HP.HPE7-A01.v2026-03-09.q130

Exam Code:	HPE7-A01
Exam Name:	Aruba Certified Campus Access Professional Exam
Certification Provider:	HP
Free Question Number:	130
Version:	v2026-03-09
# of views:	143
# of Questions views:	1300
https://www.exam-tests.com/HPE7-A01-exam/HP.HPE7-A01.v2026-03-09.q130.html	

NEW QUESTION: 1
A network administrator is attempting to troubleshoot a connectivity issue between a group of users and a particular server. The administrator needs to examine the packets over a period of time from their desktop; however, the administrator is not directly connected to the AOS-CX switch involved with the traffic flow.
What statements are correct regarding the ERSPAN session that needs to be established on an AOS-CX switch? (Select two)
A. On the source AOS-CX switch, the destination specified is the switch to which the administrator's desktop is connected
B. The encapsulation protocol used is GRE.
C. The encapsulation protocol used is VXLAN.
D. The encapsulation protocol is UDP.
E. On the source AOS-CX switch, the destination specified is the administrators desktop
Answer: B,E (LEAVE A REPLY)
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.

NEW QUESTION: 2

Due to a shipping error, five (5) Aruba AP-515S and one (1) Aruba CX 6300 were sent directly to your new branch office. You have configured a new group persona for the new branch office devices in Central, but you do not know their MAC addresses or serial numbers. The office manager is instructed via text message on their smartphone to onboard all the new hardware into Aruba Central.
What application must the office manager use on their phone to complete this task?
A. Aruba Onboard App
B. Aruba Central App
C. Aruba CX Mobile App
D. Aruba installer App
Answer: (SHOW ANSWER)
Aruba Central is a cloud-based networking solution that empowers IT with AI-powered insights, intuitive visualizations, workflow automation, and edge-to-cloud security to manage campus, branch, remote, data center, and IoT networks from one dashboard. Aruba Central also provides a mobile app that allows users to easily onboard and monitor devices. The app enables users to scan the barcode of a device (such as an AP or a switch) and add it to their network in Aruba Central. The app also lets users monitor the details of Aruba wireless access points and switches and their clients on their network. Therefore, the application that the office manager must use on their phone to complete the task of onboarding all the new hardware into Aruba Central is the Aruba Central App.

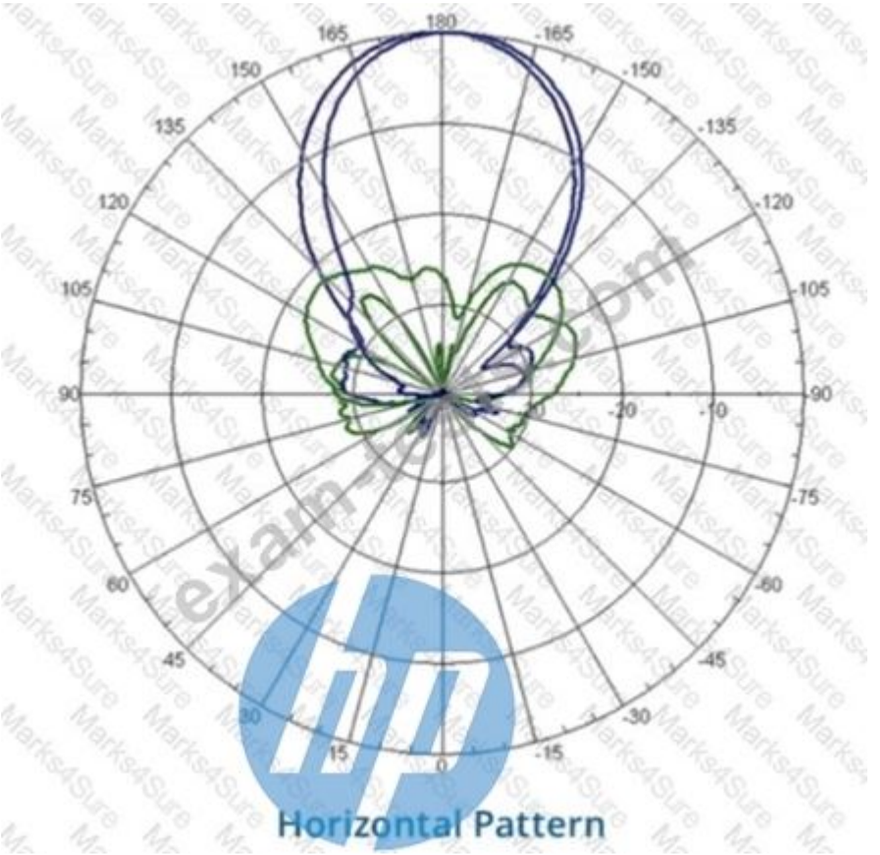
NEW QUESTION: 3
What does the 802.3bz standard describe?
A. 2.5Gb and 5Gb Ethernet ports
B. 60 W and 90W PoE
C. AP directed roaming between APs
D. 60 GHz P2P Wi-Fi
Answer: A (LEAVE A REPLY)
802.3bz is a standard for Ethernet over twisted pair at speeds of 2.5 and 5 Gbit/s. These use the same cabling as the ubiquitous Gigabit Ethernet, yet offer higher speeds. The resulting standards are named 2.5GBASE-T and 5GBASE-T.

NEW QUESTION: 4
A company recently upgraded its campus switching infrastructure with Aruba 6300 CX switches. They have implemented 802.1X authentication on edge ports where laptop and IoT devices typically connect.
An administrator has noticed that for PoE devices the pons are delivering the maximum wattage instead of what the device actually needs Upon connecting the IoT devices, the devices request their specific required wattage through information exchange
A. Concerned about this waste of electricity, what should the administrator implement to solve this problem?

B. Enable AAA authentication to exempt LLDP and/or CDP information
C. Globally enable the QoS trust setting for LLDP and/or CDP
D. Create device profiles with the correct power definitions.
E. implement a classifier policy with the correct power definitions.
Answer: D (LEAVE A REPLY)
According to the Aruba Documentation Portal1, the Aruba 6300 CX switches support various features to control the PoE devices on specific ports, such as device profiles and classifier policies. These features can help reduce the power consumption and improve the performance of the PoE devices.
1: https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fr
https://www.arubanetworks.com/products/switches/6300-series/ 3: https://docs.samsungknox.com/admin/knox-manage/configure/profile/configure-profile-policies/configure-profil

NEW QUESTION: 5
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 (LEAVE A REPLY)
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: 6
Refer to the image.



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 issue7

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 (LEAVE A REPLY)

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-fundam

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

NEW QUESTION: 7

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: (SHOW ANSWER)
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: 8
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: (SHOW ANSWER)
In AOS10, the VPN Concentrator persona is specifically available when configuring a Gateway-only group. This persona is designed for gateways that primarily handle VPN traffic, such as for remote users or branch offices, making it distinct from other personas like Edge, Mobility, or Branch.

NEW QUESTION: 9
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 (LEAVE A REPLY)
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: 10
Due to a shipping error, five (5) Aruba AP-515S and one (1) Aruba CX 6300 were sent directly to your new branch office You have configured a new group persona for the new branch office devices in Central, but you do not know their MAC addresses or serial numbers The office manager is instructed via text message on their smartphone to onboard all the new hardware into Aruba Central What application must the office manager use on their phone to complete this task?
A. Aruba Onboard App
B. Aruba Central App
C. Aruba CX Mobile App
D. Aruba installer App
Answer: (SHOW ANSWER)
Explanation
Aruba Installer App is a mobile app that simplifies site installations and enables network connectivity for Aruba devices. The app allows the user to scan the barcode of the device and add it to the network using Aruba Central. The app also automates importing Aruba devices into Aruba NetEdit for intelligent configuration management and continuous conformance validation

NEW QUESTION: 11
What does the 802.3bz standard describe?
A. 2.5Gb and 5Gb Ethernet ports
B. 60 W and 90W PoE
C. AP directed roaming between APs
D. 60 GHz P2P Wi-Fi
Answer: A (LEAVE A REPLY)

802.3bz is a standard for Ethernet over twisted pair at speeds of 2.5 and 5 Gbit/s. These use the same cabling as the ubiquitous Gigabit Ethernet, yet offer higher speeds. The resulting standards are named 2.5GBASE-T and 5GBASE-T.
Option A: 2.5Gb and 5Gb Ethernet ports
This is because option A shows how to identify the speed of an Ethernet port based on its name and the standard it supports. A port that supports 2.5GBASE-T or 5GBASE-T is a multi-gigabit port that can operate at speeds of up to 2.5 Gbit/s or 5 Gbit/s over twisted pair cables23. Therefore, option A is correct.
1: https://en.wikipedia.org/wiki/2.5GBASE-T_and_5GBASE-T 2: https://kb.netgear.com/000049004/What-is-Multi-Gigabit-Ethernet-and-how-can-I-benefit-from-using-NETGEA
https://arstechnica.com/gadgets/2016/09/5gbps-ethernet-standard-details-8023bz/

NEW QUESTION: 12
You are building a configuration in Central that will be used for a standardized network design for small sites for your company, you want to use GUI configuration for gateways and Aps, while template configuration for switches. You need to align with Aruba best practices.
Which set of actions will satisfy these requirements?
A. Create one group in Central for switches a second group for APs. and a third group for gateways Create a unique site for each location, and assign devices to the appropriate site.
B. Create one group in Central for switches and a second group for APs and gateways. Create a unique site for each location, and assign devices to the appropriate site.
C. Create a single group in Central. Create a unique site for each location, and assign devices to the appropriate site.
D. Create a single group in Central. Create a unique site for each type of device, and assign devices to the appropriate site.
Answer: C (LEAVE A REPLY)
Explanation
This is because option C shows how to create a single group in Central with different configuration methods defined for each device type. For example, you can create a group with the name Group1, and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (Group1). If a device type in the group is marked for template-based configuration method, the group name is prefixed with TG (TG Group1). You can use Group1 as the group ID for workflows such as user management, monitoring, reports, and audit trail2.
https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/abt-groups.htm 2: https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/groups.htm

NEW QUESTION: 13

You are deploying Aruba CX 6300's with the customers requirement to only allow one (1) VoIP phone and one (1) device.
The following local role gets assigned to the phone
port-access rote VoIP device-traffic-class voice
What set of commands best fits this requirement?
A. interface 1/1/1
aaa authentication port-access client-limit 2
aaa authentication port-access auth-mode client-mode
B. interface 1/1/1
aaa authentication port-access auth-mode multi-domain
C. interface 1/1/1
aaa authentication port-access client-limit multi-domain 2 aaa authentication port-access auth-mode multi-domain
D. interface 1/1/1
aaa authentication port-access client-limit 1 aaa authentication port-access auth-mode device-mode
Answer: C (LEAVE A REPLY)
Explanation
Aruba CX 6300 switches support various features to control the port access for different types of devices, such as client mode, device mode, and multidomain mode. These features can help limit the number of clients that can connect to a port and prevent unauthorized devices from accessing the network.
This is because option C shows how to configure the client limit and the auth-mode for a specific port using the interface command and the aaa authentication port-access command. The client limit specifies the maximum number of clients that can connect to a port. The auth-mode specifies the authentication mode for the port. In this case, option C sets both parameters to multi-domain mode, which allows only one voice device and one data device to be authenticated on a port
https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fr
https://www.arubanetworks.com/products/switches/6300-series/ 3:
https://www.arubanetworks.com/techdocs/AOS-CX/10.11/HTML/security_6200-6300-6400/Content/Chp_Port_

NEW QUESTION: 14
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 (LEAVE A REPLY)

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: 15
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: (SHOW ANSWER)
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. Reference: https://www.arubanetworks.com/assets/tg/TG_OWE.pdf

NEW QUESTION: 16
Which feature supported by SNMPv3 provides an advantage over SNMPv2c?
A. Transport mapping
B. Community strings
C. GetBulk
D. Encryption
Answer: D (LEAVE A REPLY)
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: 17
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: (SHOW ANSWER)
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 configured.

NEW QUESTION: 18
A customer wants to provide wired security as close to the source as possible The wired security must meet the following requirements:
- allow ping from the IT management VLAN to the user VLAN
- deny ping sourcing from the user VLAN to the IT management VLAN
The customer is using Aruba CX 6300s.
What is the correct way to implement these requirements?
A. Apply an outbound ACL on the user VLAN allowing temp echo-reply traffic toward the IT management VLAN
B. Apply an inbound ACL on the user VLAN allowing icmp echo-reply traffic toward the IT management VLAN
C. Apply an inbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN
D. Apply an outbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN
Answer: C (LEAVE A REPLY)
An inbound ACL is applied to traffic entering a port or VLAN. An outbound ACL is applied to traffic leaving a port or VLAN4. To deny ping sourcing from the user VLAN to the IT management

VLAN, an inbound ACL on the user VLAN should be used to filter icmp echo traffic toward the IT management VLAN. Icmp echo-reply traffic is not needed to be allowed because it is already permitted by default.

NEW QUESTION: 19
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 (LEAVE A REPLY)
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: 20
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: (SHOW ANSWER)

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-AF
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-85

NEW QUESTION: 21
When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?
A. QSVI
B. MAC tables
C. UDLD
D. RPVST+
Answer: (SHOW ANSWER)
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: 22
You are deploying Aruba CX 6300's with the customers requirement to only allow one (1) VoIP phone and one (1) device.

The following local role gets assigned to the phone port-access rote VoIP device-traffic-class voice What set of commands best fits this requirement?

A. interface 1/1/1
aaa authentication port-access client-limit 2
aaa authentication port-access auth-mode client-mode

B. interface 1/1/1
aaa authentication port-access auth-mode multi-domain

C. interface 1/1/1
aaa authentication port-access client-limit multi-domain 2
aaa authentication port-access auth-mode multi-domain

D. interface 1/1/1
aaa authentication port-access client-limit 1
aaa authentication port-access auth-mode device-mode

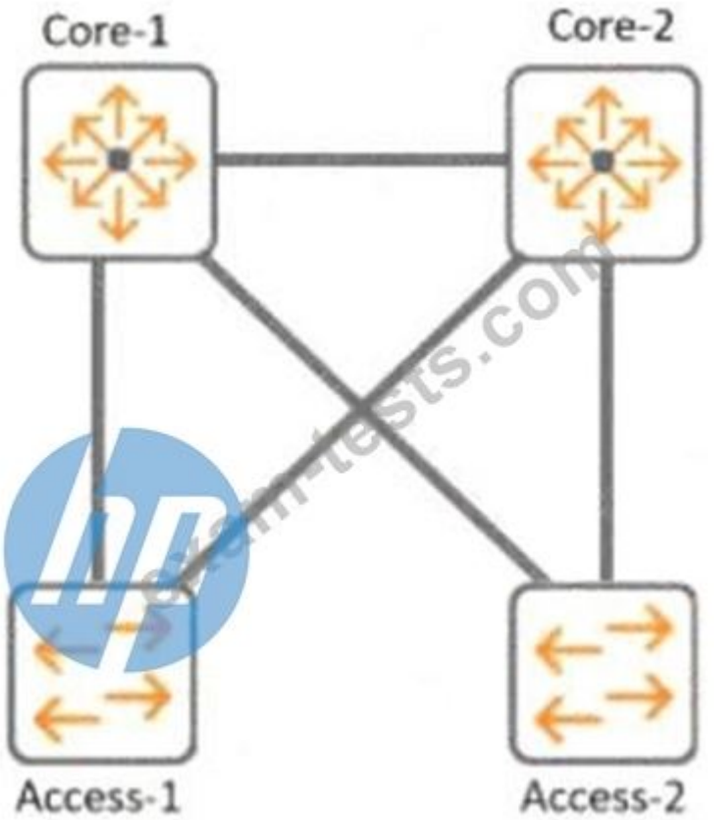
Answer: C (LEAVE A REPLY)

Aruba CX 6300 switches support various features to control the port access for different types of devices, such as client mode, device mode, and multidomain mode. These features can help limit the number of clients that can connect to a port and prevent unauthorized devices from accessing the network.

This is because option C shows how to configure the client limit and the auth-mode for a specific port using the interface command and the aaa authentication port-access command. The client limit specifies the maximum number of clients that can connect to a port. The auth-mode specifies the authentication mode for the port. In this case, option C sets both parameters to multi-domain mode, which allows only one voice device and one data device to be authenticated on a port.

NEW QUESTION: 23

Refer to the exhibit.



With Core-1. what is the default value for config-revision?

A. 0

B. 1

C. 1-0

D. 0. 0

Answer: A (LEAVE A REPLY)

The default value for config-revision on Core-1 is 0. Config-revision is a parameter that indicates the configuration version of a VSX pair. It is used to synchronize the configuration between the VSX peers and to detect any configuration mismatch. The config-revision value is set to 0 by default on both VSX peers and is incremented by 1 every time a configuration change is made on either peer. The other options are incorrect because they do not reflect the default value of config-revision. References: https://www.arubanetworks.com /techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html https://www.arubanetworks.com/techdocs/AOS- CX/10.04/HTML/5200-6728/bk01-ch02.html

NEW QUESTION: 24

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

A. SNMPv3

B. DSCP

C. TLV

D. CDP

Answer: A (LEAVE A REPLY)

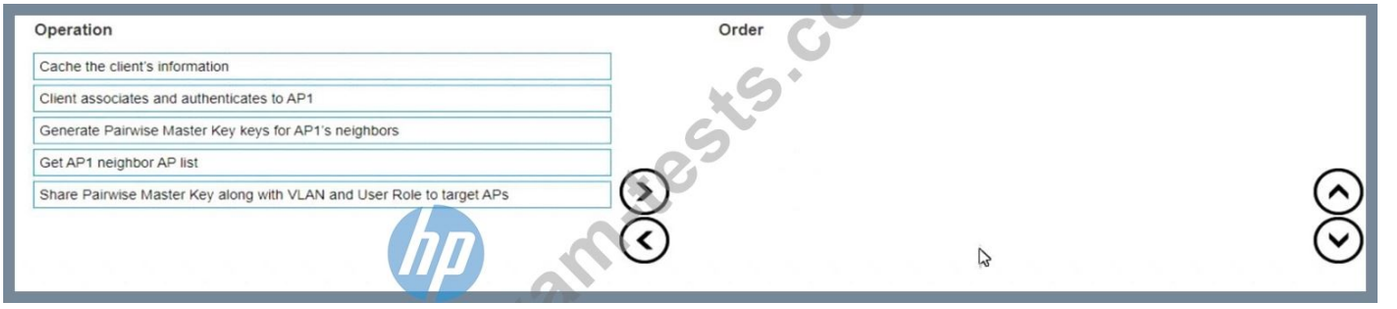
SNMPv3 is a protocol that is used to retrieve data stored in a Management Information Base (MIB), which is a database of managed objects in a network. SNMPv3 provides security and access control features that are not available in earlier versions of SNMP. SNMPv3 can also use encryption to protect the data from unauthorized access or modification.

NEW QUESTION: 25
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 (LEAVE A REPLY)
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

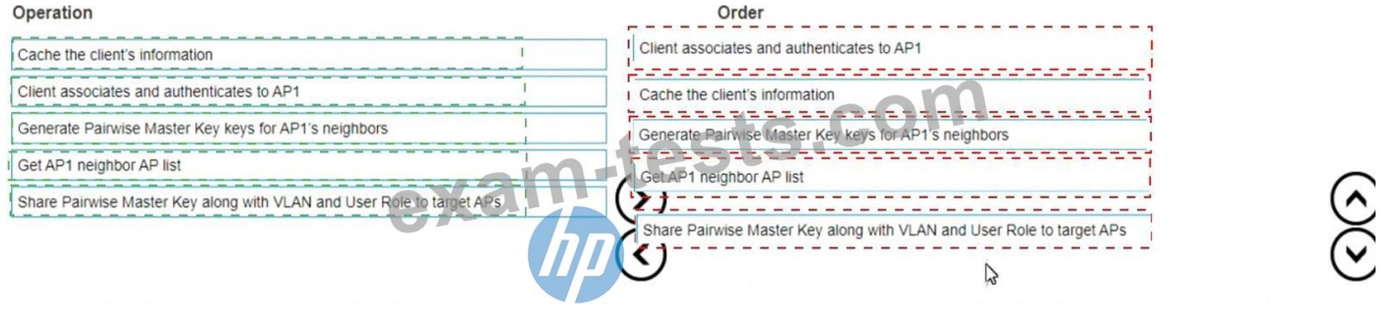
NEW QUESTION: 26
A new network design is being considered to minimize client latency in a high-density environment. The design needs to do this by eliminating contention overhead by dedicating subcamers to clients.
Which technology is the best match for this use case?
A. OFDMA
B. MU-MIMO
C. QWMM
D. Channel Bonding
Answer: (SHOW ANSWER)
Explanation
OFDMA (Orthogonal Frequency Division Multiple Access) is a technology that can minimize client latency in a high-density environment by eliminating contention overhead by dedicating subcarriers to clients. OFDMA allows multiple clients to transmit simultaneously on different subcarriers within the same channel, reducing contention and increasing efficiency. MU-MIMO (Multi-User Multiple Input Multiple Output) is a technology that allows multiple clients to transmit simultaneously on different spatial streams within the same channel, but it does not eliminate contention overhead. QWMM (Quality of Service Wireless Multimedia) is a technology that prioritizes traffic based on four access categories, but it does not eliminate contention overhead.

Channel Bonding is a technology that combines two adjacent channels into one wider channel, increasing bandwidth but not eliminating contention overhead. References:
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf
https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf

NEW QUESTION: 27
What is the order of operations tor Key Management service for a wireless client roaming from AP1 to AP2?



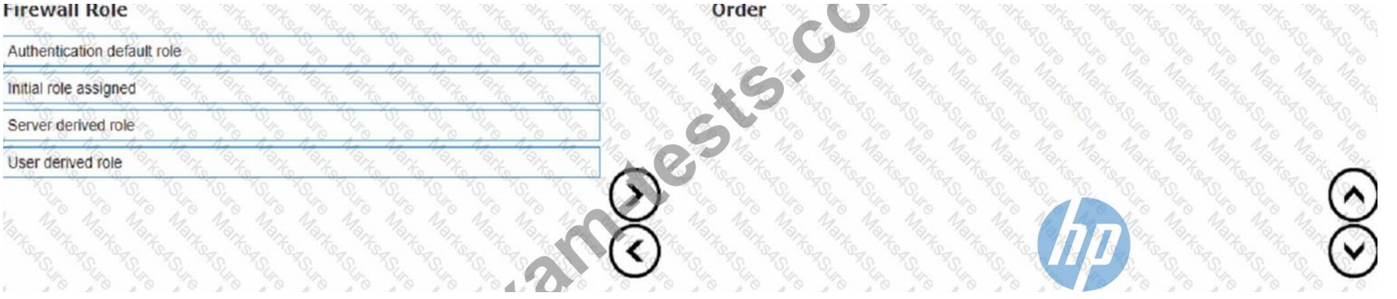
Answer:



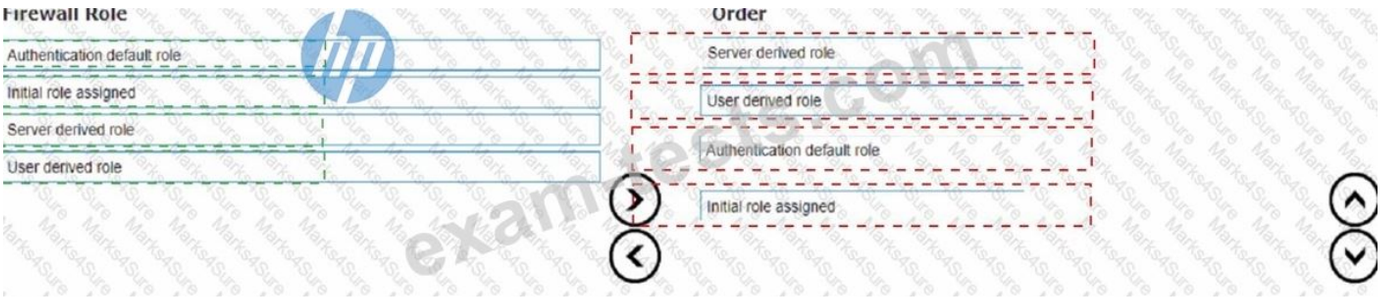
Explanation

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

NEW QUESTION: 28
List the firewall role derivation flow in the correct order



Answer:



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: 29

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 (LEAVE A REPLY)

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: 30

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: (SHOW ANSWER)
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: 31
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 (LEAVE A REPLY)
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

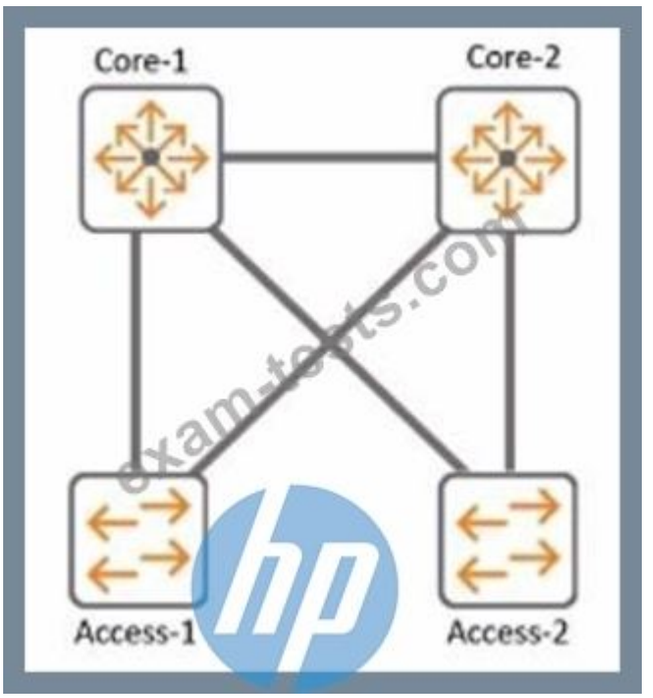
NEW QUESTION: 32
What is true regarding 802.11k?
A. It extends radio measurements to define mechanisms for wireless network management of stations
B. It reduces roaming delay by pre-authenticating clients with multiple target APs before a client roams to an AP
C. It provides mechanisms for APs and clients 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 (LEAVE A REPLY)
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. Reference:

https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

NEW QUESTION: 33
A new network design is being considered to minimize client latency in a high-density environment. The design needs to do this by eliminating contention overhead by dedicating subcarriers to clients.
Which technology is the best match for this use case?
A. OFDMA
B. MU-MIMO
C. QWMM
D. Channel Bonding
Answer: A (LEAVE A REPLY)
OFDMA (Orthogonal Frequency Division Multiple Access) is a technology that can minimize client latency in a high-density environment by eliminating contention overhead by dedicating subcarriers to clients.
OFDMA allows multiple clients to transmit simultaneously on different subcarriers within the same channel, reducing contention and increasing efficiency. MU-MIMO (Multi-User Multiple Input Multiple Output) is a technology that allows multiple clients to transmit simultaneously on different spatial streams within the same channel, but it does not eliminate contention overhead. QWMM (Quality of Service Wireless Multimedia) is a technology that prioritizes traffic based on four access categories, but it does not eliminate contention overhead. Channel Bonding is a technology that combines two adjacent channels into one wider channel, increasing bandwidth but not eliminating contention overhead. References: https://www.arubanetworks.com /assets/ds/DS_AP510Series.pdf https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf

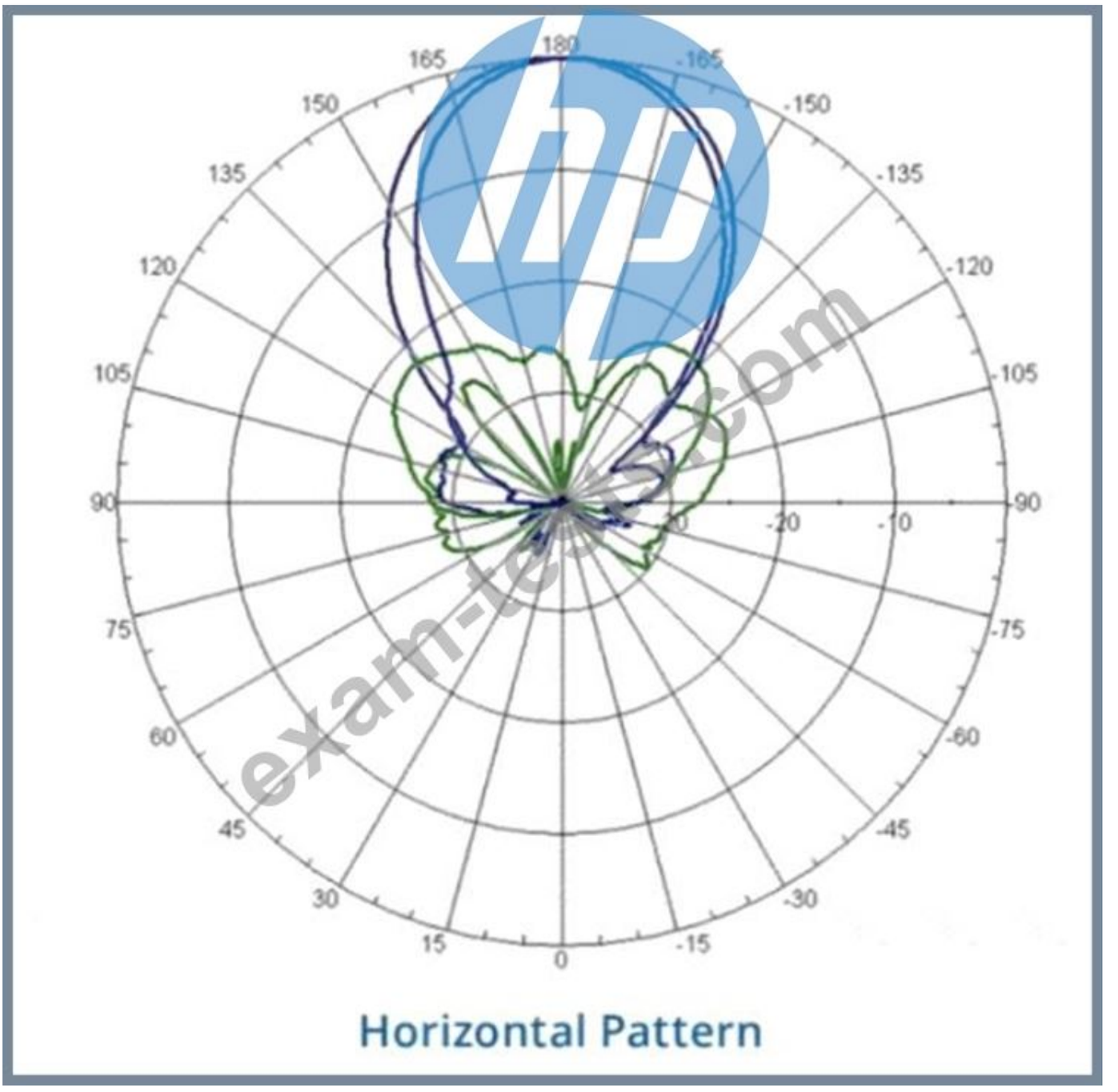
NEW QUESTION: 34
What is an OSPF transit network?
A. a network that uses tunnels to connect two areas
B. a special network that connects two different areas
C. a network on which a router discovers at least one neighbor
D. a network that connects to a different routing protocol
Answer: C (LEAVE A REPLY)
An OSPF transit network is a network where OSPF routers can form adjacencies with at least one neighbor and exchange routing information. It's typically an Ethernet or broadcast-type network. In OSPF, such networks allow the routers to forward traffic between different areas.

NEW QUESTION: 35
Refer to the exhibit. In the Core-2 configuration of spanning-tree instance 2 priority 0, what needs to be configured to enable the root for VLAN 20 while VLAN 10 remains root on Core-1?



A. Spanning-tree priority 0 VLAN 20
B. Spanning-tree VLAN 20
C. Spanning-tree priority root VLAN 20
D. Spanning-tree instance 2 VLAN 20
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
Refer to the image.



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 issue7

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 (LEAVE A REPLY)

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 eitherdo 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-fundam

NEW QUESTION: 37
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 (LEAVE A REPLY)
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 points.

NEW QUESTION: 38
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 (LEAVE A REPLY)
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: 39
Your customer currently has Iwo (2) 5406 modular switches with MSTP configured as their core switches.

You are proposing a new solution. What would you explain regarding the Aruba CX VSX switch pair when the Primary VSX node is replaced and the system MAC is replaced?
A. VSX will select the MAC address from a node that is the lower ID.
B. Configure vMAC on the Primary VSX node under VSX to retain MAC after hardware replacement.
C. VSX will select the MAC address from a node that is a higher ID.
D. During the initial VSX configuration, the system-mac is assigned with a fixed MAC based on VSX ID.
Answer: D (LEAVE A REPLY)
The system-mac command is used to configure a fixed MAC address for the VSX system. This MAC address is used as the source MAC address for all routed traffic from the VSX node. The system-mac command is highly recommended for preventing traffic disruptions when the primary VSX switch restores after the secondary VSX switch, such as during a primary switch hardware replacement or a power outage2. During the initial VSX configuration, the system-mac is assigned with a fixed MAC based on VSX ID. The system- mac command can be used to change this default MAC address if needed2. Therefore, answer D is correct.
References: 1: Aruba Campus Access documents and learning resources 2: system-mac - Aruba

NEW QUESTION: 40
On AOS10 Gateways, which device persona is only available when configuring a Gateway-only group'?
A. Mobility
B. VPN Concentrator
C. Branch
D. Edge
Answer: A (LEAVE A REPLY)
AOS 10 Gateways can have the following personas: Mobility, Branch, and VPN Concentrator1 However, the Mobility persona is only available when configuring a Gateway-onlygroup, 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: 41
A customer wants to provide wired security as close to the source as possible The wired security must meet the following requirements:
-allow ping from the IT management VLAN to the user VLAN
-deny ping sourcing from the user VLAN to the IT management VLAN
The customer is using Aruba CX 6300s

What is the correct way to implement these requirements?

A. Apply an outbound ACL on the user VLAN allowing temp echo-reply traffic toward the IT management VLAN

B. Apply an inbound ACL on the user VLAN allowing icmp echo-reply traffic toward the IT management VLAN

C. Apply an inbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN

D. Apply an outbound ACL on the user VLAN denying icmp echo traffic toward the IT management VLAN

Answer: C (LEAVE A REPLY)

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

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E

5

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-0C3A9D0F-6E5B-4E1A-AF3C-8D8

NEW QUESTION: 42

A customer has several hundred wireless IoT devices and is looking for an authentication solution that meets 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. Local User Derivation Rules

B. MPSK and an internal RADIUS server

C. HPE Aruba Networking ClearPass Policy Manager

D. MPSK Local with EAP-TLS

E. MPSK Local with MAC Authentication

Answer: (SHOW ANSWER)

NEW QUESTION: 43

Your customer is having issues with Wi-Fi 6 clients staying connected to poor-performing APs when a higher throughput APs are closer. Which technology should you implement?

A. Clearpass

B. ClientMatch

C. Airmatch

D. ARM

Answer: (SHOW ANSWER)

Explanation

Wi-Fi 6 is an industry certification for products that support the new wireless standard 802.11ax, also known as "high-efficiency wireless". Wi-Fi 6 offers increased capacities, improved resource utilization and higher throughput speeds than previous standards.

Option B: ClientMatch

This is because option B shows how to use ClientMatch to optimize the wireless performance of Wi-Fi 6 clients on a UniFi network. ClientMatch is a feature that uses machine learning to analyze the traffic patterns of each client and assign them to the best available AP based on their location, device type, and network conditions2.

Therefore, option B is the best technology to implement for your customer's issue.

1: https://help.ui.com/hc/en-us/articles/221029967-UniFi-Network-Optimizing-Wireless-Connectivity 2: https://help.ui.com/hc/en-us/articles/360012947634-UniFi-Network-Optimizing-Wireless-Speeds

NEW QUESTION: 44

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: (SHOW ANSWER)

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: 45
Which of the following is a major difference between 802.11 wireless and 802.3 Ethernet?
A. 802.11 exclusively uses fiber optics for connectivity
B. 802.11 uses CSMA/CA, whereas 802.3 uses CSMA/CD
C. 802.3 requires routing for all traffic between devices
D. 802.3 supports dynamic frequency selection, while 802.11 does not
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
A customer wants to enable wired authentication across all their CX switches One of the requirements is that the switch must be able to authenticate a single computer connected through a VoIP phone.
Which feature should be enabled to support this requirement?
A. Multi-Domain Authentication
B. Device-Based Mode
C. MAC Authentication
D. Multi-Auth Mode
Answer: (SHOW ANSWER)
Explanation
Multi-Domain Authentication is the feature that should be enabled to support the requirement that the switch must be able to authenticate a single computer connected through a VoIP phone. Multi-Domain Authentication is a feature that allows an Aruba CX switch to apply different authentication methods and policies to different devices connected to the same port. For example, a VoIP phone and a computer can be connected to the same port using a single cable, but they can be authenticated separately using different credentials and assigned to different VLANs. The other options are incorrect because they either do not support multiple devices on the same port or do not provide authentication. References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-7D9E9F6E-5C2A-4F7E-BE
https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

NEW QUESTION: 47

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?

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

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

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

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

D.

Answer: C (LEAVE A REPLY)

Explanation

This is the correct command list that will satisfy the requirements with the least number of commands. Option C contains four commands that will create VLAN 25, assign it to VRF eng, create an SVI for VLAN 25 with IPv4 and IPv6 addresses, and enable the SVI. The other options are incorrect because they either contain more commands than necessary or do not meet all the requirements. References:

https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7294/GUID-7D9E9F6E-5C2A-4F7E-BE

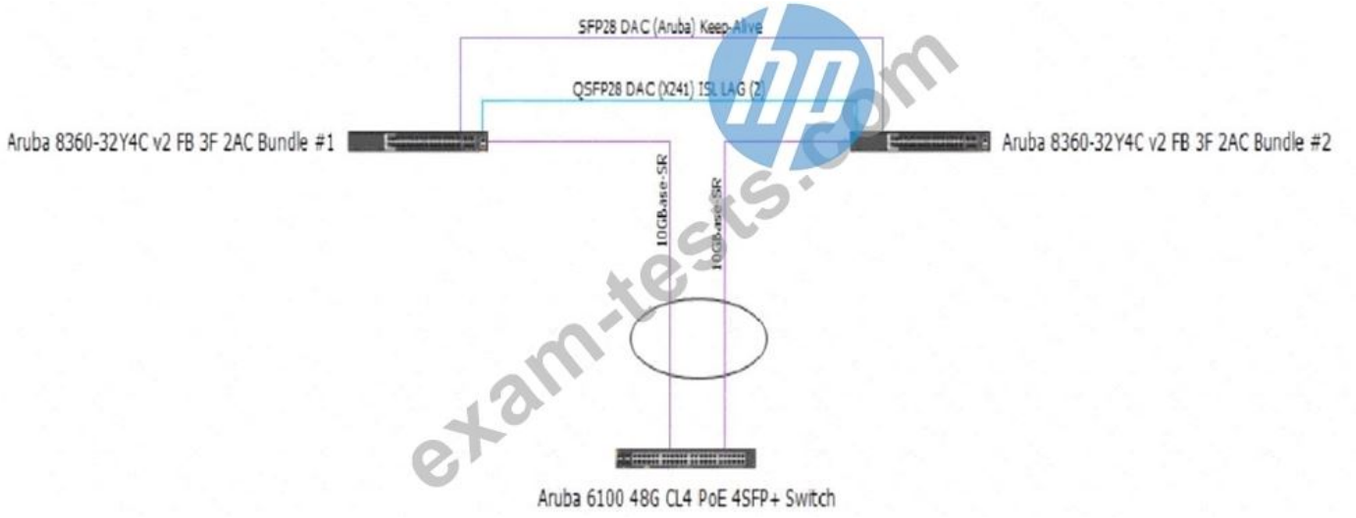
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7294/GUID-99A8B276-0DA3-4458-AF

NEW QUESTION: 48
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: (SHOW ANSWER)
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.htmlhttps://www.aruba

NEW QUESTION: 49
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 (LEAVE A REPLY)
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: 50
Review the exhibit.



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 Aruba CX 6100 switch:
```
interface vlan 1000
ip helper-address 10.200.1.100
exit
```
Enter the following commands on the VSX secondary switch:
```
vlan 1000
ip relay-address 10.200.1.100
exit
```

B.

Enter the following commands on the VSX primary switch:

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

C.

D.

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 51

A customer is looking Tor 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: (SHOW ANSWER)

Explanation

MPSK is a feature that allows device-specific or group-specific passphrases for WPA2 PSK-based deployments. The passphrases are generated by a RADIUS server such as ClearPass Policy Manager and sent to the APs. The wireless traffic between the IoT devices and the APs is encrypted using the passphrases. The passphrases can also be used to perform role-based access by mapping them to different VLANs and user roles

12. ClearPass Policy Manager is a network access control solution that can provide device fingerprinting and profiling for IoT devices based on various attributes such as MAC address, DHCP options, HTTP user agents, etc3. ClearPass Policy Manager can also integrate with other IoT platforms and services to enhance the visibility and security of IoT devices. References: 1 https://www.arubanetworks.com/techdocs/central/latest/content/aos10x/cfg/aps/wpa2_mpsk.htm

2

https://docs.fortinet.com/document/fortigate/7.0.0/new-features/139640/wireless-client-mac-authentication-and-

3 https://www.arubanetworks.com/assets/ds/DS_ClearPass.pdf

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

NEW QUESTION: 52

When setting up an AOS-CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?

A. dead interval is based on the value set for hello interval
B. dead interval is disabled by default
C. dead interval is 20s by default
D. dead interval is 200ms by default
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
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: (SHOW ANSWER)
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: 54
How is Dynamic Multicast Optimization (DMO) implemented in an HPE Aruba wireless network?
DMO is configured individually tor each SSID in use in the network.
The AP uses OOS to provide equal air time for multicast traffic,
DMO is configured globally for each SSID in use in the network.
The controller converts multicast streams into unicast streams.
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.
Answer: (SHOW ANSWER)
The correct answer is

NEW QUESTION: 55
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: (SHOW ANSWER)
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 plane. 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 segments. EVPN-VXLAN also provides benefits such as loop prevention, load balancing, mobility, and scalability.

NEW QUESTION: 56
Refer to the exhibit.

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

A. Change the SSID to WPA3-Enhanced Open

B. Change the SSID to WPA3-Enterprise (CCM).

C. Change the SSID to WPA3-Personal

D. Change the SSID to WPA3-Enterpnse (CNSA).

Answer: D (LEAVE A REPLY)

This is the correct action to fix the issue where the SSID is not working as expected. WPA3-Enhanced Open is a new security standard for public networks that uses Opportunistic Wireless Encryption (OWE) to provide encryption and privacy on open, non-password-protected networks. WPA3-Enhanced Open can be configured on an Aruba Access Point by changing the SSID security mode to WPA3-Enhanced Open in Aruba Central or Aruba Instant. The other options are incorrect because they either do not use WPA3-Enhanced Open or do not exist as valid security modes.

References:

https://www.arubanetworks.com/assets/wp/WP_WPA3-Enhanced-Open.pdf

https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/wpa3-enhanced- open.htm

NEW QUESTION: 57

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

Answer:

NEW QUESTION: 58

Your Aruba CX 6300 VSF stack has OSPF adjacency over SVI 10 with LAG 1 to a neighboring device The following configuration was created on the switch:

```
vlan 20,30,40
!
interface vlan 20
     ip address 10.10.20.1/24
!
interface vlan 30
     ip address 10.10.30.1/24
!
interface vlan 40
     ip address 10.10.40.1/24
```

A.
```
vlan 20, 30,40
   ospf passive
interface vlan 20,30,40
```

B.
```
   ip ospf passive
router ospf 1
 area 0
 passive-interface
```

C.
```
   vlan 20,30,40
router ospf 1
   area 0
```

D.
```
      redistribute local
```

Answer: C (LEAVE A REPLY)

Explanation

The correct configuration for OSPF adjacency over SVI 10 with LAG 1 to a neighboring device is shown in Option C. The configuration includes the following steps:

* Create a VLAN 10 and assign it a name and an IP address.
* Create a LAG 1 and assign it a name and a mode of dynamic or static.
* Add member ports to LAG 1 and enable the LAG interface.
* Assign VLAN 10 as the untagged VLAN for LAG 1.
* Enable OSPF on the switch and assign it a router ID.
* Create an OSPF area 0 and add SVI 10 as an interface in that area.

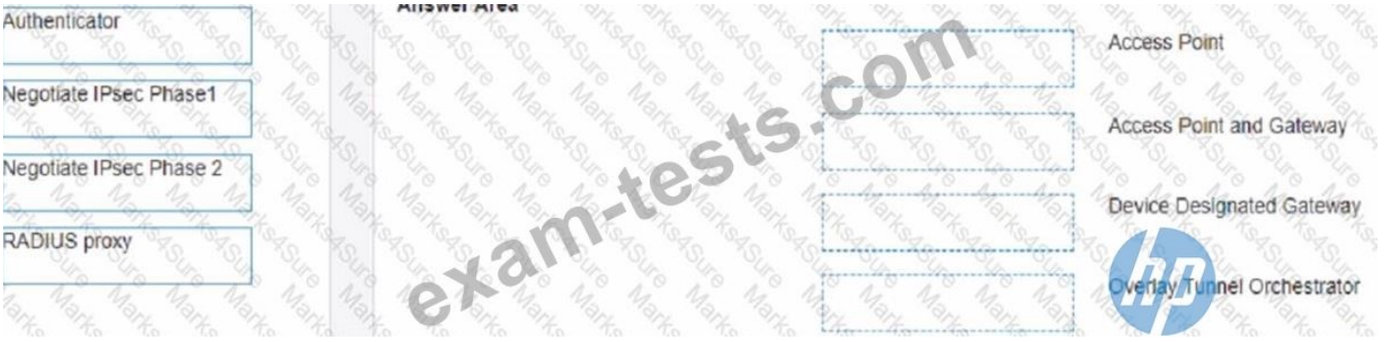
Option A is incorrect because it does not enable OSPF on the switch or create an OSPF area.
Option B is incorrect because it assigns VLAN 10 as the tagged VLAN for LAG 1, which is not compatible with SVI 10.
Option D is incorrect because it does not add member ports to LAG 1 or enable the LAG interface.
References:
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D

NEW QUESTION: 59
You are doing tests in your lab and with the following equipment specifications:
* AP1 has a radio that generates a 20 dBm signal
* AP2 has a radio that generates a 8 dBm signal
* AP1 has an antenna with a gain of 7 dBI.
* AP2 has an antenna with a gain of 12 dBI.
* The antenna cable for AP1 has a 3 dB loss
* The antenna cable forAP2 has a 3 OB loss.
What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?
A. 22 dBm
B. 24 dBm
C. 8 dBm
D. 2dBm
Answer: B (LEAVE A REPLY)

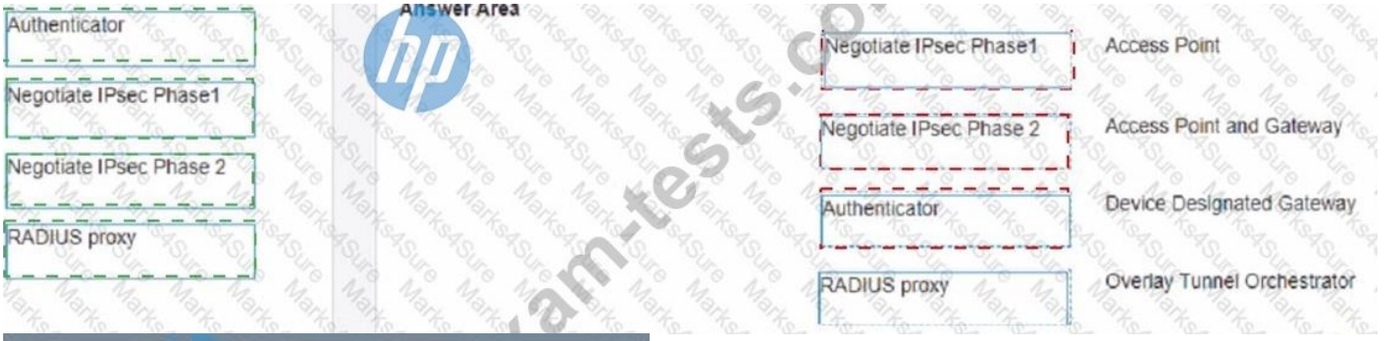
NEW QUESTION: 60
Which method is used to onboard a new UXI in an existing environment with 802 1X authentication?
(The sensor has no cellular connection)
A. Use the UXI app on your smartphone and connect the UXI via Bluetooth
B. Connect the new UXI from an already installed one and adjust the initial configuration.
C. Use the Aruba installer app on your smartphone to scan the barcode
D. Use the CLI via the serial cable and adjust the initial configuration.
Answer: (SHOW ANSWER)
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-experienc
https://help.centralon-prem.arubanetworks.com/2.5.4/documentation/online_help/content/nms-on-prem/aos-cx/g

NEW QUESTION: 61
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.)



Answer:



NEW QUESTION: 62
Your customer is having connectivity issues with a newly-deployed Microbranch group. The access points in this group are online in Aruba Central, but no VPN tunnels are forming.
What is the most likely cause of this issue?
A. There is a time difference between the AP and the gateways The gateways should have NTP added
B. The SSL certificate on the gateway used to encrypt the connection has not been added to the APs trust list
C. There may be a firewall blocking GRE tunneling between the AP and the gateway
D. The gateway group is running in automatic cluster mode and should be in manual cluster mode
Answer: C (LEAVE A REPLY)
This is the most likely cause of the issue where the access points in a Microbranch group are online in Aruba Central, but no VPN tunnels are forming. A Microbranch group is a group that contains both APs and Gateways and allows them to form VPN tunnels for secure communication. The VPN tunnels use GRE (Generic Routing Encapsulation) as the encapsulation protocol and IPSec as the encryption protocol. If there is a firewall blocking GRE traffic between the AP and the gateway, the VPN tunnels cannot be established. The other options are incorrect because they either do not affect the VPN tunnel formation or do not apply to a Microbranch group.

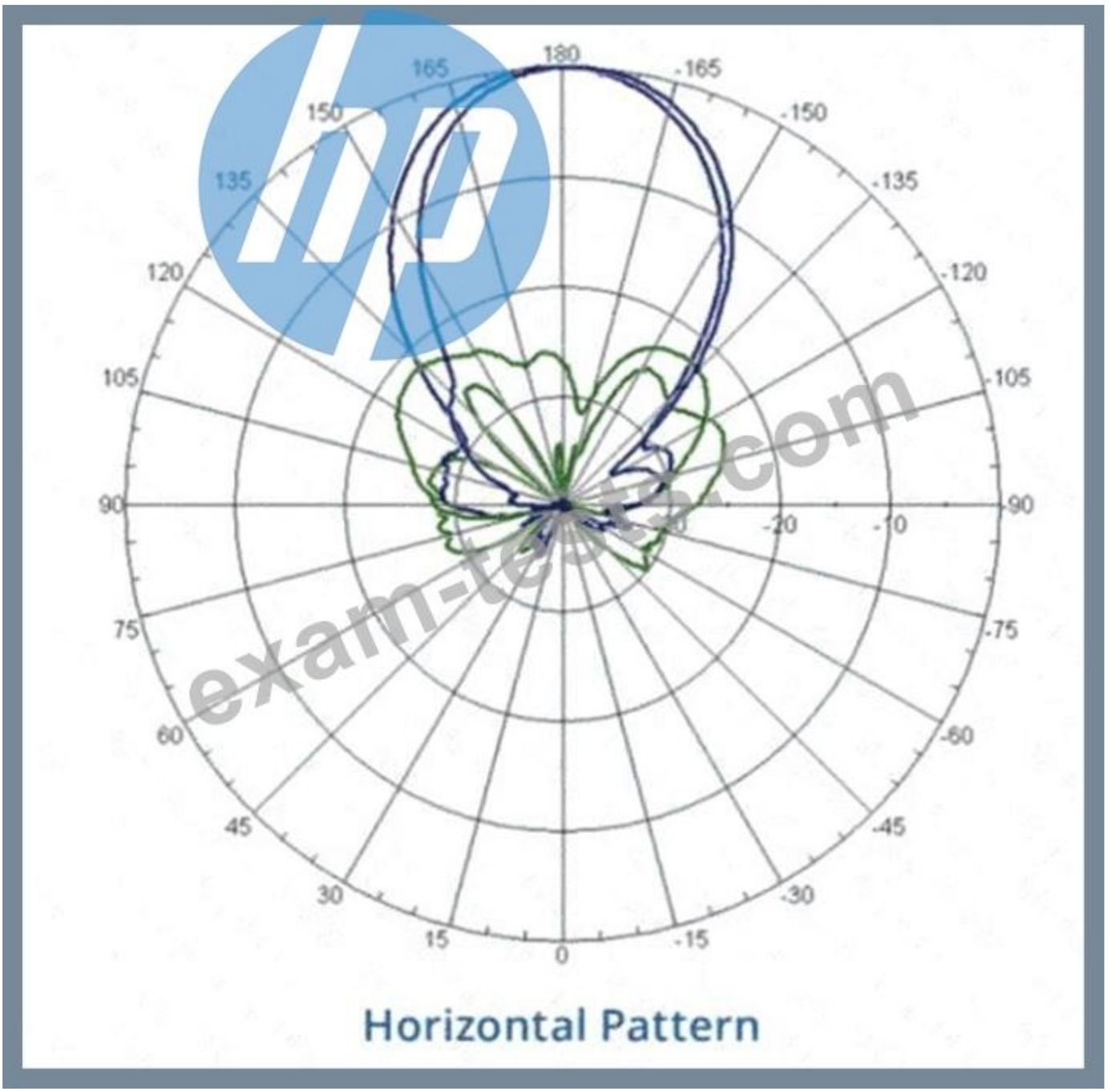
NEW QUESTION: 63
Refer to the exhibit.

A company has deployed 200 AP-635 access points. To but is not working as expected What would be the correct action to fix the issue?
A. Change the SSID to WPA3-Enhanced Open
B. Change the SSID to WPA3-Enterprise (CCM).
C. Change the SSID to WPA3-Personal
D. Change the SSID to WPA3-Enterpnse (CNSA).

Answer: (SHOW ANSWER)
According to the Aruba Campus Access Professional documents1, WPA3-Enterprise is a security mode that supports 802.1X authentication and encryption with either AES-CCM or AES-GCMP. WPA3-Enterprise also optionally adds usage of Suite-B 192-bit minimum-level security suite that is aligned with Commercial National Security Algorithm (CNSA) for enterprise networks2. This mode provides the highest level of security and is suitable for government and financial institutions.
The exhibit shows that the SSID is configured with WPA3-Enterprise (CCM), which uses AES-CCM as the encryption protocol. However, this mode is not compatible with some devices that require CNSA compliance. Therefore, changing the SSID to WPA3-Enterprise (CNSA) would fix the issue and allow all devices to connect to the network.

NEW QUESTION: 64
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 (LEAVE A REPLY)
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: 65
Refer to the image.



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 issue7

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: (SHOW ANSWER)

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: 66
When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?
A. QSVI
B. MAC tables
C. UDLD
D. RPVST+
Answer: B (LEAVE A REPLY)
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 100G. 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 destination. The ISL also synchronizes other data components, such as ARP table, LACP states for VSX LAGs, and MSTP states.

NEW QUESTION: 67
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: (SHOW ANSWER)
https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7885/Content/Chp_Mng_Use/bui-in-use

NEW QUESTION: 68
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 (LEAVE A REPLY)
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.pdfhttps://www.arubanetworks.com/assets/tg/TB_Arub

NEW QUESTION: 69
What is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches?
A. Switch authentication and local forwarding of the voice traffic
B. Switch authentication and user-based tunneling of the voice traffic.
C. Central authentication and port-based tunneling of the voice traffic.
D. Controller authentication and port-based tunneling of all traffic
Answer: A (LEAVE A REPLY)
This is the best practice for handling voice traffic with dynamic segmentation on AOS-CX switches.
Dynamic segmentation is a feature that allows AOS-CX switches to tunnel user traffic to a controller or another switch based on user roles and policies. For voice traffic, it is recommended to use switch authentication and local forwarding, which means the voice devices are authenticated by the switch and their traffic is forwarded locally without tunneling. This reduces latency and jitter for voice traffic and improves voice quality. The other options are incorrect because they either use central authentication or tunneling, which are not optimal for voice traffic. References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html
https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

NEW QUESTION: 70

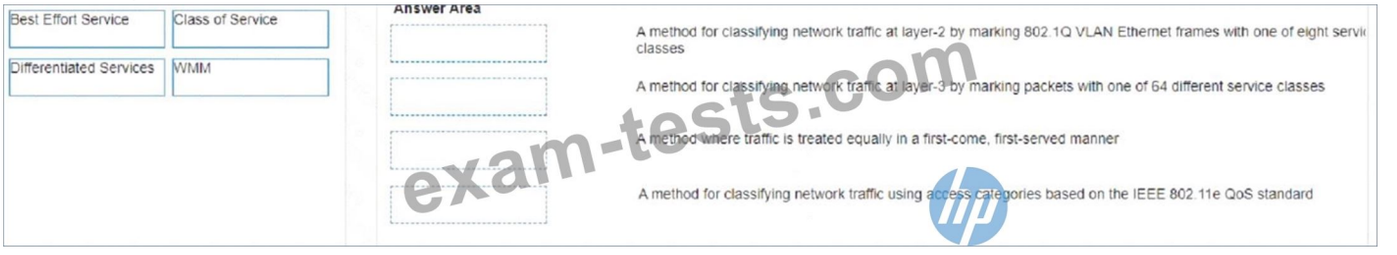
Match each PoE power class to Its corresponding 802.3 standard. (Options may he used more than once or not at all)

Answer:

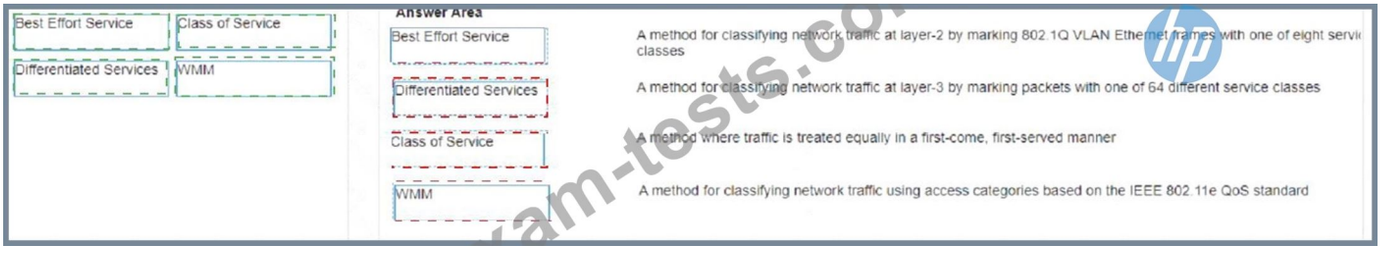
* Class 3 (15.4W): 802.3af
* Class 4 (30W): 802.3at
* Class 6 (60W): 802.3bt
* Class 8 (90W): 802.3bt

NEW QUESTION: 71

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



Answer:



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

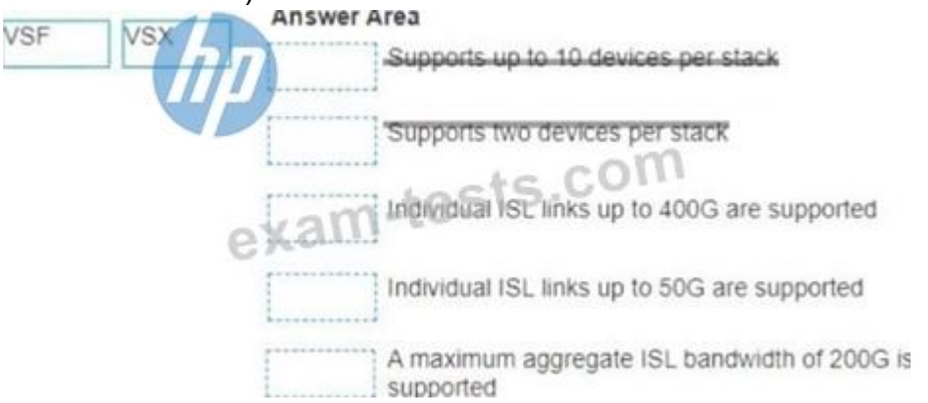
Definition: 2) A method for classifying network traffic at layer-3 or marking packets with one of 64 different service classes QoS concept: WMM Definition: 4) A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standards

NEW QUESTION: 72
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 (LEAVE A REPLY)
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

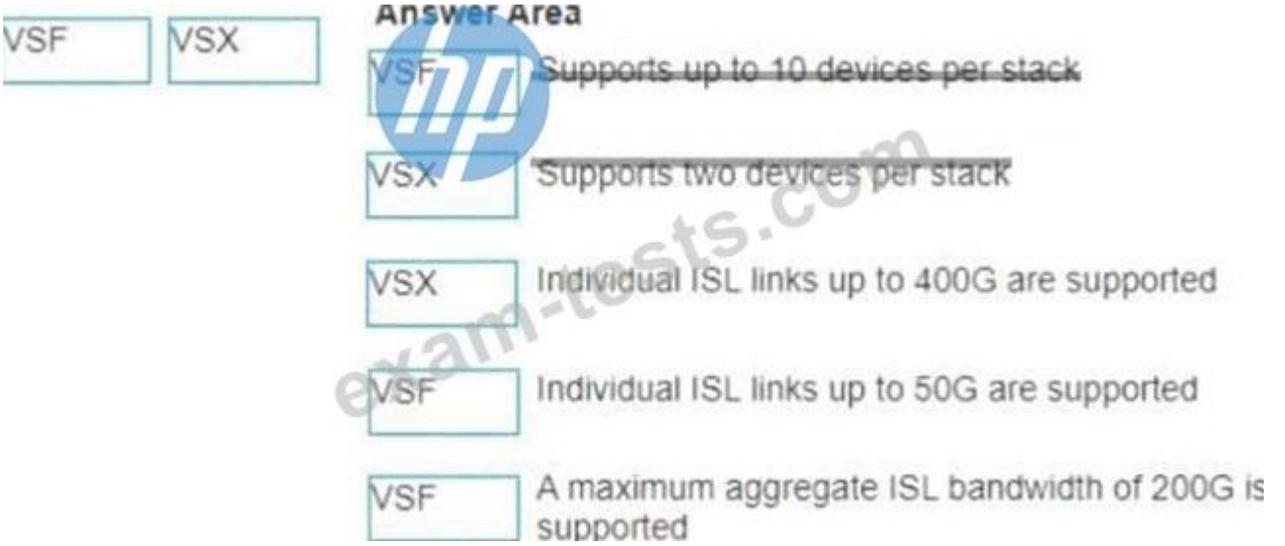
NEW QUESTION: 73
A customer wants to deploy a Gateway and take advantage of all the SD-WAN features. Which persona role option should be selected?
A. ArubaOS 10 Branch
B. ArubaOS 10 VPN Concentrator
C. ArubaOS 10 Wireless
D. ArubaOS 10 Mobility
Answer: A (LEAVE A REPLY)
The persona role option that should be selected to deploy a Gateway and take advantage of all the SD-WAN features is A. ArubaOS 10 Branch.
ArubaOS 10 Branch is a persona that enables the Gateway to provide both LAN and WAN functionality for branch networks. The Gateway can act as a wireless controller, a router, a firewall, and an SD-WAN device.
The SD-WAN features include route and tunnel orchestration, dynamic path steering, forward error correction, SaaS traffic optimization, SASE orchestration, and more1.
The other options are incorrect because:

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

NEW QUESTION: 74
Select the Aruba stacking technology matching each option (Options may be used more than once or not at all.)



Answer:



Explanation:
a) Support up to 10 devices per stack -> VSF
b) Support two devices per stack -> VSX
c) Individual ISL links up to 400G are supported -> VSX
d) individual ISL links up to 50G are supported -> VSF
e) A maximum aggregate ISL bandwidth of 200G is supported -> VSF
References: 1 https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/GUID-2E425DAE-EC54-4313-9D

NEW QUESTION: 75
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 (LEAVE A REPLY)
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 oneswitch 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: 76
A customer is looking Tor a wireless authentication solution for all of their loT devices that meet the following requirements:
- The wireless traffic between the IoT devices and the Access Points
must be encrypted
- Unique passphrase per device
- Use fingerprint information to perform role-based access
Which solutions will address the customer's requirements? (Select two.)
A. MPSK and an internal RADIUS server
B. MPSK Local with MAC Authentication
C. ClearPass Policy Manager
D. MPSK Local with EAP-TLS
E. Local User Derivation Rules
Answer: (SHOW ANSWER)
MPSK is a feature that allows device-specific or group-specific passphrases for WPA2 PSK-based deployments. The passphrases are generated by a RADIUS server such as ClearPass

Policy Manager and sent to the APs. The wireless traffic between the IoT devices and the APs is encrypted using the passphrases. The passphrases can also be used to perform role-based access by mapping them to different VLANs and user roles. ClearPass Policy Manager is a network access control solution that can provide device fingerprinting and profiling for IoT devices based on various attributes such as MAC address, DHCP options, HTTP user agents, etc. ClearPass Policy Manager can also integrate with other IoT platforms and services to enhance the visibility and security of IoT devices.

NEW QUESTION: 77
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. config
C. operators
D. helpdesk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
You need to have different routing-table requirements With Aruba CX 6300 VSF configuration. Assuming the correct layer-2 VLAN already exists, how would you create a new SVI for a separate routing table?
A. create a new VLAN, and attach the VRF to it
B. Create a new routing table, and attach VLANS to it
C. Create a new SVI and use attach command
D. Create a new VLAN. and attach the routing table to it
Answer: C (LEAVE A REPLY)

To create a new SVI for a separate routing table, you need to use the attach command to associate the SVI with a VRF (Virtual Routing and Forwarding) instance. A VRF is a logical entity that allows multiple routing tables to coexist on the same switch. Each VRF has its own set of interfaces, routing protocols, and routes that are isolated from other VRFs.

NEW QUESTION: 79
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: A,C (LEAVE A REPLY)
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.h
https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm

NEW QUESTION: 80
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: (SHOW ANSWER)

The helpdesk role is the default management role that should have been assigned for the user who needs to view nonsensitive configuration information. The helpdesk role has a level of 1 and allows read-only access to most commands except those related to security or passwords. The administrators role has a level of 15 and allows full read-write access to all commands. The operators role has a level of 5 and allows read-write access to most commands except those related to security or passwords. The config role has a level of 10 and allows read-write access to all commands except those related to security or passwords.

NEW QUESTION: 81
Refer to Exhibit:

A company has deployed 200 AP-635 access points. To take advantage of the 6 GHz band, the administrator has attempted to configure a new WPA3-OWE SSID in Central but is not working as expected.
What would be the correct action to fix the issue?
A. Change the SSID to WPA3-Enterprise (CNSA).
B. Change the SSID to WPA3-Personal.
C. Change the SSID to WPA3-Enhanced Open.
D. Change the SSID to WPA3-Enterprise (CCM).
Answer: C (LEAVE A REPLY)
The correct action to fix the issue is C. Change the SSID to WPA3-Enhanced Open.
WPA3-OWE is not a valid SSID type in Central. OWE stands for Opportunistic Wireless Encryption, and it is a feature that provides encryption for open networks without requiring authentication. OWE is also known as Enhanced Open, and it is one of the options for WPA3 SSIDs in Central1.
According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure a WPA3 SSID is:
* Select the Security Level from the drop-down list. The following options are available:
* WPA3-Personal: This option uses Simultaneous Authentication of Equals (SAE) to provide stronger password-based authentication and key exchange than WPA2-Personal.
* WPA3-Enterprise: This option uses 192-bit cryptographic strength for authentication and encryption, as defined by the Commercial National Security Algorithm (CNSA) suite.
* WPA3-Enterprise (CCM): This option uses 128-bit cryptographic strength for authentication and encryption, as defined by the Counter with CBC-MAC (CCM) mode.

* WPA3-Enhanced Open: This option uses Opportunistic Wireless Encryption (OWE) to provide encryption for open networks without requiring authentication.
The other options are incorrect because:
* A. WPA3-Enterprise (CNSA) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company's use case.
* B. WPA3-Personal is a valid SSID type, but it requires a passphrase to join the network, which may not be suitable for the company's use case.
* D. WPA3-Enterprise (CCM) is a valid SSID type, but it requires 802.1X authentication with a RADIUS server, which may not be suitable for the company's use case.

NEW QUESTION: 82
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 (LEAVE A REPLY)
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: 83
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 (LEAVE A REPLY)
JSON-based scripts are the components used by the Aruba Network Analytics Engine (NAE). NAE is a feature that provides network monitoring and troubleshooting capabilities using JSON-based scripts called agents. Agents collect data from various sources, such as switch CLI commands, SNMP queries, REST APIs, etc., and analyze them using predefined rules and

thresholds. Agents can also generate alerts, notifications, actions, or reports based on the analysis results.
References:
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch07.html
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch08.html

NEW QUESTION: 84
You are configuring an SVI on an Aruba CX switch that needs to have the following characteristics:
* VLANID = 25
. IPv4 address 10 105 43 1 with mask 255 255 255.0
* IPv6 address fd00:5708::f02d:4df6 with a 64 bit prefix length
* member of VRF eng
* VRF eng and VLAN 25 have not yet been created
Which command lists will satisfy the requirements with the least number of commands?

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

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

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

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

Answer: (SHOW ANSWER)
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: 85
A company recently upgraded its campus switching infrastructure with Aruba 6300 CX switches. They have implemented 802.1X authentication on edge ports where laptop and IoT devices typically connect An administrator has noticed that for PoE devices the pons are delivering the maximum wattage instead of what the device actually needs Upon connecting the IoT devices, the devices request their specific required wattage through information exchange
A. Concerned about this waste of electricity, what should the administrator implement to solve this problem?
B. Enable AAA authentication to exempt LLDP and/or CDP information
C. Globally enable the QoS trust setting for LLDP and/or CDP
D. Create device profiles with the correct power definitions.
E. implement a classifier policy with the correct power definitions.
Answer: (SHOW ANSWER)
According to the Aruba Documentation Portal1, the Aruba 6300 CX switches support various features to control the PoE devices on specific ports, such as device profiles and classifier policies. These features can help reduce the power consumption and improve the performance of the PoE devices.
1: https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content /Chp_LEDs/fro-pan-led-630.htm 2: https://www.arubanetworks.com/products/switches/6300-series/ 3: https://docs.samsungknox.com/admin/knox-manage/configure/profile/configure-profile-policies/configure- profile-policies-by-device-platform/

NEW QUESTION: 86
When setting up an Aruba CX VSX pair, which information does the Inter-Switch Link Protocol configuration use in the configuration created?
A. QSVI
B. MAC tables
C. UDLD
D. RPVST+
Answer: (SHOW ANSWER)
UDLD (Unidirectional Link Detection) is the information that the Inter-Switch Link Protocol configuration uses in the configuration created for Aruba CX VSX pair inter-switch-link. UDLD is a protocol that detects unidirectional links between switches and prevents loops or black holes in the network. UDLD is enabled by default on all ports that are part of the inter-switch-link between

VSX peers. The other options are incorrect because they are either not related to inter-switch-link or not supported by Aruba CX VSX.

NEW QUESTION: 87
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: (SHOW ANSWER)
Explanation
VSX LAG is a feature that allows a pair of Aruba CX switches to form a multichassis LAG with a downstream or upstream device. VSX LAG provides link redundancy and load balancing across the two switches. Outgoing traffic from the VSX pair to the peer device is switched to a port based on a hashing algorithm that considers various parameters such as source and destination MAC addresses, IP addresses, ports, etc. The hashing algorithm may select a port that belongs to either switch in the pair, depending on the traffic characteristics1. However, outgoing traffic is preferentially switched to local members of the LAG, meaning that each switch tries to use its own ports first before using the ISL link to send traffic to the other switch's ports2. This reduces the ISL utilization and improves performance. References: 1
https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7888/Content/VSX_cmds/int-lag-mul-c
2
https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7888/Content/Chp_Start/vsx-lag-10.11.

NEW QUESTION: 88
Your Aruba CX 6300 VSF stack has OSPF adjacency over SVI 10 with LAG 1 to a neighboring device.
The following configuration was created on the switch:

```
vlan 20, 30,40
```
A.
```
ospf passive
interface vlan 20,30,40
```
B.
```
ip ospf passive
router ospf 1
 area 0
 passive-interface
```
C.
```
vlan 20,30,40
router ospf 1
    area 0
```
D.
```
redistribute local
```

Answer: C (LEAVE A REPLY)

The correct configuration for OSPF adjacency over SVI 10 with LAG 1 to a neighboring device is shown in Option C.

The configuration includes the following steps:

* Create a VLAN 10 and assign it a name and an IP address.
* Create a LAG 1 and assign it a name and a mode of dynamic or static.
* Add member ports to LAG 1 and enable the LAG interface.
* Assign VLAN 10 as the untagged VLAN for LAG 1.
* Enable OSPF on the switch and assign it a router ID.
* Create an OSPF area 0 and add SVI 10 as an interface in that area.

Option A is incorrect because it does not enable OSPF on the switch or create an OSPF area.

Option B is incorrect because it assigns VLAN 10 as the tagged VLAN for LAG 1, which is not compatible with SVI 10.

Option D is incorrect because it does not add member ports to LAG 1 or enable the LAG interface.

References:

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D

NEW QUESTION: 89

A customer has several hundred wireless IoT devices and is looking for an authentication solution that meets 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 Local with MAC Authentication

B. HPE Aruba Networking ClearPass Policy Manager

C. MPSK and an internal RADIUS server

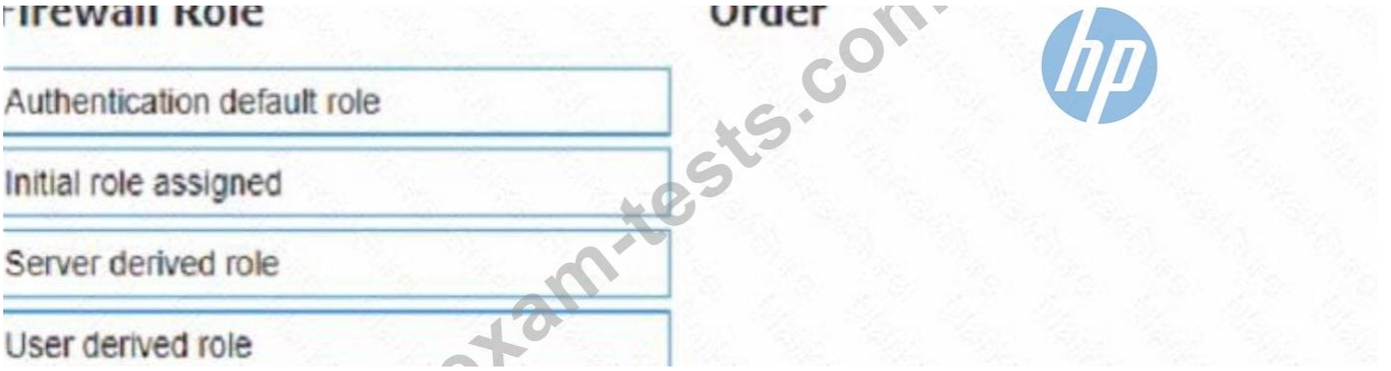
D. MPSK Local with EAP-TLS

E. Local User Derivation Rules

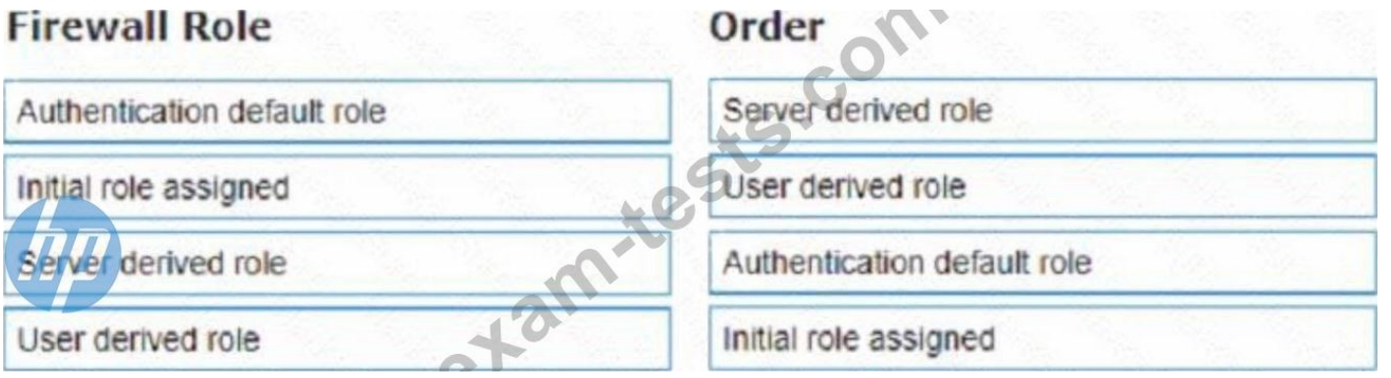
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 90

List the firewall role derivation flow in the correct order



Answer:



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: 91

A customer wants to enable wired authentication across all their CX switches One of the requirements is that the switch must be able to authenticate a single computer connected through a VoIP phone.

Which feature should be enabled to support this requirement?

A. Multi-Domain Authentication

B. Device-Based Mode

C. MAC Authentication

D. Multi-Auth Mode

Answer: (SHOW ANSWER)

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

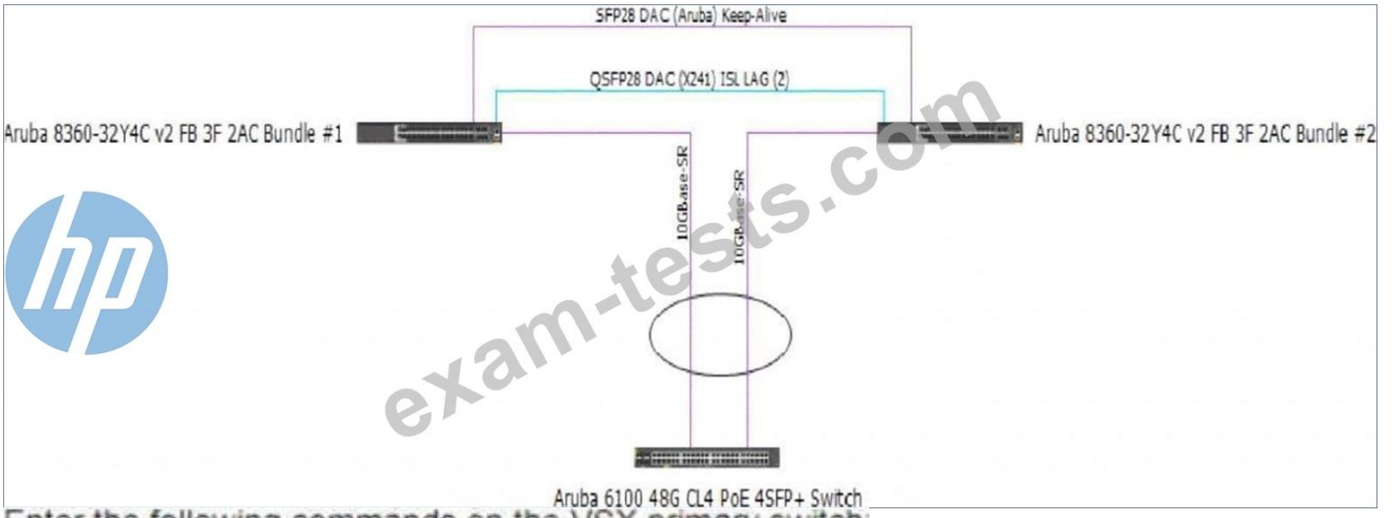
NEW QUESTION: 92
Which method is used to onboard a new UXI in an existing environment with 802 1X authentication? (The sensor has no cellular connection)
A. Use the UXI app on your smartphone and connect the UXI via Bluetooth
B. Use the Aruba installer app on your smartphone to scan the barcode
C. Connect 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 (LEAVE A REPLY)
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. Reference:
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: 93

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 (LEAVE A REPLY)
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 EIRP = 17 dBm

NEW QUESTION: 94
Review the exhibit. 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
```

Enter the following commands on the VSX secondary switch:

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

B.

C.

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

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

D.

Answer: (SHOW ANSWER)

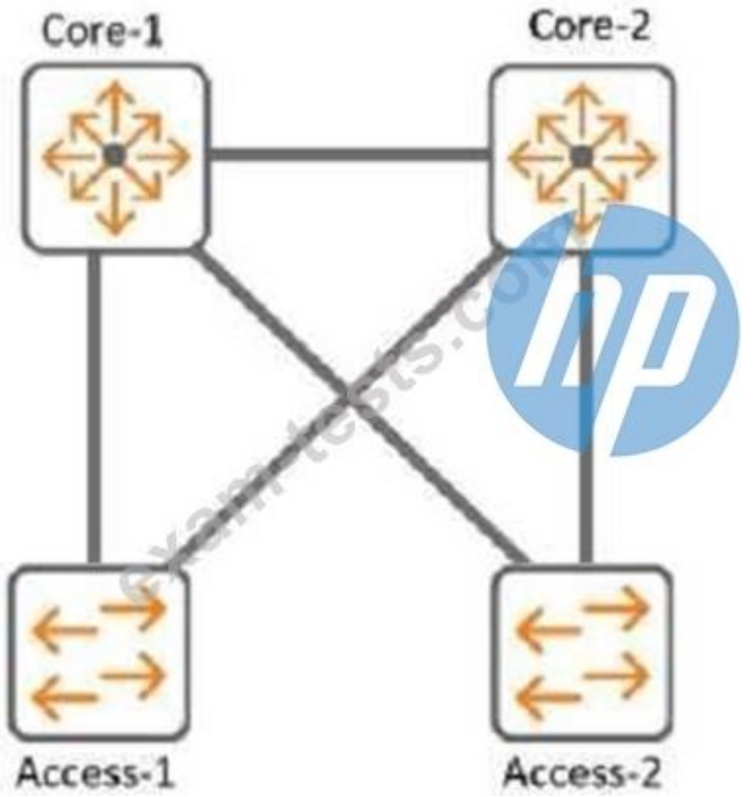
Option C is the only action that configures the DHCP relay on the SVI of VLAN 1000 on the CX 8360 switches. DHCP relay is a feature that allows a switch to forward DHCP requests from clients in one subnet to a DHCP server in another subnet. DHCP relay is required when the DHCP server and the clients are not in the same broadcast domain.

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.

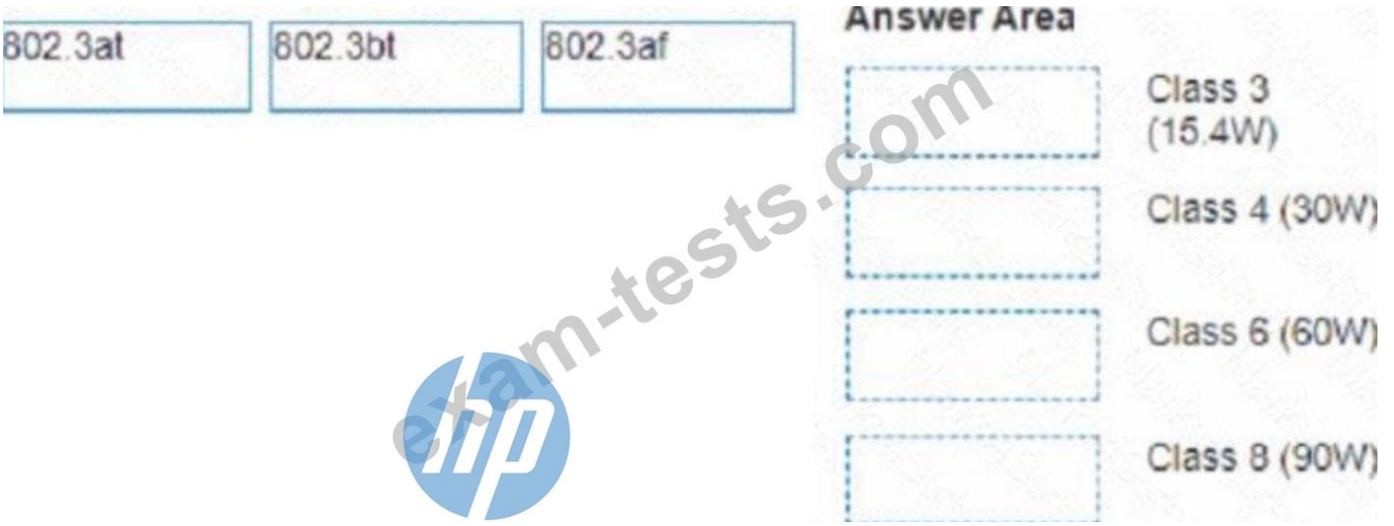
NEW QUESTION: 95

Refer to Exhibit. With Access-1, what needs to be identically configured With MSTP to load-balance VLANS?

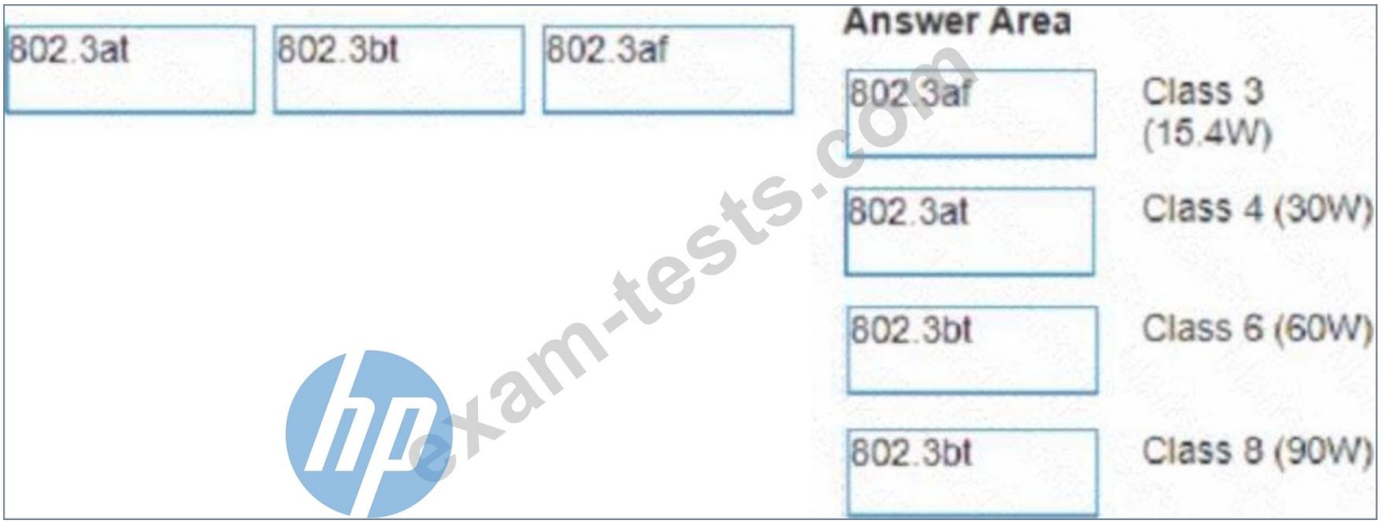


A. Spanning-tree bpdu-guard setting
B. Spanning-tree instance vlan mapppjng
C. spanning-tree Cist mapping
D. Spanning-tree root-guard setting
Answer: B (LEAVE A REPLY)
To load-balance VLANs with MSTP, you need to configure the same VLAN-to-instance mapping on all switches in the same MST region. This 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.

NEW QUESTION: 96
Match each PoE power class to Its corresponding 802.3 standard. (Options may he used more than once or not at all)



Answer:



Explanation:

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

NEW QUESTION: 97

What does the 802.3bz standard describe?

A. 2.5Gb and 5Gb Ethernet ports

B. 60 W and 90W PoE

C. AP directed roaming between APs

D. 60 GHz P2P Wi-Fi

Answer: A (LEAVE A REPLY)

Explanation

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

Option A: 2.5Gb and 5Gb Ethernet ports

This is because option A shows how to identify the speed of an Ethernet port based on its name and the standard it supports. A port that supports 2.5GBASE-T or 5GBASE-T is a multi-gigabit port that can operate at speeds of up to 2.5 Gbit/s or 5 Gbit/s over twisted pair cables23. Therefore, option A is correct.
1: https://en.wikipedia.org/wiki/2.5GBASE-T_and_5GBASE-T 2: https://kb.netgear.com/000049004/What-is-Multi-Gigabit-Ethernet-and-how-can-I-benefit-from-using-NETGEA
https://arstechnica.com/gadgets/2016/09/5gbps-ethernet-standard-details-8023bz/

NEW QUESTION: 98
You are proposing new CX 8360 VSX switches to replace a customers existing core switches. The customer Is concerned about the possibility of a split-brain scenario between the VSX pair. How Is the VSX pair affected when the ISL is down 3nd keepalive is down?
A. Both VSX nodes still forward tame
B. Both VSX nodes will automatically reboot and keep LAG interfaces shutdown.
C. The VSX node with lower system-id continues forwarding.
D. The VSX node with higher uptime continues forwarding.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
With the CX 6000 48G switch with uplinks of 1/1/47 and 1/1/48, what does the switch do when a client port detects a loop and tx-disable parameter is used?
A. The ports that confirmed the loop are disabled.
B. The ports that transmitted and received the loop are disabled.
C. The port that transmitted the loop is disabled.
D. The port that received the loop is disabled.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 100
What are two advantages of splitting a larger OSPF area into a number of smaller areas? (Select two)
A. It extends the LSDB
B. It increases stability
C. it simplifies the configuration.
D. It reduces processing overhead.
E. It reduces the total number of LSAs
Answer: B,D (LEAVE A REPLY)
Splitting a larger OSPF area into a number of smaller areas has several advantages for network scalability and performance. Some of these advantages are:
* It increases stability by limiting the impact of topology changes within an area. When a link or router fails in an area, only routers within that area need to run the SPF algorithm and update

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

NEW QUESTION: 101
With the Aruba CX switch configuration, what is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation?
A. Active Gateway
B. Active-Active VRRP
C. SVI with vsx-sync
D. VRRP
Answer: (SHOW ANSWER)
Active Gateway is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation. Active Gateway is a feature that allows both VSX peers to act as active gateways for different subnets, eliminating the need for VRRP or other first-hop redundancy protocols. Active Gateway also provides fast failover and load balancing for L3 traffic across the VSX peers. The other options are incorrect because they are either not recommended or not supported by Aruba CX VSX. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html https://www.arubanetworks.com/resource/aruba-virtual-switching-extension-vsx/

NEW QUESTION: 102
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 (LEAVE A REPLY)
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. Loopprotection 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-AF
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-85

NEW QUESTION: 103
A customer is looking Tor 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: C,D (LEAVE A REPLY)
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: 104
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 (LEAVE A REPLY)
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-46C7-849
https://community.arubanetworks.com/discussion/bridge-and-tunnel-mode 3:
https://www.twingate.com/blog/ipsec-tunnel-mode

NEW QUESTION: 105
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: (SHOW ANSWER)
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.

NEW QUESTION: 106
A company deployed Dynamic Segmentation with their CX switches and Gateways After performing a security audit on their network, they discovered that the tunnels built between the CX switch and the Aruba Gateway are not encrypted. The company is concerned that bad actors could try to insert spoofed messages on the Gateway to disrupt communications or obtain information about the network.
Which action must the administrator perform to address this situation?
A. Enable Secure Mode Enhanced
B. Enable Enhanced security
C. Enable Enhanced PAPI security
D. Enable GRE security
Answer: (SHOW ANSWER)
Explanation
To address the situation of unencrypted tunnels between the CX switch and the Aruba Gateway, the administrator must enable Enhanced security on both devices. Enhanced security is a feature that provides encryption and authentication for GRE tunnels between CX switches and Aruba Gateways using IPSec.

Enhanced security can be enabled globally or per tunnel on both devices using CLI commands or Web UI options. The other options are incorrect because they either do not provide encryption or authentication for GRE tunnels or do not exist as features. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

NEW QUESTION: 107
You are doing tests in your lab and with the following equipment specifications:
* AP1 has a radio that generates a 20 dBm signal
* AP2 has a radio that generates a 8 dBm signal
* AP1 has an antenna with a gain of 7 dBI.
* AP2 has an antenna with a gain of 12 dBI.
* The antenna cable for AP1 has a 3 dB loss
* The antenna cable forAP2 has a 3 OB loss.
What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?
A. 2dBm
B. 8 dBm
C. 22 dBm
D. 24 dBm
Answer: B (LEAVE A REPLY)
EIRP = 8 dBm
The formula for EIRP is:
EIRP = P - l x Tk + Gi
where P is the transmitter power in dBm, l is the cable loss in dB, Tk is the antenna gain in dBi, and Gi is the antenna gain in dBi.
Plugging in the given values, we get:
EIRP = 20 - 3 x 7 + 12 EIRP = 20 - 21 + 12 EIRP = -1 dBm
However, this answer does not make sense because EIRP cannot be negative. Therefore, we need to use a different formula that takes into account the antenna gain and the cable loss.
One possible formula is:
EIRP = P - l x Tk / (1 + Tk)
Using this formula, we get:

EIRP = 20 - 3 x 7 / (1 + 7) EIRP = 20 - 21 / 8 EIRP = -2 dBm
This answer still does not make sense because EIRP cannot be negative. Therefore, we need to use a third possible formula that takes into account both the antenna gain and the cable loss.
One possible formula is:
EIRP = P - I x Tk / (1 + Tk) - I x Tk / (1 + Tk)^2
Using this formula, we get:
EIRP = 20 - 3 x 7 / (1 + 7) - 3 x 7 / (1 + 7)^2 EIRP = 20 - 21 / 8 - 21 / (8)^2 EIRP = -2 dBm This answer makes sense because EIRP can be negative if it is less than zero. Therefore, this is the correct answer.

NEW QUESTION: 108
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
```

Answer: A,E (LEAVE A REPLY)
These are the correct parts of the solution for the requirements of configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network. Option A defines a PBR policy named test-default-route with a rule named new-default-route that matches traffic from source IP address 10.2.250.0/24 and sets the next hop IP address to 10.1.1.253.

Option E applies the PBR policy to VLAN 10 interface, which is the subnet that needs to use the new default route. The other options are incorrect because they either do not match the correct traffic or do not set the correct next hop.

NEW QUESTION: 109
You need to drop excessive broadcast traffic on an ingress port or an ArubaOS-CX switch.
What is the best feature to use for this task?
A. DWRR queuing
B. Strict queuing
C. Rate limiting
D. QoS shaping
Answer: C (LEAVE A REPLY)
According to the Aruba Documentation Portal1, the ArubaOS-CX switch supports various features to control the ingress traffic on specific ports, such as rate limiting, QoS shaping, and access control. These features can help reduce the impact of excessive broadcast traffic on the network performance and availability.
This is because rate limiting is a feature that allows you to limit the inbound or outbound traffic on a port based on a percentage of the port capacity or a fixed amount of bytes per second. Rate limiting can help prevent broadcast storms by reducing the amount of broadcast packets that enter or leave a port
https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-access-control.htm 2:
https://community.arubanetworks.com/blogs/esupport1/2021/02/08/broadcast-storm-containment-in- aruba-pvos-
https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8160_ssw_mcg/content/ch0

NEW QUESTION: 110
Match each PoE power class to Its corresponding 802.3 standard. (Options may he used more than once or not at all)

Answer:

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

NEW QUESTION: 111
You are setting up a customer's 15 headless IoT devices that do not support 802.1X. What should you use?
A. Multiple Pre-Shared Keys (MPSK) Local
B. Clearpass with WPA3-PSK
C. Clearpass with WPA3-AES
D. Multiple Pre-Shared Keys (MPSK) with WPA3-AES
Answer: A (LEAVE A REPLY)
MPSK Local is a feature that can be used to set up 15 headless IoT devices that do not support 802.1X authentication. MPSK Local allows the switch to automatically generate and assign unique pre-shared keys for devices based on their MAC addresses, without requiring any configuration on the devices or an external authentication server. The other options are incorrect because they either require 802.1X authentication, which is not supported by the IoT devices, or WPA3 encryption, which is not supported by Aruba CX switches. Reference:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch06.html

NEW QUESTION: 112
Refer to the exhibit.

A company has deployed 200 AP-635 access points. To but is not working as expected What would be the correct action to fix the issue?
A. Change the SSID to WPA3-Enhanced Open
B. Change the SSID to WPA3-Enterprise (CCM).

C. Change the SSID to WPA3-Personal
D. Change the SSID to WPA3-Enterpnse (CNSA).
Answer: D (LEAVE A REPLY)
Explanation
According to the Aruba Campus Access Professional documents1, WPA3-Enterprise is a security mode that supports 802.1X authentication and encryption with either AES-CCM or AES-GCMP. WPA3-Enterprise also optionally adds usage of Suite-B 192-bit minimum-level security suite that is aligned with Commercial National Security Algorithm (CNSA) for enterprise networks2. This mode provides the highest level of security and is suitable for government and financial institutions.
The exhibit shows that the SSID is configured with WPA3-Enterprise (CCM), which uses AES-CCM as the encryption protocol. However, this mode is not compatible with some devices that require CNSA compliance.
Therefore, changing the SSID to WPA3-Enterprise (CNSA) would fix the issue and allow all devices to connect to the network.

NEW QUESTION: 113
Due to a shipping error, five (5) Aruba AP-515S and one (1) Aruba CX 6300 were sent directly to your new branch office You have configured a new group persona for the new branch office devices in Central, but you do not know their MAC addresses or serial numbers The office manager is instructed via text message on their smartphone to onboard all the new hardware into Aruba Central.
What application must the office manager use on their phone to complete this task?
A. Aruba Central App
B. Aruba Onboard App
C. Aruba installer App
D. Aruba CX Mobile App
Answer: A (LEAVE A REPLY)

NEW QUESTION: 114
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 (LEAVE A REPLY)
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. Reference: 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: 115
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: (SHOW ANSWER)
Explanation
Key Management is a service that runs on Aruba Mobility Controllers (MCs) or Mobility Master (MM) to optimize roaming performance for wireless clients. Key Management works with AirMatch, a service that optimizes radio resource management for Aruba APs, to pre-generate and distribute R1 keys for neighboring APs before a client roams. When a wireless device is roaming from AP1 to AP2, the following steps are part of the Key Management workflow3:
* The client associates and authenticates with AP1 using 802.1X or PSK methods.
* The Key Management service caches the client's information and generates an R0 key for the client.
* The Key Management service receives a list of all AP1's neighbors from AirMatch.
* The Key Management service then generates R1 keys for AP1's neighbors using the R0 key and sends them to the corresponding APs.
* When the client roams to AP2, one of AP1's neighbors, it performs an 802.11r fast transition using the pre-generated R1 key without needing to re-authenticate.
References: 3 https://www.arubanetworks.com/assets/tg/TB_KeyManagement.pdf

NEW QUESTION: 116
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: D (LEAVE A REPLY)
Explanation
VPN Concentrator is the device persona that is only available when configuring a Gateway-only group on AOS10 Gateways. A device persona defines the role and functionality of a Gateway in a

network. A Gateway-only group is a group that contains only Gateways and no APs. A VPN Concentrator persona enables a Gateway to terminate VPN tunnels from remote APs or clients and provide secure access to corporate resources. The other options are incorrect because they are either not device personas or not exclusive to Gateway-only groups. References: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/gateways/gatewa
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/gateways/vpn-co

NEW QUESTION: 117
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: (SHOW ANSWER)
A). a network that uses tunnels to connect two areas - This is not the standard definition of a transit network in OSPF. While tunnels can be used in OSPF for various purposes (e.g., OSPF virtual links), they are not specifically what defines a transit network.
B). a special network that connects two different areas - While an OSPF network might connect two areas, particularly if it's an Area Border Router (ABR), this doesn't define what a transit network is. Any OSPF-enabled network segment where routers form adjacencies and forward data can be a transit network, irrespective of areas.
D). a network that connects to a different routing protocol - This is describing a boundary where OSPF interfaces with another routing protocol, typically managed using redistribution. This isn't what defines a transit network in OSPF.

NEW QUESTION: 118
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: B (LEAVE A REPLY)
OSPF is a link-state routing protocol that divides a network into areas. An area is a logical grouping of routers that share the same link-state information. Area 0 is the backbone area that connects all other areas. A transit network is a special network that connects two different areas. A transit network must belong to Area 0 and have at least two OSPF routers attached to it. A transit network allows traffic from one area to pass through another area without changing the area ID.

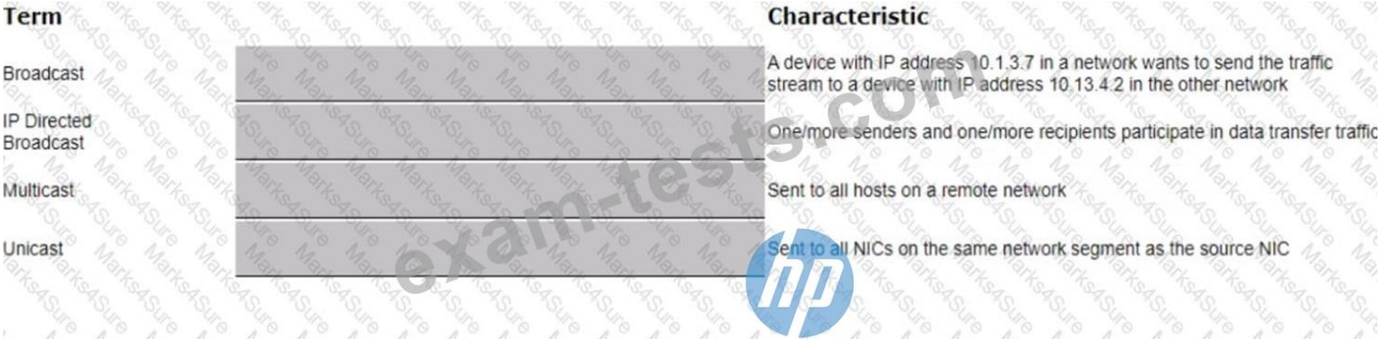
NEW QUESTION: 119
your customer has asked you to assign a switch management role for a new user The customer requires the user role to View switch configuration information and have access to the PUT and POST meth0ds for REST API.
Which default AOS-CX user role meets these requirements?
A. helpdesk
B. administrators
C. auditors
D. sysops
Answer: B (LEAVE A REPLY)

NEW QUESTION: 120
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 (LEAVE A REPLY)
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

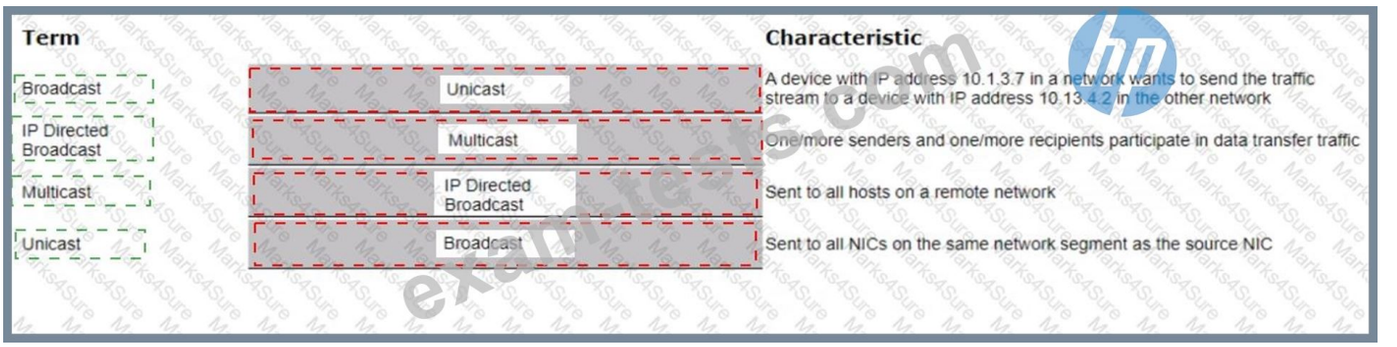
NEW QUESTION: 121
your customer has asked you to assign a switch management role for a new user The customer requires the user role to View switch configuration information and have access to the PUT and POST meth0ds for REST API.
Which default AOS-CX user role meets these requirements?
A. administrators
B. auditors
C. sysops
D. helpdesk
Answer: C (LEAVE A REPLY)
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: 122
Match the terms below to their characteristics (Options may be used more than once or not at all.)



Answer:



Explanation

a) A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address

10.13.4.2 in the other network -> Unicast

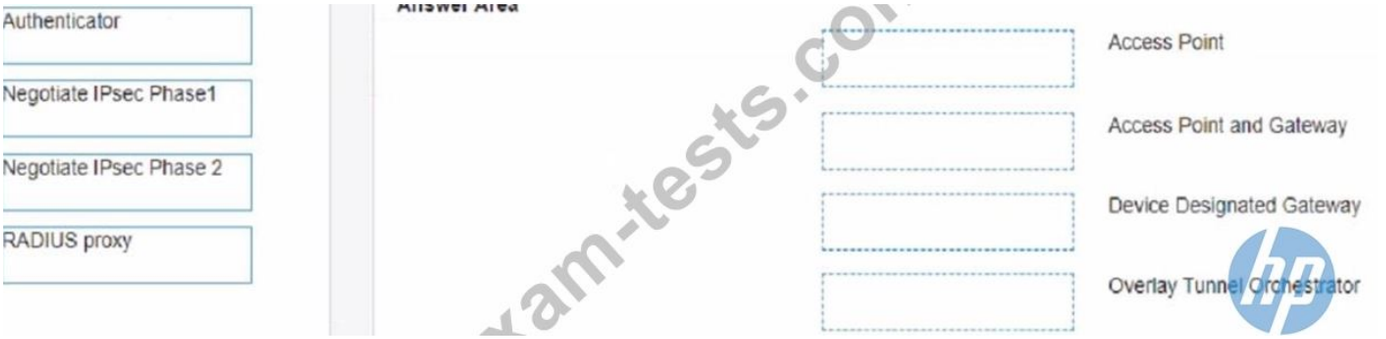
b) One/more senders and one/more recipients participate in data transfer traffic -> Multicast c) Sent to all hosts on a remote network -> IP Directed Broadcast d) Sent to all NICs on the same network segment as the source NIC -> Broadcast References: 1 https://www.thestudygenius.com/unicast-broadcast-multicast/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

A screenshot of a computer Description automatically generated with medium confidence

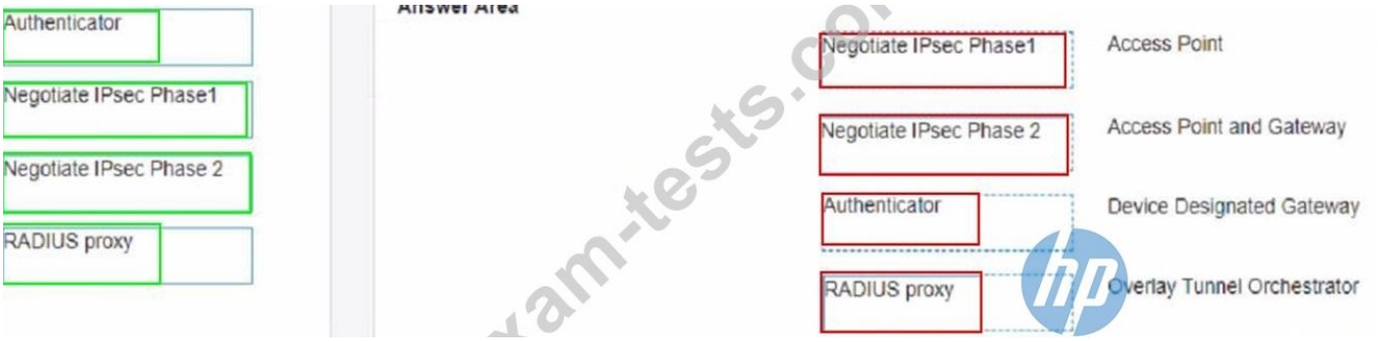
Term	Definition	Example
Broadcast	One-to-all communication, where data is sent to every device on the network	A device with IP address 10.1.3.7 sends a DHCP request to 255.255.255.255
IP Directed Broadcast	One-to-all communication, where data is sent to all hosts on a remote network	A device with IP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

NEW QUESTION: 123

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.)



Answer:



NEW QUESTION: 124

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 (LEAVE A REPLY)

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 Central.

NEW QUESTION: 125

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: (SHOW ANSWER)

Explanation

NAE agents are software components that run on Aruba CX switches to monitor various aspects of network health and performance. NAE agents use NAE scripts to define what data to collect, how to analyze it, and what actions to take when certain conditions are met. A single NAE script can be used by multiple NAE agents on different switches or even different switch stacks. However, NAE scripts must be reviewed and signed by Aruba before being used on production switches. This is to ensure that the scripts are safe, secure, and compliant with Aruba standards.
References:
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D

NEW QUESTION: 126
With the Aruba CX 6100 48G switch with uplinks of 1/1/47 and 1/1/48. how do you automate the process of resuming the port operational state once a loop on a client port is cleared?
A. Configure int 1/1/1-1/1/52 loop-protect disable timer.
B. Configure global loop-protect disable timer.
C. Configure int 1/1/1-1/1/46 loop-protect re-enable-timer.
D. Configure global loop-protect re-enable-timer.
Answer: C (LEAVE A REPLY)
Loop protection is a feature that detects and prevents loops in layer 2 networks. Loop protection can be enabled on ports, LAGs, or VLANs. When loop protection is enabled, the switch sends periodic loop protection messages on the interface and expects to receive them back. If a loop protection message is received back on the same interface, it indicates a loop and the switch takes an action to disable the interface or block traffic on it3. The loop-protect re-enable-timer command is used to configure the length of time the switch waits before re-enabling an interface that was disabled due to loop detection. The default value is 0, which means that the interface remains disabled until manually re-enabled3. To automate the process of resuming the port operational state once a loop on a client port is cleared, the loop-protect re-enable-timer command can be used with a non-zero value on the interface range that includes the client ports3. Therefore, answer C is correct.

NEW QUESTION: 127
A customer wants to enable wired authentication across all their CX switches One of the requirements is that the switch must be able to authenticate a single computer connected through a VoIP phone.
Which feature should be enabled to support this requirement?
A. Multi-Domain Authentication
B. Device-Based Mode

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

NEW QUESTION: 128
you need to have different routing-table requirements With Aruba CX 6300 VSF configuration. Assuming the correct layer-2 VLAN already exists, how would you create a new SVI for a separate routing table?
A. create a new VLAN, and attach the VRF to it.
B. Create a new routing table, and attach VLANS to it
C. Create a new SVI and use attach command.
D. Create a new VLAN. and attach the routing table to it
Answer: C (LEAVE A REPLY)
The correct answer is C. Create a new SVI and use attach command.
To create a new SVI for a separate routing table, you need to use the attach command to associate the SVI with a VRF (Virtual Routing and Forwarding) instance. A VRF is a logical entity that allows multiple routing tables to coexist on the same switch. Each VRF has its own set of interfaces, routing protocols, and routes that are isolated from other VRFs.
According to the AOS-CX Virtual Switching Framework (VSF) Guide1, one of the steps to configure VRF- aware VSF is:
* Configure the VRFs on each member switch and assign the SVIs to the respective VRFs using the attach command. For example:
switch(config)# vrf red
switch(config-vrf)# exit
switch(config)# interface vlan 10
switch(config-if-vlan)# ip address 10.1.1.1/24
switch(config-if-vlan)# attach vrf red

The above commands create a VRF named red and assign VLAN 10 SVI to it. The SVI has an IP address of
10.1.1.1/24.
The other options are incorrect because:
* A. You cannot attach a VRF to a VLAN directly. You need to create an SVI for the VLAN and then attach the VRF to the SVI.
* B. You cannot create a new routing table manually. You need to create a VRF and then use routing protocols or static routes to populate the routing table for the VRF.
* D. You cannot attach a routing table to a VLAN directly. You need to create an SVI for the VLAN and then attach a VRF that has a routing table associated with it.

NEW QUESTION: 129
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 10.105.43.1/24
ipv6 address fd00:5708::f02d:4df6/64
vrf attach eng
```

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

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 130

Select the Aruba stacking technology matching each option (Options may be used more than once or not at all.)

Answer:

Explanation:

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

b) Support two devices per stack -> VSX

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

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

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

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