

HP

Exam Questions HPE7-A01

Aruba Certified Campus Access Professional Exam



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

How is Multicast Transmission Optimization implemented in an HPE Aruba wireless network?

- A. "The optimal rate for sending multicast frames is based on the highest broadcast rate across all associated clients"
- B. When this option is enabled the minimum default rate for multicast traffic is set to 12 Mbps for 5 GHz
- C. The optimal rate for sending multicast frames is based on the lowest broadcast rate across all associated clients.
- D. The optimal rate for sending multicast frames is based on the lowest unicast rate across all associated clients.

Answer: D

Explanation:

multicast transmission optimization is a feature that allows the IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients¹. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5.0 GHz is 6 Mbps. This option is disabled by default¹.

NEW QUESTION 3

A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working across the campus which is connected via layer-3. The legacy devices are connected to Aruba CX 6300 switches throughout the campus. Which technology minimizes flooding so the legacy application can work efficiently?

- A. Generic Routing Encapsulation (GRE)
- B. EVPN-VXLAN
- C. Ethernet over IP (EoIP)
- D. Static VXLAN

Answer: B

Explanation:

EVPN-VXLAN is a technology that allows layer-2 communication across layer-3 networks by using Ethernet VPN (EVPN) as a control plane and Virtual Extensible LAN (VXLAN) as a data plane³. EVPN-VXLAN can be used to support legacy applications that communicate at layer-2 across different campuses or data centers that are connected via layer-3. EVPN-VXLAN minimizes flooding by using BGP to distribute MAC addresses and IP addresses of hosts across different VXLAN segments³. EVPN-VXLAN also provides benefits such as loop prevention, load balancing, mobility, and scalability³. References: 3

https://www.arubanetworks.com/assets/tg/TG_EVPN_VXLAN.pdf

NEW QUESTION 4

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 5

On AOS10 Gateways, which device persona is only available when configuring a Gateway-only group?

- A. Edge
- B. Mobility
- C. Branch
- D. VPN Concentrator

Answer: B

Explanation:

AOS 10 Gateways can have the following personas: Mobility, Branch, and VPN Concentrator¹ However, the Mobility persona is only available when configuring a Gateway-only group, which is a group that contains only one gateway device² The Mobility persona provides Overlay WLAN and (or) wired LAN functionalities for campus networks¹ The Branch persona provides the Aruba Instant OS and SD-Branch (LAN + WAN) functionality for branch and microbranch networks¹ The VPN Concentrator persona provides VPN termination and routing functionality for remote access networks³ The Edge persona is not a valid option, as it is not a supported device persona for AOS 10 Gateways.

NEW QUESTION 6

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

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

Answer: A

Explanation:

The Aruba CX 6400 switch is a modular switch that supports high- performance and high-density Ethernet switching for campus and data center networks. One of the features that distinguishes the Aruba CX 6400 switch from most typical campus switches is virtual output queueing (VOQ). VOQ is a technique that implements large ingress packet buffers on each port to prevent head-of-line blocking and packet loss due to congestion². VOQ allows each port to have multiple queues for different output ports and prioritize packets based on their destination and QoS class². VOQ enables the Aruba CX 6400 switch to achieve high throughput and low latency for various traffic types and scenarios. References: ² https://www.arubanetworks.com/assets/ds/DS_CX6400Series.pdf

NEW QUESTION 7

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

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

Answer: A

Explanation:

The standard that is supported by some Aruba APs and can enable a customer to accurately locate wireless client devices within a few meters is A. 802.11mc. * 802.11mc is an IEEE standard that enables computing devices to measure the distance to nearby Wi-Fi access points using a technique called Fine Timing Measurement (FTM). FTM uses precise timestamps to calculate the round-trip time of Wi-Fi frames between the device and the access point, and then converts it to a distance estimate. By using multiple access points and triangulation methods, the device can determine its location with high accuracy¹. According to the Aruba document 802.11mc Support, this feature is supported on 500 Series, 510 Series, 530 Series, 550 Series, 560 Series and 570 Series access points. These APs act as FTM responders to time measurement queries sent from a client. To configure the AP to send FTM responses, you need to enable the ftm-responder-enable parameter in the WLAN SSID profile¹.

NEW QUESTION 8

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 9

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

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

Answer: C

Explanation:

According to the Aruba Documentation Portal¹, 802.1X is a standard for port- based network access control that uses a RADIUS server to authenticate and authorize wireless clients. 802.1X can be configured in different modes, such as bridge mode, tunnel mode, or split tunnel mode.

Option C: GRE tunnel

This is because option C shows how to configure an SSID in tunnel mode with the default AP-group settings on an Aruba switch. In tunnel mode, all client traffic from the access points is tunneled back to the controller and the controller would in turn put the client traffic onto the network². The GRE protocol is used to encapsulate and decapsulate the traffic between the access points and the controller³.

Therefore, option C is correct.

1: <https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html> 2: <https://community.arubanetworks.com/discussion/bridge-and-tunnel-mode> 3: <https://www.twingate.com/blog/ipsec-tunnel-mode>

NEW QUESTION 10

A customer has a site with 200 AP-515 access points 75AP-565 access points installed.
The customer is rolling out new mobile phones with Wi-Fi-calling. 802.1X is in use for authentication
What should be enabled to ensure the best roaming experience?

- A. 802.1X
- B. 802. 11r
- C. 802.11W
- D. 802 .11h

Answer: A

Explanation:

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

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

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

NEW QUESTION 10

Which feature allows the device to remain operational when a remote link failure occurs between a Gateway cluster and a RADIUS server that is either in the cloud or a datacenter?

- A. MAC caching
- B. MAC Authentication
- C. Authentication survivability
- D. Opportunistic key caching

Answer: C

Explanation:

Authentication survivability is a feature that allows the device to remain operational when a remote link failure occurs between a Gateway cluster and a RADIUS server that is either in the cloud or a datacenter. Authentication survivability enables the Gateway cluster to cache successful authentication requests from the RADIUS server and use them to authenticate clients when the RADIUS server is unreachable. Authentication survivability also allows clients to use MAC caching or MAC authentication bypass (MAB) methods to access the network when the RADIUS server is down. References:

https://www.arubanetworks.com/assets/tg/TG_AuthSurvivability.pdf

NEW QUESTION 13

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. RPSVST+

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 18

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

- AP1 has a radio that generates a 16 dBm signal.
- AP2 has a radio that generates a 13 dBm signal.
- AP1 has an antenna with a gain of 8 dBi.
- AP2 has an antenna with a gain of 12 dBi. The antenna cable for AP1 has a 4 dB loss. The antenna cable for AP2 has a 3 dB loss.

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

- A. -9 dBm
- B. 20 dBm
- C. 40 dBm
- D. 15 dBm

Answer: B

Explanation:

The Equivalent Isotropic Radiated Power (EIRP) is the measured radiated power of an antenna in a specific direction. It is also called Equivalent Isotropic Radiated Power. It is the output power when a signal is concentrated into a smaller area by the Antenna. The EIRP can take into account the losses in transmission line, connectors and includes the gain of the antenna. It is represented in dB2. The formula for EIRP is:

$EIRP = P_{TLc} + G_a$ where PT is the output power of the transmitter in dBm, Lc is the cable and connector loss in dB, and Ga is the antenna gain in dBi.

For AP1, the EIRP can be calculated as: $EIRP = 16 + 8 = 20$ dBm

Therefore, the answer B is correct.

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

NEW QUESTION 22

Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements. After the configuration was complete, it was noted that a user assigned with the auditors role did not have the appropriate level of access on the switch.

The user was not allowed to perform firmware upgrades and a privilege level of 15 was not assigned to their role. Which default management role should have been assigned for the user?

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

Answer: B

Explanation:

The correct answer is B. sysops.

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

The other options are incorrect because:

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

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

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

NEW QUESTION 23

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

- AP1 has a radio that generates a 10 dBm signal
- AP2 has a radio that generates a 11 dBm signal
- AP1 has an antenna with a gain of 9 dBi
- AP2 has an antenna with a gain of 12 dBi.
- The antenna cable for AP1 has a 2 dB loss
- The antenna cable for AP2 has a 3 dB loss

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

- A. 26 dBm
- B. 30 dBm
- C. 17 dBm
- D. -12 dBm

Answer: C

Explanation:

The calculated Equivalent Isotropic Radiated Power (EIRP) for AP1 is 17 dBm.

EIRP is the measured radiated power of an antenna in a specific direction. It is equal to the input power to the antenna multiplied by the gain of the antenna. It can also take into account the losses in transmission line, connectors, and other components. The formula for EIRP is:

$EIRP = P + G - L$

where P is the output power of the radio, G is the gain of the antenna, and L is the loss of the cable and connectors.

For AP1, we have:

$P = 10$ dBm $G = 9$ dBi $L = 2$ dB

Therefore,
 $EIRP = 10 + 9 - 2 = 17 \text{ dBm}$

NEW QUESTION 26

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 29

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 32

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 36

DRAG DROP

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

Client Insights

The Fabric Wizard

Cloud Auth

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 37

DRAG DROP

Match the topics of an AOS10 Tunneled mode setup between an AP and a Gateway. (Options may be used more than once or not at all.)

Authenticator

Negotiate IPsec Phase1

Negotiate IPsec Phase 2

RADIUS proxy

Answer Area

Access Point

Access Point and Gateway

Device Designated Gateway

Overlay Tunnel Orchestrator

A. Mastered
B. Not Mastered

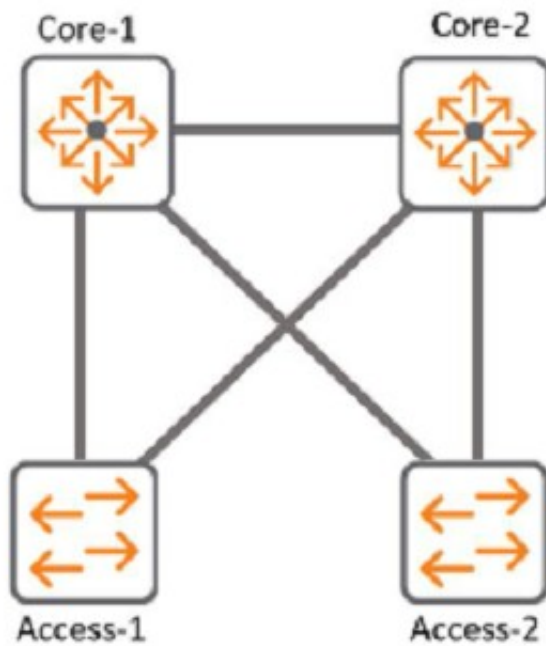
Answer: A

Explanation:



NEW QUESTION 41

Refer to Exhibit:



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

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

Answer: B

Explanation:

The correct answer is B. Spanning-tree instance VLAN mapping.

To load-balance VLANs with MSTP, you need to configure the same VLAN-to-instance mapping on all switches in the same MST region. This means that you need to assign different VLANs to different MST instances, and then adjust the spanning tree parameters (such as priority, cost, or port role) for each instance to achieve the desired load balancing. For example, you can make one switch the root for instance 1 and another switch the root for instance 2, and then map half of the VLANs to instance 1 and the other half to instance 2.

According to the Cisco document Understand the Multiple Spanning Tree Protocol (802.1s), one of the steps to configure MST is:

? Split your set of VLANs into more instances and configure different MST settings for each of these instances. In order to easily achieve this, elect Bridge D1 to be the root for VLANs 501 through 1000, and Bridge D2 to be the root for VLANs 1 through 500. These statements are true for this configuration:

Switch D1(config)#spanning-tree mst configuration Switch D1(config-mst)#instance 1 vlan 501-1000 Switch D1(config-mst)#exit

Switch D1(config)#spanning-tree mst 1 priority 0

Switch D2(config)#spanning-tree mst configuration Switch D2(config-mst)#instance 2 vlan 1-500 Switch D2(config-mst)#exit

Switch D2(config)#spanning-tree mst 2 priority 0

The above commands create two MST instances, 1 and 2, and map VLANs 501-1000 to instance 1 and VLANs 1-500 to instance 2. Then, they make switch D1 the root for instance 1 and switch D2 the root for instance 2.

The other options are incorrect because:

? A. Spanning-tree bpdu-guard setting is a security feature that disables a port if it receives a BPDU from an unauthorized device. It does not affect load balancing with MSTP.

? C. Spanning-tree CIST mapping is not a valid command. CIST stands for Common and Internal Spanning Tree, which is the spanning tree instance that runs within an MST region and interacts with other regions or non-MST switches.

? D. Spanning-tree root-guard setting is another security feature that prevents a port from becoming a root port if it receives superior BPDUs from another switch. It does not affect load balancing with MSTP.

NEW QUESTION 42

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

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

Answer: AC

Explanation:

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

NEW QUESTION 45

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 48

You are configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network Traffic originating from 10.2.250.0/24 should use a new default route to 10.1.1.253. Other non-default routes for this subnet should not be affected by this change.

What are two parts of the solution for these requirements? (Select two.)

A)

```
pbr-action-list def_route_test
default-nexthop 10.1.1.253/24
```

B)

```
class ip test_subnet
  10 match any 10.2.250.0/24 any
policy def_route_test_policy
  10 class ip test_subnet action pbr def_route_test
interface vlan 100
  ip address 10.2.250.0/24
  apply policy pbr_test routed in
```

C)

```
class ip test_subnet
  10 match any 10.2.250.0 255.255.255.0 any
policy def_route_test_policy
  10 class ip ip_test_subnet action pbr def_route_test
interface vlan 100
  ip address 10.2.250.0/24
  apply policy pbr_test routed out
```

D)

```
pbr-action-list def_route_test
default-nexthop 10.1.1.253
interface null
```

E)

```
pbr-action-list def_route_test
nexthop 10.1.1.253
interface null
```

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

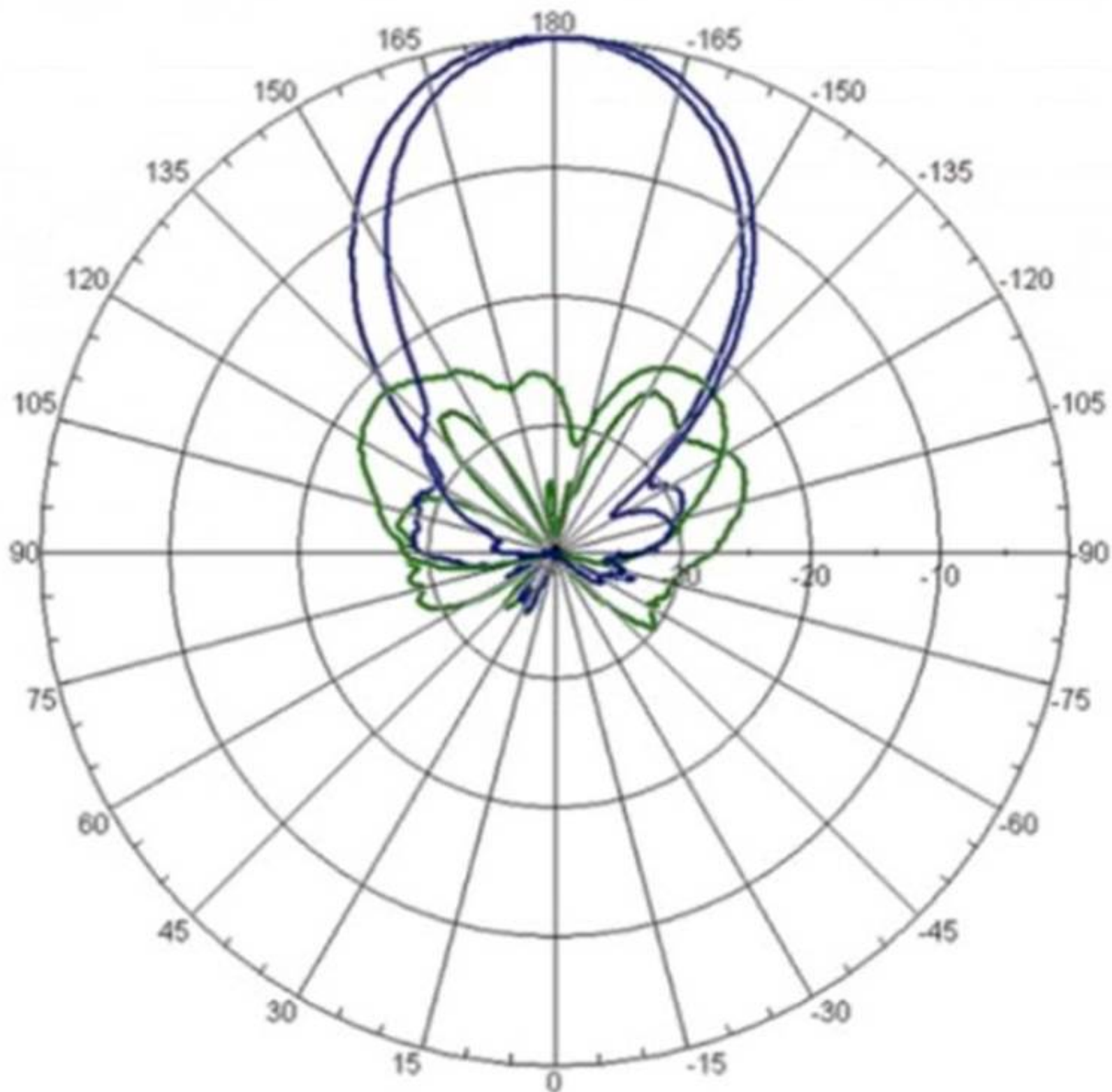
Answer: CE

Explanation:

Two parts of the solution for these requirements are Option C and Option E. Option C is a part of the solution because it defines a policy-based routing action list named route_test, which specifies the next hop IP address as 10.1.1.253 for the matching traffic. This is the new default route that the user wants to use for the subnet 10.2.250.0/24. The interface null parameter indicates that the traffic will be routed to the next hop without using a specific interface1. Option E is a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 250, which has an IP address of 10.2.250.1/24. This is the subnet that the user wants to test the new default route for. The apply policy command enables policy-based routing on the interface and associates it with the action list2. Option A is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify the next hop IP address as 10.1.1.253, which is the new default route that the user wants to use. Instead, it specifies a next hop IP address of 10.1.1.254, which is different from the requirement. Option B is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify any next hop IP address at all, which is necessary for policy-based routing to work. Instead, it specifies an interface null parameter without any IP address, which is invalid. Option D is not a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 200, which has an IP address of 10.2.200.1/24. This is not the subnet that the user wants to test the new default route for, but a different subnet that should not be affected by this change.

NEW QUESTION 49

Refer to the image.



Horizontal Pattern

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

- A. The AP is a remote access point.
- B. The AP is using a directional antenna.
- C. The AP is an outdoor access point.

D. The AP is configured in Mesh mode

Answer: B

Explanation:

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

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/antennas.htm

NEW QUESTION 54

Your customer is interested in hearing more about how roles can help keep consistent policy enforcement in a distributed overlay fabric How would you explain this concept to them"

- A. Group Based Policy ID is applied on egress VTEP after device authentication and policy is enforced on ingress VTEP
- B. Role-based policies are tied to IP addresses which have an advantage over IP-based policies and role names are sent between VTEPs
- C. Group Based Policy ID is applied on ingress VTEP after device authentication and policy is enforced on egress VTEP
- D. Role-based policies enhance User Based Tunneling across the campus network and the policy traffic is protected with iPsec

Answer: C

Explanation:

This is the correct explanation of how roles can help keep consistent policy enforcement in a distributed overlay fabric. Roles are used to assign group based policy IDs (GBPs) to devices after they authenticate with ClearPass or a local database. GBPs are then used to tag the traffic from the devices and send them to the ingress VTEP, which applies the GBP on the VXLAN header. The egress VTEP then enforces the policy based on the GBP and the destination device. The other options are incorrect because they either do not describe the correct sequence of events or do not use the correct terms. References:

<https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html>

NEW QUESTION 57

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-disable 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 61

Your manufacturing client is having installers deploy seventy headless scanners and fifty IP cameras in their warehouse These new devices do not support 802.1X authentication.

How can HPE Aruba reduce the IT administration overhead associated with this deployment while maintaining a secure environment using MPSK?

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

Answer: C

Explanation:

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

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch05.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch06.html

NEW QUESTION 63

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

- A. JSON-based scripts
- B. Lisp-based agents

- C. Ruby-based scripts
- D. Current State Database

Answer: A

Explanation:

The component that is used by the Aruba Network Analytics Engine (NAE) is D. Current State Database.

The Current State Database is a database that stores the configuration and state information of the switch, such as interfaces, VLANs, routing protocols, statistics, and more. The NAE can access this database through the AOS-CX REST API and monitor the values of any data point using monitors. The NAE can also track the history of the values in a time-series database and correlate them with network events or configuration changes¹. The Current State Database provides NAE with direct visibility into the entire current state of the device, which enables intelligent troubleshooting and automation of network tasks¹. The other options are incorrect because:

? A. JSON-based scripts: JSON is a data format that is used to exchange information between applications. It is not a scripting language that can be used by NAE. NAE scripts are written in Python, which is a popular and powerful programming language¹.

? B. Lisp-based agents: Lisp is a family of programming languages that are mainly used for artificial intelligence and functional programming. It is not a language that can be used by NAE. NAE agents are instances of scripts that run on the switch and collect relevant network information and trigger alerts or actions¹.

? C. Ruby-based scripts: Ruby is a general-purpose programming language that is known for its expressiveness and elegance. It is not a language that can be used by NAE. NAE scripts are written in Python, which is a popular and powerful programming language¹.

NEW QUESTION 66

Your customer has four (4) Aruba 7200 Series Gateways and two (2) 7000 Series Gateways. The customer wants to form a cluster with these Gateways. What design consideration would prevent you from using all of those Gateways?

- A. Multiple versions between Gateways in the same cluster profile are not allowed AOS 10.x.
- B. A heterogeneous cluster is not supported in AOS 10.x.
- C. The AP load should be lowest value of worst-case scenario load.
- D. A combination of 7200 series and 7000 series gateways supports up to 4 nodes

Answer: A

Explanation:

The reason is that AOS 10.x does not support clustering gateways with different versions in the same cluster profile. A cluster profile defines the configuration settings for a group of gateways that are managed by Aruba Central.

According to the Aruba documentation², ??You can combine 7200 Series and 7000 Series gateways in the same cluster with a maximum size of four devices with reduced AP client capacity on 7000 Series gateways.??

NEW QUESTION 71

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

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

Answer: AB

Explanation:

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

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-qos/lldp-med.htm

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/poe.htm

NEW QUESTION 76

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 81

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 84

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 86

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

Operation

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

Order

>

<

↑

↓

- 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 90

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 91

Your customer has asked you to assign a switch management role for a new user The customer requires the user role to only have Web UI access to the System > Log page and only have access to the GET method for REST API for the /logs/event resource Which default AOS-CX user role meets these requirements?

- A. administrators
- B. auditors
- C. sysops
- D. operators

Answer: A

Explanation:

The auditors role is the default AOS-CX user role that meets the requirements of having Web UI access to the System > Log page and having access to the GET method for REST API for the /logs/event resource. The auditors role has a level of 1 and allows read-only access to most commands except those related to security or passwords. It also allows access to the Web UI and REST API with limited permissions. The other options are incorrect because they either have higher levels of access or do not allow access to the Web UI or REST API. References: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch01.html> <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch04.html>

NEW QUESTION 95

DRAG DROP

List the WPA 4-Way Handshake functions in the correct order.

Function	Order
Distributes an encrypted GTK to the client	
Exchanges messages for generating PTK	
Proves knowledge of the PMK	
Sets first initialization vector (IV)	

>

<

⬆

⬇

- A. Mastered
- B. Not Mastered

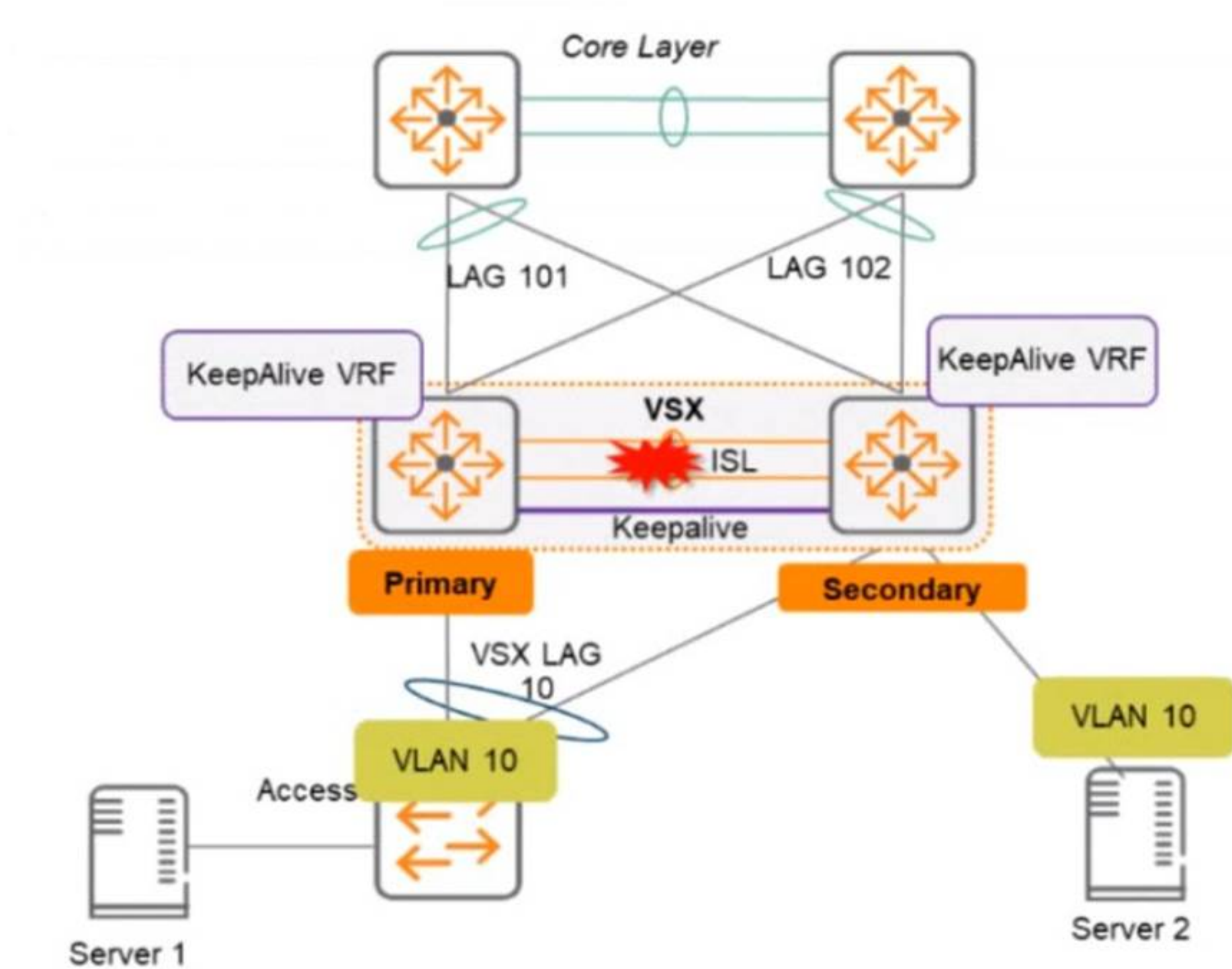
Answer: A

Explanation:

- ? Proves knowledge of the PMK
- ? Exchanges messages for generating PTK
- ? Distributes an encrypted GTK to the client
- ? Sets first initialization vector (IV)

NEW QUESTION 98

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 keepalive 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 100

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 104

Which feature supported by SNMPv3 provides an advantage over SNMPv2c?

- A. Transport mapping
- B. Community strings
- C. GetBulk
- D. Encryption

Answer: D

Explanation:

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

NEW QUESTION 109

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 114

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 methods 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 119

A network administrator is troubleshooting some issues guest users are having when connecting and authenticating to the network. The access switches are AOS-CX switches.

What command should the administrator use to examine information on which role the guest user has been assigned?

- A. show aaa authentication port-access interface all client-status
- B. show port-access captiveportal profile
- C. show port-access role
- D. diag-dump captiveportal client verbose

Answer: A

Explanation:

The show aaa authentication port-access interface all client-status command displays the status of all clients authenticated by port-based access control on all interfaces. The output includes the MAC address, user role, VLAN ID, and session timeout for each client. This command can be used to examine information on which role the guest user has been assigned by the AOS-CX switch. References: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

NEW QUESTION 121

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

- A. DMO is configured individually for 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 124

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 129

DRAG DROP

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

Best Effort Service	Class of Service	Answer Area 	A method for classifying network traffic at layer-2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Differentiated Services	WMM		A method for classifying network traffic at layer-3 by marking packets with one of 64 different service classes
			A method where traffic is treated equally in a first-come, first-served manner
			A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 131

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

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

Answer: BE

Explanation:

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

NEW QUESTION 134

With Aruba CX 6300, how do you configure IP address 10.10.10.1 for the interface in default state for interface 1/1/1?

- A. int 1/1/1. switching, ip address 10.10.10.1/24
 B. int 1/1/1. no switching, ip address 10.10.10.1/24
 C. int 1/1/1. ip address 10.10.10.1/24
 D. int 1/1/1. routing, ip address 10.10.10.1/24

Answer: B

Explanation:

To configure an IP address for an interface in default state for interface 1/1/1 on Aruba CX 6300 switch, you need to disable switching on the interface first with the command no switching. Then you can assign an IP address with the command ip address. The other options are incorrect because they either do not disable switching or use invalid keywords such as switching or routing. References: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch01.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html

NEW QUESTION 136

A customer is looking for a wireless authentication solution for all of their IoT devices that meet the following requirements

- The wireless traffic between the IoT devices and the Access Points must be encrypted
- Unique passphrase per device
- Use fingerprint information to perform role-based access

Which solutions will address the customer's requirements? (Select two.)

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

Answer: CD

Explanation:

The correct answers are C and D.

MPSK (Multi Pre-Shared Key) is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices¹. MPSK requires MAC authentication against a ClearPass Policy Manager server, which returns the encrypted passphrase for the device in a RADIUS VSA². ClearPass Policy Manager is a platform that provides role-and device-based network access control for any user across any wired, wireless and VPN infrastructure³. ClearPass Policy Manager can also use device profiling and posture assessment to assign roles based on device fingerprint information⁴.

MPSK Local is a variant of MPSK that allows the user to configure up to 24 PSKs per SSID locally on the device, without requiring ClearPass Policy Manager⁵. MPSK Local can be combined with EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), which is a secure authentication method that uses certificates to encrypt the wireless traffic between the IoT devices and the access points⁶. EAP-TLS can also use device certificates to perform role-based access control⁶.

Therefore, both ClearPass Policy Manager and MPSK Local with EAP-TLS can meet the customer's requirements for wireless authentication, encryption, unique passphrase, and role-based access for their IoT devices.

MPSK and an internal RADIUS server is not a valid solution, because MPSK does not support internal RADIUS servers and requires ClearPass Policy Manager⁷⁸⁹. MPSK Local with MAC Authentication is not a valid solution, because MAC Authentication does not encrypt the wireless traffic or use fingerprint information for role-based access². Local User Derivation Rules are not a valid solution, because they do not provide unique passphrase per device or use fingerprint information for role-based access¹⁰¹¹¹².

NEW QUESTION 138

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

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

Answer: AD

Explanation:

The correct answers are A and D.

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

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

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

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

NEW QUESTION 142

What is an OSPF transit network?

- A. a network that uses tunnels to connect two areas
- B. a special network that connects two different areas
- C. a network on which a router discovers at least one neighbor
- D. a network that connects to a different routing protocol

Answer: A

Explanation:

An OSPF transit network is a network that has at least two routers that are connected by a multi-access link and can forward traffic for other networks¹. A transit network is different from a stub network, which has only one router connected to it and does not forward traffic for other networks². A transit network is also different from a virtual link, which is a logical connection between two areas that are not physically adjacent². A transit network is not necessarily connected to a different routing protocol, although it can be if the router performs redistribution². Therefore, the correct answer is C. A network on which a router discovers at least one neighbor.

NEW QUESTION 147

Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements After the configuration was complete, it was noted that a user assigned with the administrators role did not have the appropriate level of access on the switch.

The user was not limited to viewing nonsensitive configuration information and a level of 1 was not assigned to their role Which default management role should have been assigned for the user?

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

Answer: B

Explanation:

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

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

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

NEW QUESTION 149

You are configuring an SVI on an Aruba CX switch that needs to have the following characteristics:

- VLANID = 25
- IPv4 address 10.105.43.1 with mask 255.255.255.0
- IPv6 address fd00:5708::f02d:4df6 with a 64 bit prefix length
- member of VRF eng
- VRF eng and VLAN 25 have not yet been created

Which command lists will satisfy the requirements with the least number of commands?

A)

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

B)

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

C)

```
interface vlan 25
vrf attach eng
ip address 10.105.43.1/24
ipov6 address fd00:5708::f02d:4df6/64
```

D)

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

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

Answer: C

Explanation:

The other options either use more commands or do not create the VRF or the VLAN.

Option C uses the following commands:

? vrf eng: This command creates a VRF named eng and enters the VRF configuration mode1.

? vlan 25: This command creates a VLAN with ID 25 and enters the VLAN configuration mode2.

? interface vlan 25: This command creates an SVI on VLAN 25 and enters the interface configuration mode3.

? ip address 10.105.43.1/24 ipv6 address fd00:5780::102d:4df6/64 vrf attach eng: This command assigns an IPv4 address of 10.105.43.1 with a subnet mask of 255.255.255.0 and an IPv6 address of fd00:5780::102d:4df6 with a prefix length of 64 to the SVI, and attaches it to the VRF eng.

NEW QUESTION 153

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

HPE7-A01 Practice Exam Features:

- * HPE7-A01 Questions and Answers Updated Frequently
- * HPE7-A01 Practice Questions Verified by Expert Senior Certified Staff
- * HPE7-A01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * HPE7-A01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The HPE7-A01 Practice Test Here](#)