Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam

https://www.2passeasy.com/dumps/HPE7-A01/

NEW QUESTION 1

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

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

Answer: D

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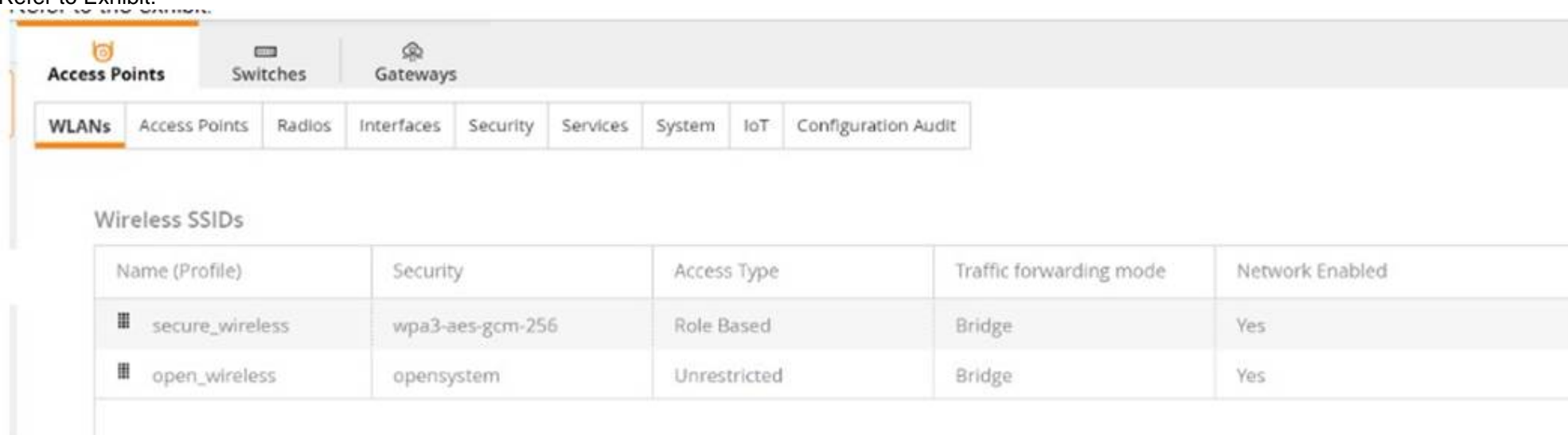? Active-active forwarding provides better performance. Unlike spanning tree, where some links are blocked to prevent loops, VSX switches use all available links for forwarding traffic, providing load balancing and increased bandwidth utilization.
? Multichassis LAG provides better redundancy. Unlike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

NEW QUESTION 2
Refer to Exhibit:

A company has deployed 200 AP-635 access points. To take advantage of the 6 GHz band, the administrator has attempted to configure a new WPA3-OWE SSID in Central but is not working as expected.
What would be the correct action to fix the issue?

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

Answer: C

Explanation:
 The correct action to fix the issue is C. Change the SSID to WPA3-Enhanced Open.
WPA3-OWE is not a valid SSID type in Central. OWE stands for Opportunistic Wireless Encryption, and it is a feature that provides encryption for open networks without requiring authentication. OWE is also known as Enhanced Open, and it is one of the options for WPA3 SSIDs in Central1.
According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure a WPA3 SSID is:
? Select the Security Level from the drop-down list. The following options are available:
The other options are incorrect because:
? A. WPA3-Enterprise (CNSA) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company??s use case.
? B. WPA3-Personal is a valid SSID type, but it requires a passphrase to join the network, which may not be suitable for the company??s use case.
? D. WPA3-Enterprise (CCM) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company??s use case.

NEW QUESTION 3
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 4
When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

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

Answer: D

Explanation:
The reason is that the Inter-Switch Link Protocol (ISLP) is a protocol that enables VSX stack join and synchronization between two VSX peer switches. ISLP uses a hello interval to exchange control messages between the switches.
The hello interval is a parameter that specifies the time interval between sending hello messages. The default value of the hello interval is 1 second. The hello interval can be configured from 1 second to 10 seconds. https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/index.html

NEW QUESTION 5
What is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches?

A. Switch authentication and local forwarding of the voice traffic
B. Switch authentication and user-based tunneling of the voice traffic.
C. Central authentication and port-based tunneling of the voice traffic.
D. Controller authentication and port-based tunneling of all traffic

Answer: A

Explanation:
This is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches. Dynamic segmentation is a feature that allows AOS-CX switches to tunnel user traffic to a controller or another switch based on user roles and policies. For voice traffic, it is recommended to use switch authentication and local forwarding, which means the voice devices are authenticated by the switch and their traffic is forwarded locally without tunneling. This reduces latency and jitter for voice traffic and improves voice quality. The other options are incorrect because they either use central authentication or tunneling, which are not optimal for voice traffic. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01- ch05.html
https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

NEW QUESTION 6
What is true regarding 802.11k?

A. It extends radio measurements to define mechanisms for wireless network management of stations
B. It reduces roaming delay by pre-authenticating clients with multiple target APs before a client roams to an AP
C. It provides mechanisms for APs and clients to dynamically measure the available radio resources.
D. It considers several metrics before it determines if a client should be steered to the 5GHz band, including client RSSI

Answer: C

Explanation:
802.11k is a standard that provides mechanisms for APs and clients to dynamically measure the available radio resources in a wireless network. 802.11k defines radio resource management (RRM) functions, such as neighbor reports, link measurement, beacon reports, etc., that allow APs and clients to exchange information about the RF environment and make better roaming decisions. The other options are incorrect because they describe other standards, such as 802.11r, 802.11v, or 802.11ax. References: https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

NEW QUESTION 7
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 8
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 9
How do you allow a new VLAN 100 between VSX pair inter-switch-link 256 for port 1/45 and 2/45?

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

Answer: C

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

NEW QUESTION 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 10
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 11
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 14
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
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 21
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
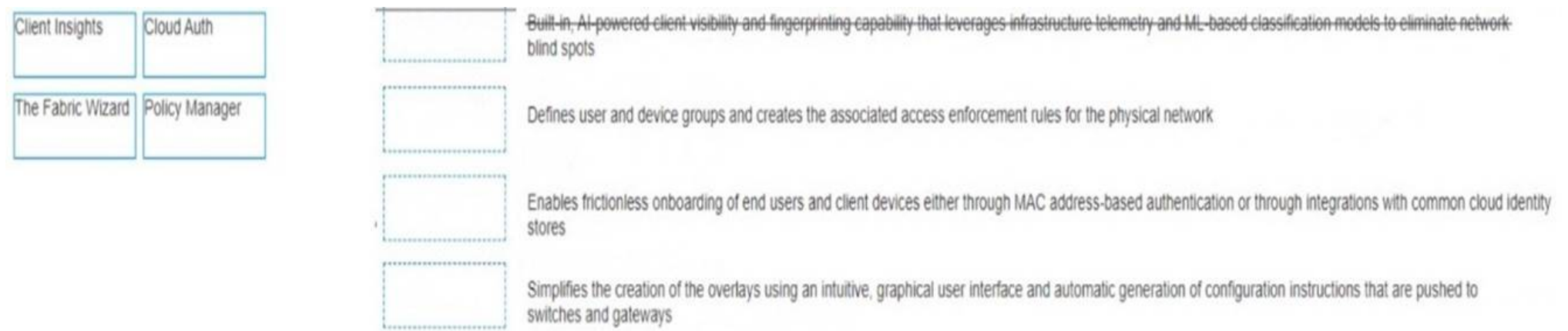B. 802.11mc
C. 802.11be
D. 802.11V

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 25
DRAG DROP
Match the solution components of NetConductor (Options may be used more than once or not at all.)

| Client Insights | Cloud Auth |
| The Fabric Wizard | Policy Manager |

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
 Client Insights matches with Built in , AI powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML based classification models to eliminate network bling spots
Client Insights is a solution component of NetConductor that provides built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML- based classification models to eliminate network blind spots. Client Insights uses machine learning to automatically detect, identify, and classify devices on the network, such as IoT devices, BYOD devices, or rogue devices. Client Insights also provides behavioral analytics and anomaly detection to monitor device performance and security posture. Client Insights helps network administrators gain visibility into the device landscape, enforce granular access policies, and troubleshoot issues faster. References: https://www.arubanetworks.com/products/network-management- operations/central/netconductor/
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf
Cloud Auth matches with Enables fictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores
Cloud Auth is a solution component of NetConductor that enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores. Cloud Auth is a cloud-native network access control (NAC) solution that is delivered via Aruba Central. Cloud Auth allows network administrators to define user and device groups, assign roles and policies, and enforce access control across wired and wireless networks. Cloud Auth supports MAC authentication for devices that do not support 802.1X, as well as integrations with cloud identity providers such as Azure AD, Google Workspace, Okta, etc. References: https://www.arubanetworks.com/products/network-management- operations/central/netconductor/
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf
The Fabric Wizard matches with Simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways
The Fabric Wizard is a solution component of NetConductor that simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways. The Fabric Wizard is a tool that allows network administrators to design, deploy, and manage overlay networks using VXLAN and EVPN protocols. The Fabric Wizard provides a graphical representation of the network topology, devices, and links, and allows users to drag and drop virtual components such as VRFs, VLANs, and subnets. The Fabric Wizard also generates the configuration commands for each device based on the user input and pushes them to the switches and gateways via Aruba Central. References:
https://www.arubanetworks.com/products/network-management- operations/central/netconductor/
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf
Policy Manager matches with Defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network
Policy Manager is a solution component of NetConductor that defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network. Policy Manager is a tool that allows network administrators to create and manage network policies based on user and device identities, roles, and contexts. Policy Manager uses Group Policy Identifier (GPID) to carry policy information in traffic for in-line enforcement. Policy Manager also integrates with Cloud Auth, ClearPass, or third-party solutions to provide flexible network access control. References:
https://www.arubanetworks.com/products/network-management- operations/central/netconductor/
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

NEW QUESTION 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 33
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 38
For an Aruba AOS10 AP in mixed mode, which factors can be used to determine the forwarding role assigned to a client? (Select two.)

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

Answer: AD

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

NEW QUESTION 39
You are working on a network where the customer has a dedicated router with redundant Internet connections Tor outbound high-importance real-time audio streams from their datacenter All of this traffic.
• originates from a single subnet
• uses a unique range of UDP ports
• is required to be routed to the dedicated router
All other traffic should route normally The SVI for the subnet containing the servers originating the traffic is located on the core routing switch in the datacenter
What should be configured?

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

Answer: C

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

NEW QUESTION 43
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 48
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 51
You are deploying Aruba CX 6300's with the customers requirement to only allow one (1) VoIP phone and one (1) device.

The following local role gets assigned to the phone port-access 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 53
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 57
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 62
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 64
Which statement best describes QoS?

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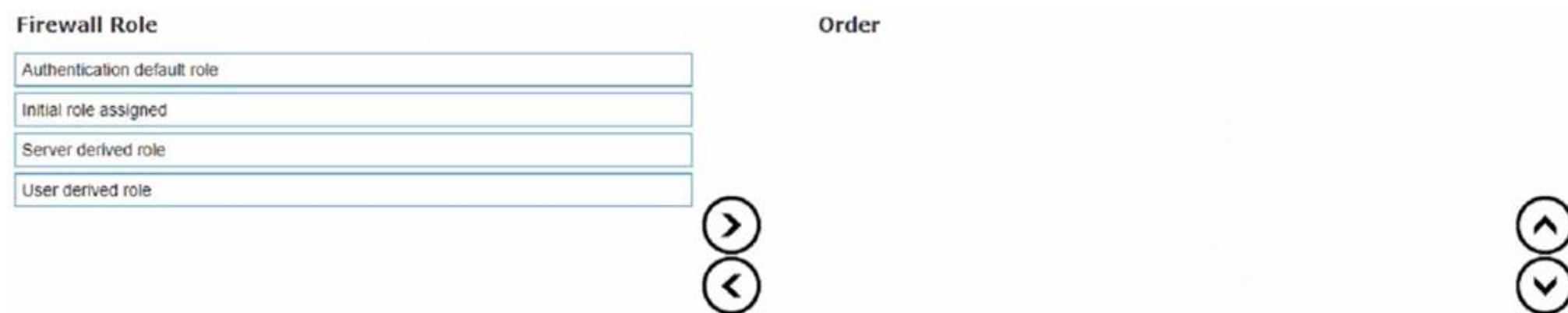
Answer: A

Explanation:
QoS stands for Quality of Service and is a mechanism that allows network devices to prioritize and differentiate traffic based on certain criteria, such as application type, source, destination, etc3. QoS involves identifying specific traffic for special treatment and applying policies and actions to improve its performance or meet certain service level agreements (SLAs)3. QoS can help network devices to manage congestion, delay, jitter, packet loss, bandwidth allocation, etc., for different types of traffic3. QoS can be implemented at various layers of the network stack and across different network domains. References: 3
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mt-book/qos-overview.html

NEW QUESTION 69
DRAG DROP
List the firewall role derivation flow in the correct order

Firewall Role	Order
Authentication default role	
Initial role assigned	
Server derived role	
User derived role	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
According to the Aruba Documentation Portal1, the firewall role derivation flow in the correct order is:
? Server derived role
? User derived role
? Authentication default role
? Initiation role assigned

NEW QUESTION 73
you are implementing ClearPass Policy Manager with EAP-TLS for authenticating all corporate-owned devices.
What are two possible solutions to the problem of deploying client certificates to corporate MacBooks that are joined to a Windows domain? (Select two.)

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

Answer: AB

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

NEW QUESTION 74
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 77
DRAG DROP
What is the order of operations tor Key Management service for a wireless client roaming from AP1 to AP2?

Operation	Order
Cache the client's information	
Client associates and authenticates to AP1	
Generate Pairwise Master Key keys for AP1's neighbors	
Get AP1 neighbor AP list	
Share Pairwise Master Key along with VLAN and User Role to target APs	

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 80
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 85
Two AOS-CX switches are configured with VSX at the the Access-Aggregation layer where servers attach to them An SVI interface is configured for VLAN 10 and serves as the default gateway for VLAN 10. The ISL link between the switches fails, but the keepalive interface functions. Active gateway has been configured on the VSX switches.
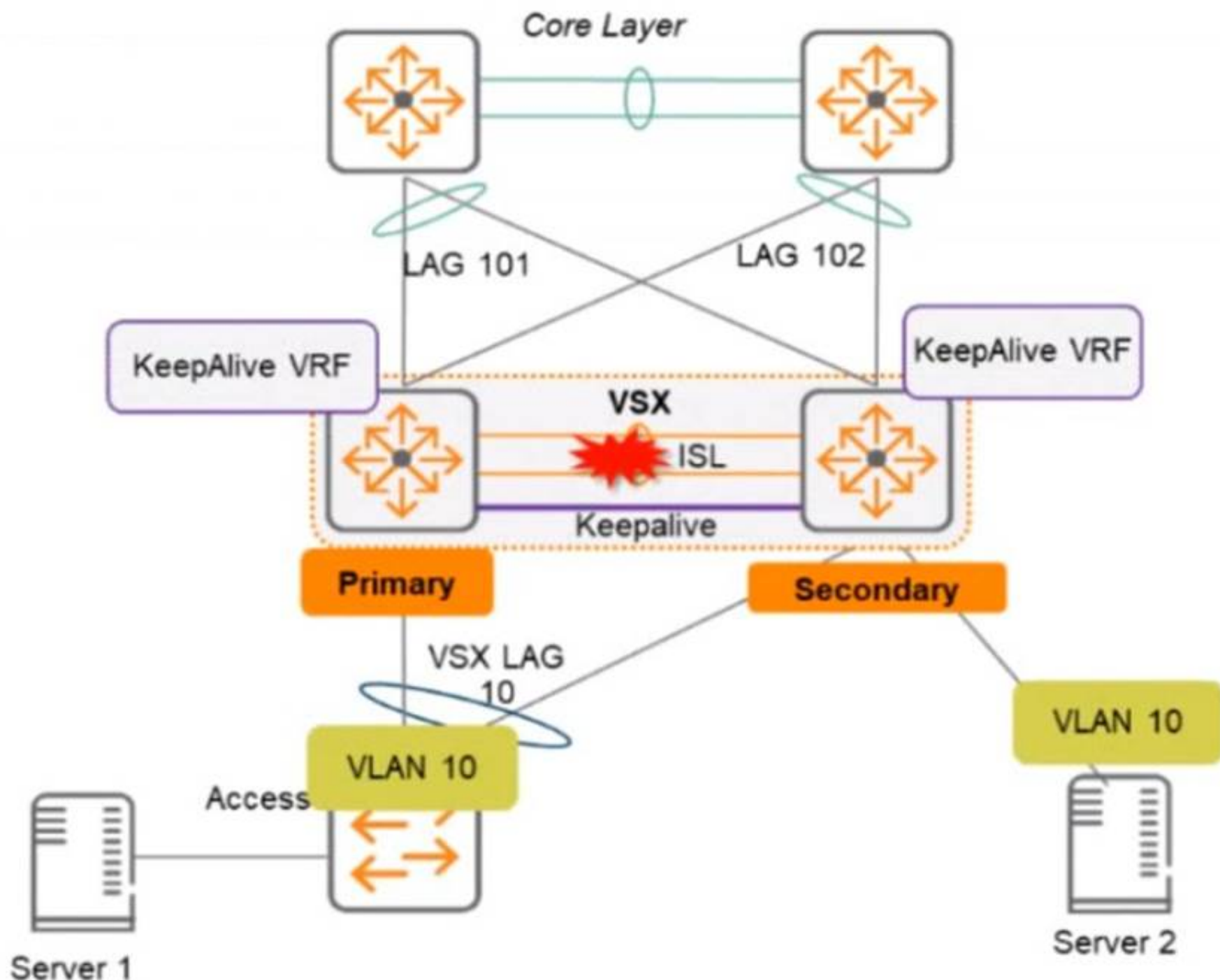
What is correct about access from the servers to the Core? (Select two.)

A. Server 1 can access the core layer via the keepalrve link
B. Server 2 can access the core layer via the keepalive link
C. Server 2 cannot access the core layer.
D. Server 1 can access the core layer via both uplinks
E. Server 1 and Server 2 can communicate with each other via the core layer
F. Server 1 can access the core layer on only one uplink

Answer: DE

Explanation:
 These are the correct statements about access from the servers to the Core when the ISL link between the switches fails, but the keepalive interface functions. Server 1 can access the core layer via both uplinks because it is connected to VSX-A, which is still active for VLAN 10. Server 2 can also access the core layer via its uplink to VSX-B, which is still active for VLAN 10 because of Active Gateway feature. Server 1 and Server 2 can communicate with each other via the core layer because they are in the same VLAN and subnet, and their traffic can be routed through the core switches. The other statements are incorrect because they either describe scenarios that are not possible or not relevant to the question. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-

NEW QUESTION 89
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 94
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 network12.
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 series2.
The other options are incorrect because:
? A. Sixteen different VMACs are not supported total as shared. They are supported for each IPv4 and IPv6 stack separately.
? B. Active gateway can be used without MSTP instances. MSTP is a protocol that allows multiple spanning tree instances to coexist on the same switch, but it does not affect how active gateway works.
? D. Active gateway does not copy traffic over the ISL link for an optimized path. It avoids using the ISL link for routed traffic and uses the local switch interface MAC instead of the virtual MAC address (VMAC) for source address1.

NEW QUESTION 96
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 99
Which statements regarding Aruba NAE agents are true? (Select two)

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

Answer: AC

Explanation:
The statements that are true regarding Aruba NAE agents are A and C.
* A. A single NAE script can be used by multiple NAE agents. This means that you can create different instances of the same script with different parameters or settings. For example, you can use the same script to monitor different VLANs or interfaces on the switch1.
* C. NAE agents will never consume more than 10% of switch processor resources. This is a built-in safeguard that prevents the agents from affecting the switch performance or stability. If an agent exceeds the 10% limit, it will be automatically disabled and an alert will be generated2.
The other options are incorrect because:
? B. NAE agents are not active at all times. They can be enabled or disabled by the user, either manually or based on a schedule. They can also be disabled automatically if they encounter an error or exceed the resource limit1.
? D. NAE scripts do not need to be reviewed and signed by Aruba before being used. You can create your own custom scripts using Python and upload them to the switch or Aruba Central. You can also use the scripts provided by Aruba or other sources, as long as they are compatible with the switch firmware version1.
? E. A single NAE agent cannot be used by multiple NAE scripts. An agent is an instance of a script that runs on the switch. Each agent can only run one script at a time1.

NEW QUESTION 100
A customer wants to deploy a Gateway and take advantage of all the SD-WAN features. Which persona role option should be selected?

A. ArubaOS 10 Branch
B. ArubaOS 10 VPN Concentrator
C. ArubaOS 10 Wireless
D. ArubaOS 10 Mobility

Answer: A

Explanation:
The persona role option that should be selected to deploy a Gateway and take advantage of all the SD-WAN features is A. ArubaOS 10 Branch.
ArubaOS 10 Branch is a persona that enables the Gateway to provide both LAN and WAN functionality for branch networks. The Gateway can act as a wireless controller, a router, a firewall, and an SD-WAN device. The SD-WAN features include route and tunnel orchestration, dynamic path steering, forward error correction, SaaS traffic optimization, SASE orchestration, and more1.
The other options are incorrect because:

? B. ArubaOS 10 VPN Concentrator: This is a persona that enables the Gateway to act as a VPN concentrator for remote access or site-to-site VPN connections. It does not provide SD-WAN features2.
? C. ArubaOS 10 Wireless: This is a persona that enables the Gateway to act as a wireless controller for campus networks. It does not provide SD-WAN features3.
? D. ArubaOS 10 Mobility: This is a persona that enables the Gateway to act as a mobility controller for campus networks. It does not provide SD-WAN features.

NEW QUESTION 102
A network administrator is attempting to troubleshoot a connectivity issue between a group of users and a particular server The administrator needs to examine the packets over a period of time from their desktop; however, the administrator is not directly connected to the AOS-CX switch involved with the traffic flow.
What statements are correct regarding the ERSPAN session that needs to be established on an AOS-CX switch'? (Select two)

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

Answer: BE

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

NEW QUESTION 105
A customer is looking Tor a wireless authentication solution for all of their loT devices that meet the following requirements
- The wireless traffic between the IoT devices and the Access Points must be encrypted
- Unique passphrase per device
- Use fingerprint information to perform role-based access
Which solutions will address the customer's requirements? (Select two.)

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

Answer: CD

Explanation:
 The correct answers are C and D.
MPSK (Multi Pre-Shared Key) is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices1. MPSK requires MAC authentication against a ClearPass Policy Manager server, which returns the encrypted passphrase for the device in a RADIUS VSA2. ClearPass Policy Manager is a platform that provides role-and device-based network access control for any user across any wired, wireless and VPN infrastructure3. ClearPass Policy Manager can also use device profiling and posture assessment to assign roles based on device fingerprint information4.
MPSK Local is a variant of MPSK that allows the user to configure up to 24 PSKs per SSID locally on the device, without requiring ClearPass Policy Manager5.
MPSK Local can be combined with EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), which is a secure authentication method that uses certificates to encrypt the wireless traffic between the IoT devices and the access points6. EAP-TLS can also use device certificates to perform role-based access control6.
Therefore, both ClearPass Policy Manager and MPSK Local with EAP-TLS can meet the customer??s requirements for wireless authentication, encryption, unique passphrase, and role-based access for their IoT devices.
MPSK and an internal RADIUS server is not a valid solution, because MPSK does not support internal RADIUS servers and requires ClearPass Policy Manager789. MPSK Local with MAC Authentication is not a valid solution, because MAC Authentication does not encrypt the wireless traffic or use fingerprint information for role-based access2. Local User Derivation Rules are not a valid solution, because they do not provide unique passphrase per device or use fingerprint information for role-based access101112.

NEW QUESTION 107
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 108
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 110
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual HPE7-A01 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the HPE7-A01 Product From:

https://www.2passeasy.com/dumps/HPE7-A01/

Money Back Guarantee

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