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

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

Answer: AD

Explanation:
The correct steps that are part of the Key Management workflow when a wireless device is roaming from AP1 to AP2 are A and D.
* A. AP1 will cache the client??s information and send it to the Key Management service. This is true because when a client associates and authenticates with AP1, AP1 will generate a pairwise master key (PMK) for the client and store it in its cache. AP1 will also send the PMK and other client information, such as MAC address, VLAN, and SSID, to the Key Management service, which is a centralized service that runs on Aruba Mobility Controllers (MCs) or Mobility Master (MM) devices1. The Key Management service will use this information to facilitate fast roaming for the client.
* D. The Key Management service then generates R1 keys for AP2??s neighbors. This is true because when the Key Management service receives the client information from AP1, it will use the PMK to derive R0 and R1 keys for the client. R0 keys are used to generate R1 keys, which are used to generate pairwise transient keys (PTKs) for encryption. The Key Management service will distribute the R1 keys to AP2 and its neighboring APs, which are determined by AirMatch based on RF proximity2. This way, when the client roams to AP2 or any of its neighbors, it can skip the 802.1X authentication and use the R1 key to quickly generate a PTK with the new AP3.
* B. The Key Management service receives from AirMatch a list of all AP2??s neighbors. This is false because the Key Management service does not receive this information from AirMatch directly. AirMatch is a feature that runs on MCs or MM devices and optimizes the RF performance of Aruba devices by using machine learning algorithms. AirMatch periodically sends neighbor reports to all APs, which contain information about their nearby APs based on signal strength and interference. The APs then send these reports to the Key Management service, which uses them to determine which APs should receive R1 keys for a given client2.
* C. The Key Management service receives a list of all AP1 s neighbors from AirMatch. This is false for the same reason as B. The Key Management service does not receive this information from AirMatch directly, but from the APs that send their neighbor reports.
* E. A client associates and authenticates with the AP2 after roaming from AP1. This is false because a client does not need to authenticate with AP2 after roaming from AP1 if it has already authenticated with AP1 and received R1 keys from the Key Management service. The client only needs to associate with AP2 and perform a four-way handshake using the R1 key to generate a PTK for encryption3. This is called fast roaming or 802.11r roaming, and it reduces the latency and disruption caused by full authentication.
1: ArubaOS 8.7 User Guide 2: ArubaOS 8.7 User Guide 3: ArubaOS 8.7 User Guide : ArubaOS 8.7 User Guide

NEW QUESTION 3
You need to ensure that voice traffic sent through an ArubaOS-CX switch arrives with minimal latency What is the best scheduling technology to use for this task?

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

Answer: A

Explanation:
Strict queuing is the best scheduling technology to use for voice traffic on an AOS-CX switch. Scheduling is a mechanism that determines how packets are transmitted from different queues on an egress port. Strict queuing is a scheduling method that gives the highest priority queue absolute preference over all other queues, regardless of their size or utilization. Voice traffic should be assigned to the highest priority queue and scheduled with strict queuing to ensure minimal latency and jitter. The other options are incorrect because they are either not scheduling methods or not optimal for voice traffic. 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 4

A customer is using stacked Aruba CX 6200 and CX 6300 switches for access and a VSX pair of Aruba CX 8325 as a collapsed core 802 1X is implemented for authentication. Due to the lack of cabling, some unmanaged switches are still in use Sometimes devices behind these switches cause network outages The switch should send a warning to the helpdesk when the problem occurs You have been asked to implement an effective solution to the problem
What is the solution for this?

A. Configure spanning tree on the Aruba CX 8325 switches Set the trap-option
B. Configure loop protection on all edge ports of the Aruba CX 6200 and CX 6300 switches No trap option is needed
C. Configure loop protection on all edge ports of the Aruba CX 6200 and CX 6300 switches Set up the trap-option
D. Configure spanning tree on the Aruba CX 6200 and CX 6300 switches No trap option is needed

Answer: C

Explanation:
This is the correct solution to the problem of devices behind unmanaged switches causing network outages due to loops. Loop protection is a feature that allows an Aruba CX switch to detect and prevent loops by sending loop protection packets on each port, LAG, or VLAN on which loop protection is enabled. If a loop protection packet is received by the same switch that sent it, it indicates a loop exists and an action is taken based on the configuration. Loop protection should be configured on all edge ports of the Aruba CX 6200 and CX 6300 switches, which are the ports that connect to end devices or unmanaged switches. The trap-option should be set up to send a warning to the helpdesk when a loop is detected. The other options are incorrect because they either do not configure loop protection or do not set up the trap-option. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-99A8B276-0DA3-4458-AFD8-42BFECE29D4F5.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-8561-17DB0311ED8F.html

NEW QUESTION 5
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 6
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 7
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

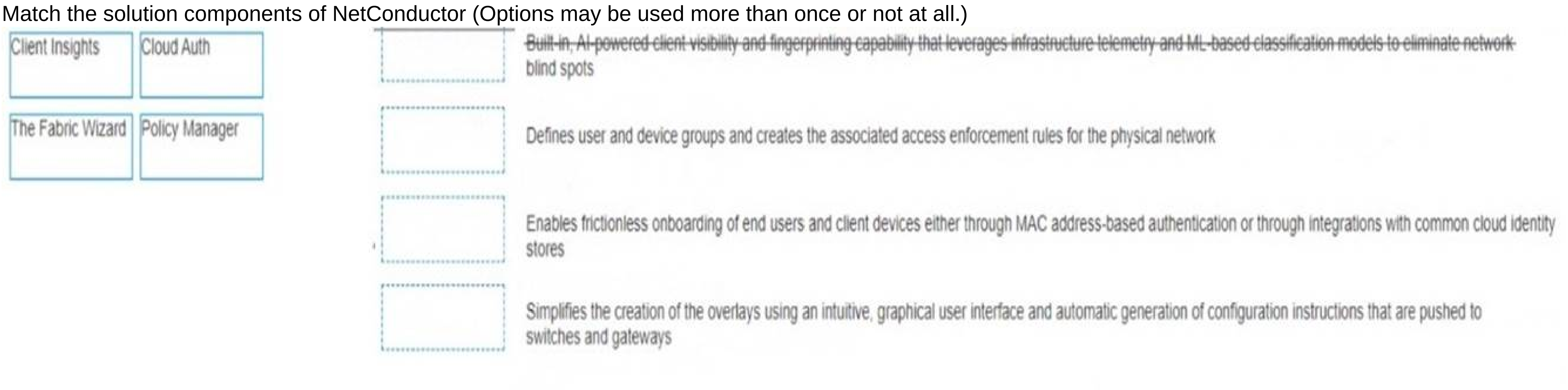
Explanation:
According to the Aruba Documentation Portal1, user-based tunneling (UBT) is a feature that uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. UBT enables a switch to provide a centralized security policy, using per- user authentication and access 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 8

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 9

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.

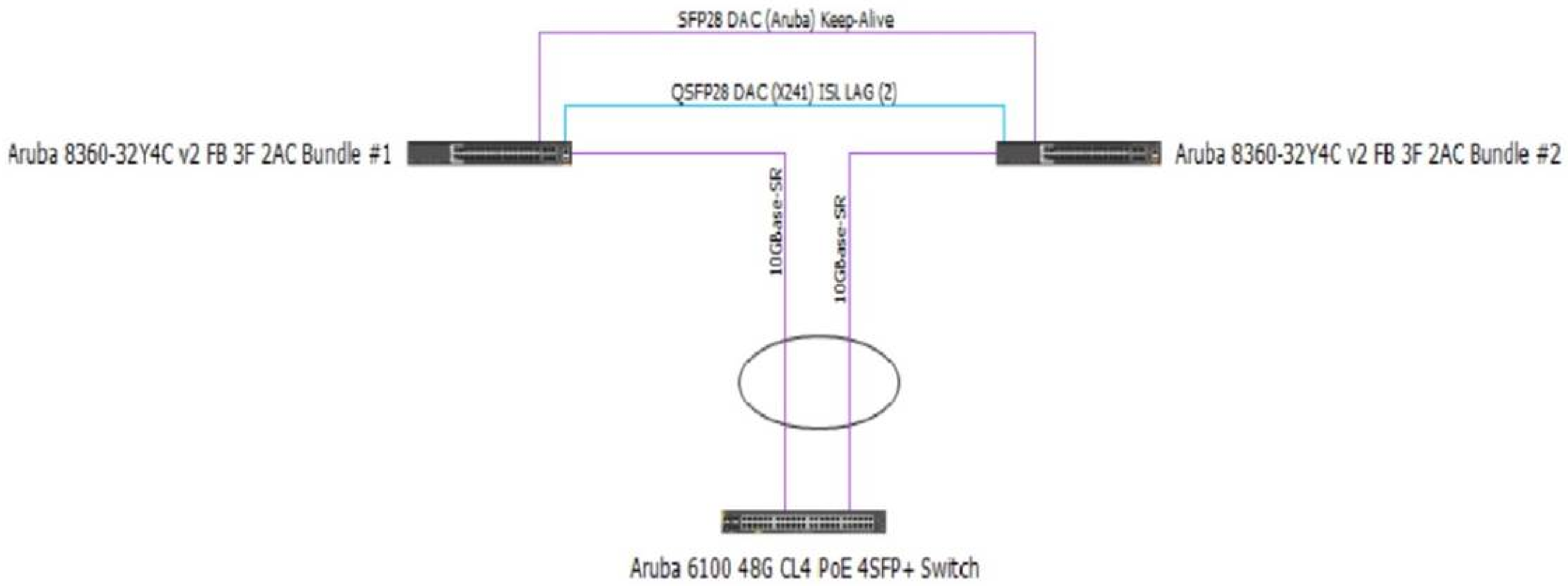
NEW QUESTION 10
What is a primary benefit of BSS coloring?

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

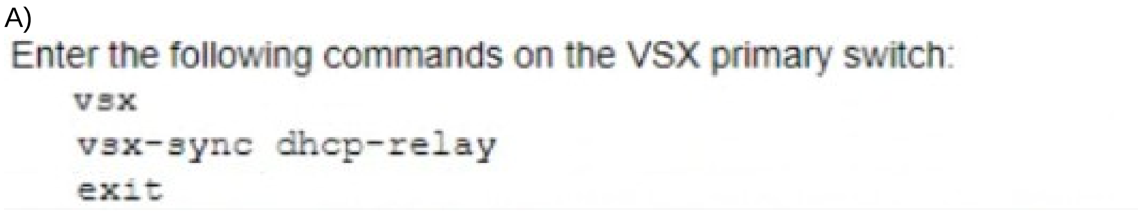
Answer: D

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 10
Review the exhibit.


SFP28 DAC (Aruba) Keep-Alive
QSFP28 DAC (X241) ISL LAG (2)
Aruba 8360-32Y4C v2 FB 3F 2AC Bundle #1
Aruba 8360-32Y4C v2 FB 3F 2AC Bundle #2
10GBase-SR
10GBase-SR
Aruba 6100 48G CL4 PoE 4SFP+ Switch

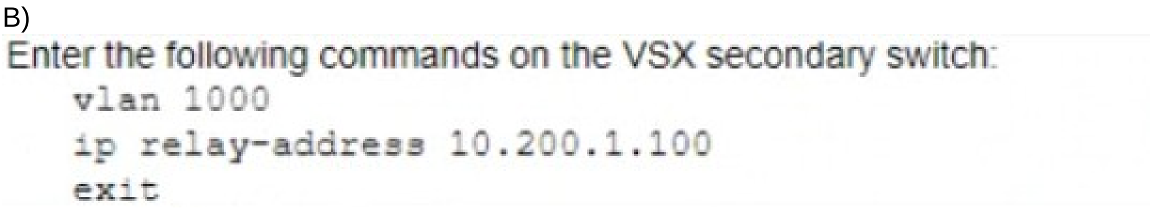
You are troubleshooting an issue with a 10 102.39 0/24 subnet which is also VLAN 1000 used Tor wireless clients on a pair of Aruba CX 8360 switches The subnet SVI is configured on the 8360 pair, and the DHCP server is a Microsoft Windows Server 2022 Standard with an IP address of 10 200 1.100. The 10.102.250.0/24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



Enter the following commands on the VSX primary switch:

```
    vsx
    vsx-sync dhcp-relay
    exit
```

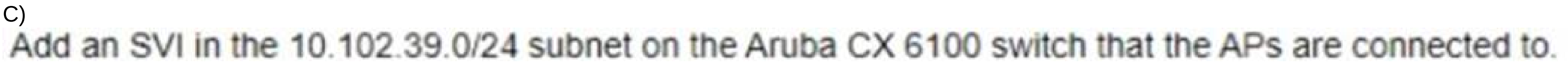
B)



Enter the following commands on the VSX secondary switch:

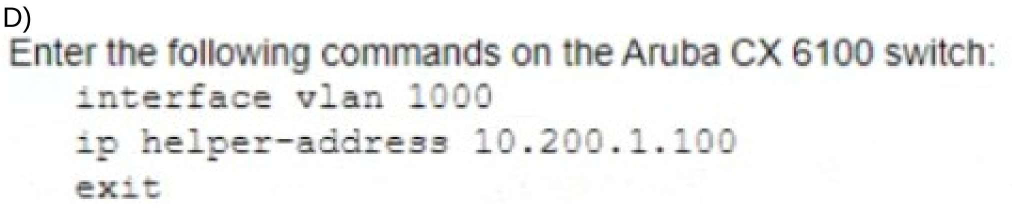
```
    vlan 1000
    ip relay-address 10.200.1.100
    exit
```

C)



Add an SVI in the 10.102.39.0/24 subnet on the Aruba CX 6100 switch that the APs are connected to.

D)



Enter the following commands on the Aruba CX 6100 switch:

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

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

Answer: C

Explanation:
Option C is the only action that configures the DHCP relay on the SVI of VLAN 1000 on the CX 8360 switches. DHCP relay is a feature that allows a switch to forward DHCP requests from clients in one subnet to a DHCP server in another subnet. DHCP relay is required when the DHCP server and the clients are not in the same broadcast domain1.
Option C uses the following commands:
? interface vlan 1000: This command enters the interface configuration mode for the SVI of VLAN 1000, which has an IP address of 10.102.39.1/24 and is used for wireless clients.
? ip helper-address vrf default 10.200.1.100: This command configures the IP address of the DHCP server as a helper address for the SVI, which means that the switch will forward DHCP requests from clients on VLAN 1000 to this address. The vrf default parameter indicates that the SVI and the DHCP server are in the same VRF.

NEW QUESTION 15
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 19
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 21
With the Aruba CX 6000 24G switch with uplinks of 1/1/25 and what does the switch do when a client port detects a loop and the do-not-disabie parameter is used?

A. Port status will be validated once status is cleared
B. An event log message is created.
C. The network analytics engine is triggered.
D. Port status led blinks in amber with 100hz.

Answer: B

Explanation:
The correct answer is B. An event log message is created.
The do-not-disable parameter is used to prevent the switch from disabling the port when a loop is detected by the loop-protect feature. Instead, the switch will generate an event log message that indicates the port number and the VLAN ID where the loop was detected. The switch will also send a trap to the SNMP manager, if configured1.
The other options are incorrect because:
? A. Port status will not be validated once status is cleared. The port will remain enabled even if a loop is detected, unless the loop-protect action is changed to tx-disable or tx-rx-disable1.
? C. The network analytics engine will not be triggered by a loop detection. The network analytics engine is a feature that allows users to monitor and troubleshoot network issues using scripts and agents2.
? D. Port status LED will not blink in amber with 100Hz. The port status LED will indicate the normal port status, such as link speed and activity, regardless of the loop detection3.

NEW QUESTION 24

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 26
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.

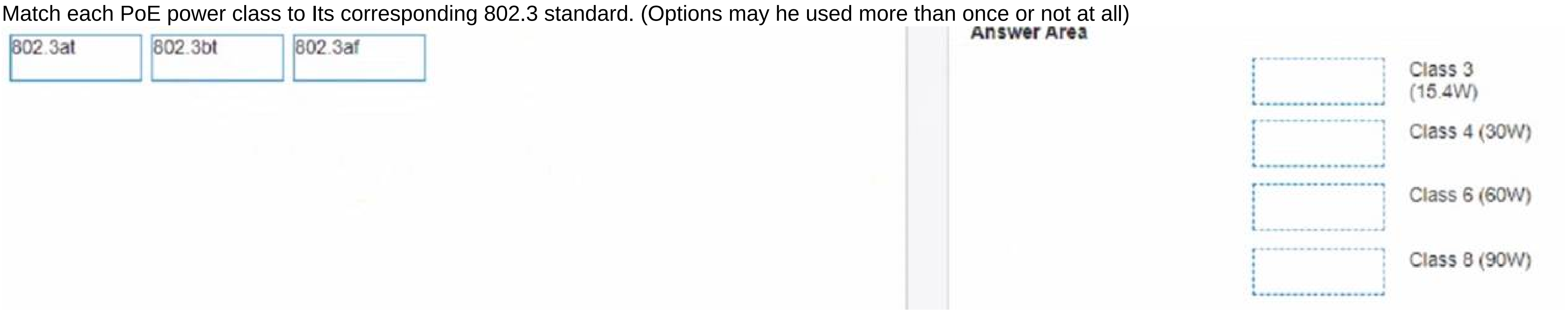
NEW QUESTION 27
What is enabled by LLDP-MED? (Select two.)

A. Voice VLANs can be automatically configured for VoIP phones
B. APs can request power as needed from PoE-enabled switch ports
C. iSCSl client devices can request to have flow control enabled
D. GVRP VLAN information can be used to dynamically add VLANs to a trunk
E. iSCSl client devices can set the required MTU setting for the port.

Answer: AB

Explanation:
These are two benefits enabled by LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery). LLDP-MED is an extension of LLDP that provides additional capabilities for network devices such as VoIP phones and APs. One of the capabilities is to automatically configure voice VLANs for VoIP phones, which allows them to be placed in a separate VLAN from data devices and receive QoS and security policies. Another capability is to request power as needed from PoE-enabled switch ports, which allows APs to adjust their power consumption and performance based on the available power budget. The other options are incorrect because they are either not enabled by LLDP-MED or not related to LLDP-MED. References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-qos/lldp-med.htm
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/poe.htm

NEW QUESTION 28
DRAG DROP
Match each PoE power class to Its corresponding 802.3 standard. (Options may he used more than once or not at all)

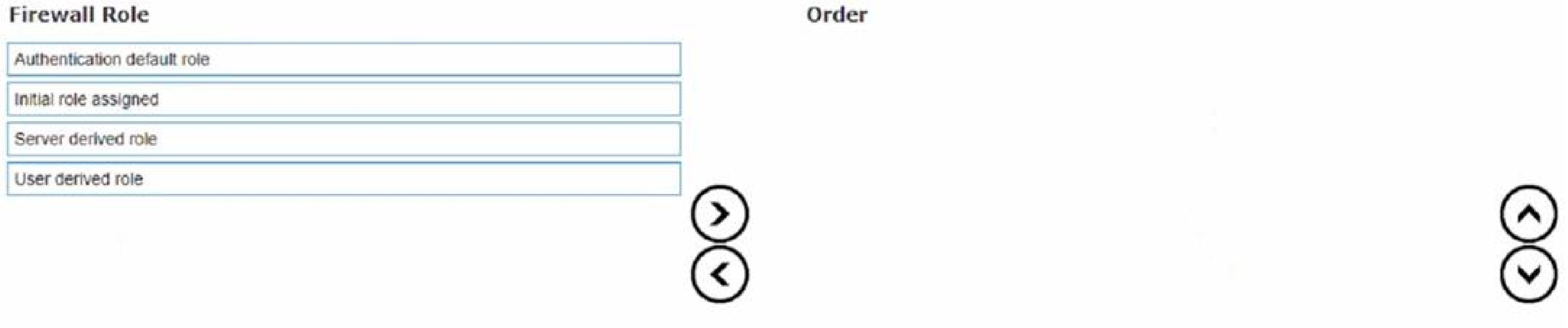


A. Mastered
B. Not Mastered

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 31
DRAG DROP
List the firewall role derivation flow in the correct order



Firewall Role

Authentication default role

Initial role assigned

Server derived role

User derived role

Order

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 36
your customer has asked you to assign a switch management role for a new user The customer requires the user role to View switch configuration information and have access to the PUT and POST meth0ds for REST API.
Which default AOS-CX user role meets these requirements?

A. administrators
B. auditors
C. sysops
D. helpdesk

Answer: C

Explanation:
The correct answer is C. sysops.
The sysops user role is a predefined role that allows users to view switch configuration information and have access to the PUT and POST methods for REST API. The sysops user role can also use the PATCH and DELETE methods for REST API, but not for all resources. The sysops user role is suitable for users who need to perform system operations on the switch, such as backup, restore, upgrade, or reboot.
According to the AOS-CX REST API Reference basics1, one of the predefined user roles is:
? sysops: Users with this role can view switch configuration information and have access to the PUT and POST methods for REST API. They can also use the PATCH and DELETE methods for REST API, but not for all resources. Users with this role can perform system operations on the switch, such as backup, restore, upgrade, or reboot.
The other options are incorrect because:
? A. administrators: Users with this role have full access to all switch configuration information and all REST API methods. This role is more than what the customer requires.
? B. auditors: Users with this role can only view switch configuration information and have access to the GET method for REST API. They cannot use the PUT and POST methods for REST API.
? D. helpdesk: Users with this role can view switch configuration information and have access to the GET method for REST API. They can also use the PATCH method for REST API, but only for a limited set of resources. They cannot use the PUT and POST methods for REST API.

NEW QUESTION 39
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 41
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 45
Which Aruba AP mode is sending captured RF data to Aruba Central for waterfall plot?

A. Hybrid Mode
B. Air Monitor
C. Spectrum Monitor
D. Dual Mode

Answer: C

Explanation:
Spectrum Monitor is an Aruba AP mode that is sending captured RF data to Aruba Central for waterfall plot. Spectrum Monitor is a mode that allows an AP to scan all channels in both 2.4 GHz and 5 GHz bands and collect information about the RF environment, such as interference sources, noise floor, channel utilization, etc. The AP then sends this data to Aruba Central, which is a cloud-based network management platform that can display the data in various formats, including waterfall plot. Waterfall plot is a graphical representation of the RF spectrum over time, showing the frequency, amplitude, and duration of RF signals.
The other options are incorrect because they are either not AP modes or not sending RF data to Aruba Central. References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/spectrum_monitor.htm
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/waterfall_plot.htm
https://www.arubanetworks.com/products/network-management-operations/aruba-central/

NEW QUESTION 48
......