the client has 250 devices1.

NEW QUESTION 35
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 tor 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 36

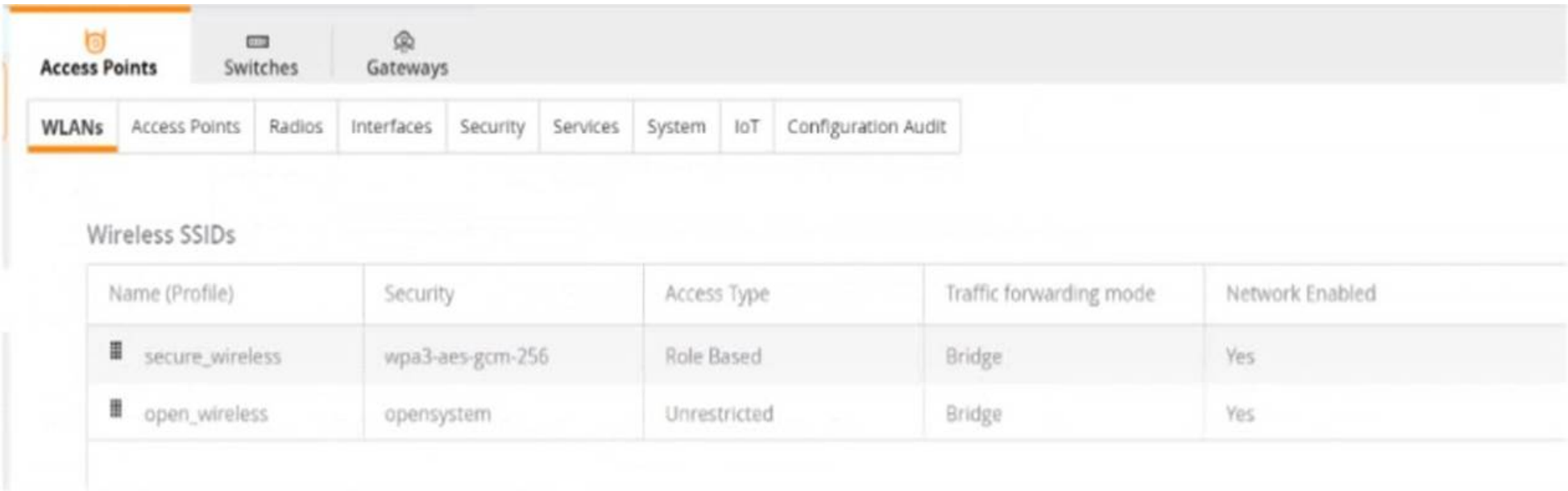
you need to have different routing-table requirements With Aruba CX 6300 VSF configuration.
Assuming the correct layer-2 VLAN already exists, how would you create a new SVI for a separate routing table?

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 38
Refer to the exhibit.



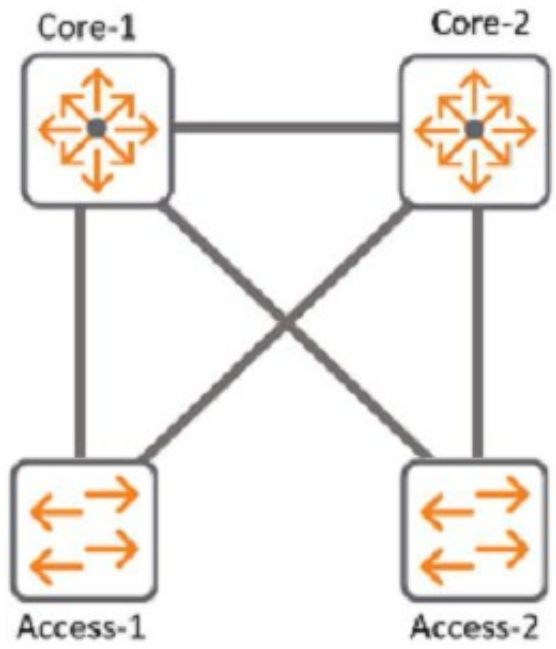
A company has deployed 200 AP-635 access points. To but is not working as expected What would be the correct action to fix the issue?

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 43
Refer to Exhibit:



With Access-1, What needs to be identically configured With MSTP to load-balance VLANS?

A. Spanning-tree bpdu-guard setting
B. Spanning-tree instance vlan mapppjng
C. spanning-tree Cist mapping
D. Spanning-tree root-guard setting

Answer: B

Explanation:
The correct answer is B. Spanning-tree instance VLAN mapping.
To load-balance VLANs with MSTP, you need to configure the same VLAN-to-instance mapping on all switches in the same MST region. This means that you need to assign different VLANs to different MST instances, and then adjust the spanning tree parameters (such as priority, cost, or port role) for each instance to achieve the desired load balancing. For example, you can make one switch the root for instance 1 and another switch the root for instance 2, and then map half of the VLANs to instance 1 and the other half to instance 2.
According to the Cisco document Understand the Multiple Spanning Tree Protocol (802.1s), one of the steps to configure MST is:
? Split your set of VLANs into more instances and configure different MST settings for each of these instances. In order to easily achieve this, elect Bridge D1 to be the root for VLANs 501 through 1000, and Bridge D2 to be the root for VLANs 1 through 500. These statements are true for this configuration:
Switch D1(config)#spanning-tree mst configuration Switch D1(config-mst)#instance 1 vlan 501-1000 Switch D1(config-mst)#exit
Switch D1(config)#spanning-tree mst 1 priority 0
Switch D2(config)#spanning-tree mst configuration Switch D2(config-mst)#instance 2 vlan 1-500 Switch D2(config-mst)#exit
Switch D2(config)#spanning-tree mst 2 priority 0
The above commands create two MST instances, 1 and 2, and map VLANs 501-1000 to instance 1 and VLANs 1-500 to instance 2. Then, they make switch D1 the root for instance 1 and switch D2 the root for instance 2.
The other options are incorrect because:
? A. Spanning-tree bpdu-guard setting is a security feature that disables a port if it receives a BPDU from an unauthorized device. It does not affect load balancing with MSTP.
? C. Spanning-tree CIST mapping is not a valid command. CIST stands for Common and Internal Spanning Tree, which is the spanning tree instance that runs within an MST region and interacts with other regions or non-MST switches.
? D. Spanning-tree root-guard setting is another security feature that prevents a port from becoming a root port if it receives superior BPDUs from another switch. It does not affect load balancing with MSTP.

NEW QUESTION 46
A customer is concerned about me unprotected traffic between an AOS-CX switch and a gateway, running on AOStO. What is a feasible option to protect this traffic?

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

Answer: A

Explanation:
According to the Aruba Documentation Portal1, PAPI (Port Aggregation Protocol) is a protocol that allows multiple physical ports to be aggregated into a single logical port for increased bandwidth and performance. PAPI can be used between AOS-CX switches and gateways, or between AOS-CX switches and other devices.
Option A: Implement an IPSec tunnel to protect PAPI between the AOS-CX switches and the gateway
This is because option A shows how to implement an IPSec tunnel between two devices using the interface command and the ipsec command. An IPSec tunnel can provide encryption and authentication for PAPI traffic between two devices, such as an AOS-CX switch and a gateway2.
Therefore, option A is a feasible option to protect this traffic.
I hope this helps you. If you need more information, please let me know. 1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7727/Content/Chp_prev_traf_loss/Act_gtw_act_fwd/act-gat-ove-vsx-10.htm 2: https://community.arubanetworks.com/blogviewer?blogkey=989fc43a-e0df-42db-9c0b- f96d6565a1fa

NEW QUESTION 47
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 52
With the Aruba CX switch configuration, what is the Active Gateway feature that is used for and is unique to VSX configuration?

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

Answer: A

Explanation:

Active gateway is a first hop redundancy protocol that eliminates a single point of failure. The active gateway feature is used to increase the availability of the default gateway servicing hosts on the same subnet. An active gateway improves the reliability and performance of the host network by enabling a virtual router to act as the default gateway for that network. If you have enabled active gateway, VRRP is not required3. Active gateway is similar to VRRP in that routed traffic from the VSX node is sourced from the switch interface MAC and not the virtual MAC address (VMAC). Each active gateway sends a periodic broadcast hello packet to avoid VMAC aging on the access switches. The switch views the active gateway IP as a self IP address3. Active gateway is preferable over VRRP because with VRRP traffic is still pushed over the ISL link, resulting in latency in the network3. Therefore, VRRP and active gateway are mutually exclusive on a VLAN, and answer A is correct.
References: 1: Aruba Campus Access documents and learning resources 3: Active gateway over VSX - Aruba

NEW QUESTION 53
Your manufacturing client is having installers deploy seventy headless scanners and fifty IP cameras in their warehouse These new devices do not support 802 1X authentication.
How can HPE Aruba reduce the IT administration overhead associated with this deployment while maintaining a secure environment using MPSK?

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

Answer: C

Explanation:
MPSK Local is a feature that can reduce the IT administration overhead associated with deploying devices that do not support 802.1X authentication while maintaining a secure environment. MPSK Local allows the switch to automatically generate and assign unique pre-shared keys for devices based on their MAC addresses, without requiring any configuration on the devices or an external authentication server. The other options are incorrect because they either require manual intervention by the installers or the MPSK gateway, or they do not provide unique pre-shared keys for devices. References:
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01- ch05.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch06.html

NEW QUESTION 56
You must ensure the HPEAruba 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 59
What are two advantages of splitting a larger OSPF area into a number of smaller areas? (Select two)

A. It extends the LSDB
B. It increases stability
C. it simplifies the configuration.
D. It reduces processing overhead.
E. It reduces the total number of LSAs

Answer: BD

Explanation:
Splitting a larger OSPF area into a number of smaller areas has several advantages for network scalability and performance. Some of these advantages are:
? It increases stability by limiting the impact of topology changes within an area.
When a link or router fails in an area, only routers within that area need to run the SPF algorithm and update their routing tables. Routers in other areas are not affected by the change and do not need to recalculate their routes.
? It reduces processing overhead by reducing the size and frequency of link-state advertisements (LSAs). LSAs are packets that contain information about the network topology and are flooded within an area. By dividing a network into smaller areas, each area has fewer LSAs to generate, store, and process, which saves CPU and memory resources on routers.
? It reduces bandwidth consumption by reducing the amount of routing information exchanged between areas. Routers that connect different areas, called area border routers (ABRs), summarize the routing information from one area into a single LSA and advertise it to another area. This reduces the number of LSAs that need to be transmitted across area boundaries and saves network bandwidth.
References: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first- ospf/7039-1.html https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first- ospf/13703-8.html

NEW QUESTION 60
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 rote 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 61
DRAG DROP
Match the terms below to their characteristics (Options may be used more than once or not at all.)

Term		Characteristic
Broadcast		A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address 10.13.4.2 in the other network
IP Directed Broadcast		One/more senders and one/more recipients participate in data transfer traffic
Multicast		Sent to all hosts on a remote network
Unicast		Sent to all NICs on the same network segment as the source NIC

A. Mastered
B. Not Mastered

Answer: A

Explanation:
a) A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address 10.13.4.2 in the other network -> Unicast
b) One/more senders and one/more recipients participate in data transfer traffic ->
Multicast
c) Sent to all hosts on a remote network -> IP Directed Broadcast
d) Sent to all NICs on the same network segment as the source NIC -> Broadcast
References: 1 https://www.thestudygenius.com/unicast-broadcast-multicast/
The terms broadcast, IP directed broadcast, multicast, and unicast are different types of communication or data transmission over a network. They differ in how many devices are involved in the communication and how they address the messages. The following table summarizes the characteristics of each term1:

Term	Definition	Example
Broadcast	One-to-all communication, where data is sent to every device on the network	A device with IP address 10.1.3.7 sends a DHCP request to 255.255.255.255
IP Directed Broadcast	One-to-all communication, where data is sent to all hosts on a remote network	A device with IP address 10.1.3.7 sends a ping request to 10.13.4.255
Multicast	One-to-many or many-to-many communication, where data is sent to a group of devices that have joined a multicast group	A device with IP address 10.1.3.7 sends a video stream to 239.0.0.1
Unicast	One-to-one communication, where data is sent to only one device	A device with IP address 10.1.3.7 sends an email to a device with IP address 10.13.4.2

NEW QUESTION 62
A customer wants to enable wired authentication across all their CX switches One of the requirements is that the switch must be able to authenticate a single computer connected through a VoIP phone.
Which feature should be enabled to support this requirement?

A. Multi-Domain Authentication
B. Device-Based Mode
C. MAC Authentication
D. Multi-Auth Mode

Answer: A

Explanation:
Multi-Domain Authentication is the feature that should be enabled to support the requirement that the switch must be able to authenticate a single computer connected through a VoIP phone. Multi-Domain Authentication is a feature that allows an Aruba CX switch to apply different authentication methods and policies to different devices connected to the same port. For example, a VoIP phone and a computer can be connected to the same port using a single cable, but they can be authenticated separately using different credentials and assigned to different VLANs. The other options are incorrect because they either do not support multiple devices on the same port or do not provide authentication.
References: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-7D9E9F6E-5C2A-4F7E-BE6D-A2C3A6C7B9F9.html
https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

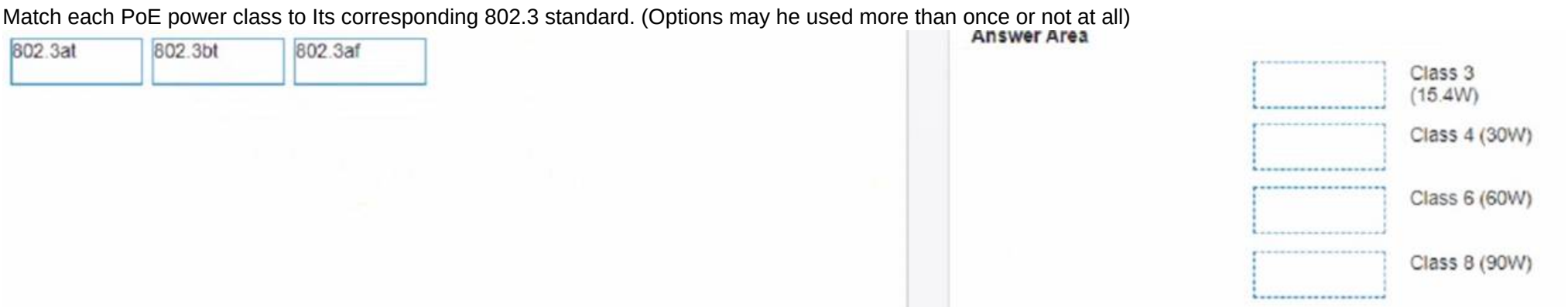
NEW QUESTION 63
Which component is used by the Aruba Network Analytics Engine (NAE)?

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
DRAG DROP
Match each PoE power class to Its corresponding 802.3 standard. (Options may he used more than once or not at all)



A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Class 3 (15.4W): 802.3af
? Class 4 (30W): 802.3at
? Class 6 (60W): 802.3bt
? Class 8 (90W): 802.3bt

NEW QUESTION 71
You are setting up a customer's 15 headless loT 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 72
You are troubleshooting an issue with a pair of Aruba CX 8360 switches configured with VSX Each switch has multiple VRFs. You need to find the IP address of a particular client device with a known MAC address You run the "show arp" command on the primary switch in the pair but do not find a matching entry for the client MAC address.
The client device is connected to an Aruba CX 6100 switch by VSX LAG. Which action can be used to find the IP address successfully?
A)

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

B)

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

C)

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

D)

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

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

Answer: B

Explanation:
The show arp command displays the ARP table for a specific VRF or all VRFs on the switch. The ARP table contains the IP address to MAC address mappings for hosts that are directly connected to the switch or reachable through a gateway. If the client device is connected to another switch by VSX LAG, the ARP entry for the client device will not be present on the primary switch unless it has communicated with it recently. Therefore, to find the IP address of the client device, the administrator should run the show arp command on the secondary switch in the VSX pair, specifying the VRF name that contains the client device??s subnet. References: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

NEW QUESTION 74
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 75
Which feature supported by SNMPv3 provides an advantage over SNMPv2c?

A. Transport mapping

B. Community strings
C. GetBulk
D. Encryption

Answer: D

Explanation:
Encryption is a feature supported by SNMPv3 that provides an advantage over SNMPv2c. Encryption protects the confidentiality and integrity of SNMP messages by encrypting them with a secret key. SNMPv2c does not support encryption and relies on community strings for authentication and authorization, which are transmitted in clear text and can be easily intercepted or spoofed. Transport mapping, community strings, and GetBulk are features that are common to both SNMPv2c and SNMPv3. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/snmp/snmp.htm https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmpv3.htm

NEW QUESTION 76
Due to a shipping error, five (5) Aruba AP-515S and one (1) Aruba CX 6300 were sent directly to your new branch office You have configured a new group persona for the new branch office devices in Central, but you do not know their MAC addresses or serial numbers The office manager is instructed via text message on their smartphone to onboard all the new hardware into Aruba Central
What application must the office manager use on their phone to complete this task?

A. Aruba Onboard App
B. Aruba Central App
C. Aruba CX Mobile App
D. Aruba installer App

Answer: D

Explanation:
Aruba Installer App is a mobile app that simplifies site installations and enables network connectivity for Aruba devices. The app allows the user to scan the barcode of the device and add it to the network using Aruba Central. The app also automates importing Aruba devices into Aruba NetEdit for intelligent configuration management and continuous conformance validation

NEW QUESTION 77
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

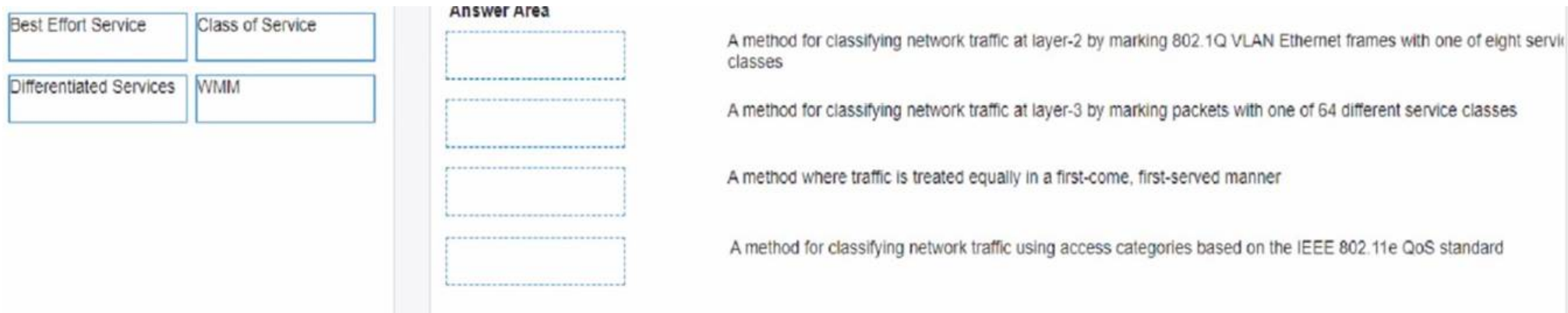
NEW QUESTION 78
How is Dynamic Multicast Optimization (DMO) implemented in an HPE Aruba wireless network?

A. DMO is configured individually tor each SSID in use in the network.
B. The AP uses OOS to provide equal air time for multicast traffic,
C. DMO is configured globally for each SSID in use in the network.
D. The controller converts multicast streams into unicast streams.

Answer: A

Explanation:
The correct answer is A. DMO is configured individually for each SSID in use in the network.
DMO is a feature that allows the AP to convert multicast streams into unicast streams over the wireless link. This enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. DMO is configured individually for each SSID in use in the network, as different SSIDs may have different multicast requirements.
According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure DMO is:
? Dynamic multicast optimization: Select Enabled to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients.
The other options are incorrect because:
? B. The AP does not use QoS to provide equal air time for multicast traffic. QoS is a feature that prioritizes different types of traffic based on their importance and latency sensitivity. QoS does not affect how multicast streams are transmitted over the wireless link.
? C. DMO is not configured globally for each SSID in use in the network. DMO is configured individually for each SSID, as different SSIDs may have different multicast requirements.
? D. The controller does not convert multicast streams into unicast streams. The AP does the conversion, as it is closer to the wireless clients and can optimize the transmission based on the client capabilities and channel conditions.

NEW QUESTION 81
DRAG DROP
Match the appropriate QoS concept with its definition. (Options may be used more than once or not at all.)



A. Mastered
B. Not Mastered

Answer: A

Explanation:
QoS concept: Class of Service Definition: 3) A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standards
QoS concept: Differentiated services Definition: 2) A method for classifying network traffic at layer-3 or marking packets with one of 64 different service classes
QoS concept: WMM Definition: 4) A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standards

NEW QUESTION 86
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

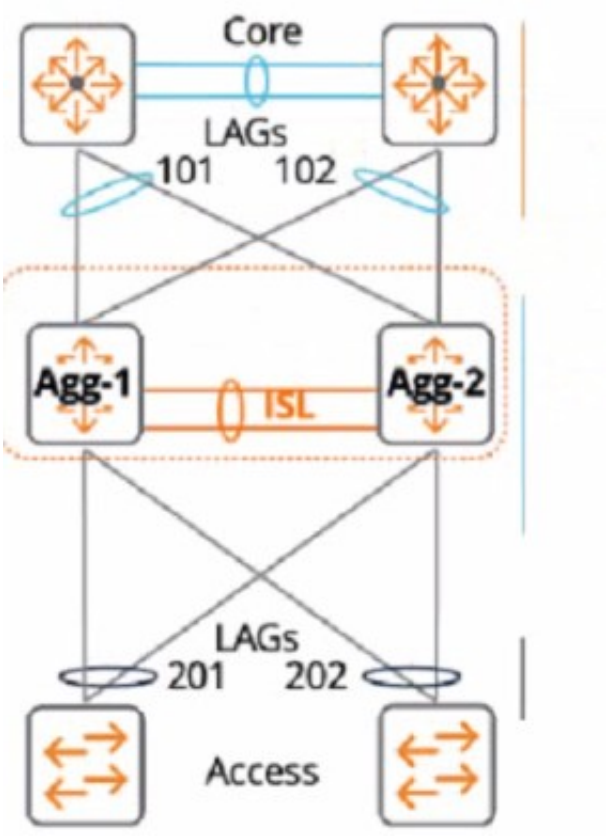
NEW QUESTION 89
What does the 802.3bz standard describe?

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 92
A customer just upgraded aggregation layer switches and noticed traffic dropping for 120 seconds after the aggregation layer came online again. What is the best way to avoid having this traffic dropped given the topology below?



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

Answer: C

Explanation:
The reason is that the linkup delay timer is a feature that delays bringing downstream VSX links up, following a VSX device reboot or an ISL flap. The linkup delay timer has two phases: initial synchronization phase and link-up delay phase.
The initial synchronization phase is the download phase where the rebooted node learns all the LACP+MAC+ARP+STP database entries from its VSX peer through ISLP. The initial synchronization timer, which is not configurable, is the required time to download the database information from the peer.
The link-up delay phase is the duration for installing the downloaded entries to the ASIC, establishing router adjacencies with core nodes and learning upstream routes. The link-up delay timer default value is 180 seconds. Depending on the network size, ARP/routing tables size, you might be required to set the timer to a higher value (maximum 600 seconds).
When both VSX devices reboot, the link-up delay timer is not used.
Therefore, by configuring the linkup delay timer to include LAGs 101 and 102, which are part of the same VSX device as LAG 201, you can ensure that both devices have enough time to synchronize their databases and form routing adjacencies before bringing down their downstream links.

NEW QUESTION 93
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 96
DRAG DROP
Select the Aruba stacking technology matching each option (Options may be used more than once or not at all.)

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 99
You are configuring an SVI on an Aruba CX switch that needs to have the following characteristics:
• VLANID = 25
. IPv4 address 10 105 43 1 with mask 255 255 255.0
• IPv6 address fd00:5708::f02d:4df6 with a 64 bit prefix length
• member of VRF eng
• VRF eng and VLAN 25 have not yet been created
Which command lists will satisfy the requirements with the least number of commands?
A)

```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43.1 255.255.255.0
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

B)

```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
```

C)

```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
```

D)

```
vrf eng
vlan 25
interface vlan 25
ip address 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

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

Answer: C

Explanation:
The other options either use more commands or do not create the VRF or the VLAN.
Option C uses the following commands:
? vrf eng: This command creates a VRF named eng and enters the VRF configuration mode1.
? vlan 25: This command creates a VLAN with ID 25 and enters the VLAN configuration mode2.
? interface vlan 25: This command creates an SVI on VLAN 25 and enters the interface configuration mode3.
? ip address 10.105.43.1/24 ipv6 address fd00:5780::102d:4df6/64 vrf attach eng: This command assigns an IPv4 address of 10.105.43.1 with a subnet mask of 255.255.255.0 and an IPv6 address of fd00:5780::102d:4df6 with a prefix length of 64 to the SVI, and attaches it to the VRF eng.

NEW QUESTION 100
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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