HP.HPE7-A01.v2023-08-15.q35

Exam Code:	HPE7-A01
Exam Name:	Aruba Certified Campus Access Professional Exam
Certification Provider:	HP
Free Question Number:	35
Version:	v2023-08-15
# of views:	833
# of Questions views:	350
https://www.freepdfdumps.com/HP.HPE7-A01.v2023-08-15.q35.html	

NEW QUESTION: 1
You are troubleshooting an issue with a pair of Aruba CX 8360 switches configured with VSX Each switch has multiple VRFs. You need to find the IP address of a particular client device with a known MAC address You run the "show arp" command on the primary switch in the pair but do not find a matching entry for the client MAC address.
The client device is connected to an Aruba CX 6100 switch by VSX LAG.
Which action can be used to find the IP address successfully?

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

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

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

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

Answer: B (LEAVE A REPLY)
Explanation
The show arp command displays the ARP table for a specific VRF or all VRFs on the switch. The ARP table contains the IP address to MAC address mappings for hosts that are directly connected to the switch or reachable through a gateway. If the client device is connected to another switch by VSX LAG, the ARP entry for the client device will not be present on the primary switch unless it has communicated with it recently.
Therefore, to find the IP address of the client device, the administrator should run the show arp command on the secondary switch in the VSX pair, specifying the VRF name that contains the client device's subnet.
References:

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

NEW QUESTION: 2
With the Aruba CX switch configuration, what is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation?
A. Active Gateway
B. Active-Active VRRP
C. SVI with vsx-sync
D. VRRP
Answer: A (LEAVE A REPLY)
Explanation
Active Gateway is the first-hop protocol feature that is used for VSX L3 gateway as per Aruba recommendation. Active Gateway is a feature that allows both VSX peers to act as active gateways for different subnets, eliminating the need for VRRP or other first-hop redundancy protocols. Active Gateway also provides fast failover and load balancing for L3 traffic across the VSX peers. The other options are incorrect because they are either not recommended or not supported by Aruba CX VSX. References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html
https://www.arubanetworks.com/resource/aruba-virtual-switching-extension-vsx/

NEW QUESTION: 3
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: (SHOW ANSWER)
Explanation
To onboard a new UXI in an existing environment with 802.1X authentication, you need to use the UXI app on your smartphone and connect the UXI via Bluetooth. The UXI app allows you to scan the QR code on the UXI sensor and configure its network settings, such as SSID, password, IP address, etc. The Bluetooth connection allows you to communicate with the UXI sensor without requiring any network access or cellular connection. The other options are incorrect because they either do not use the UXI app or do not use Bluetooth. References:
https://www.arubanetworks.com/products/network-management-operations/analytics-monitoring/user-experienc
https://help.centralon-prem.arubanetworks.com/2.5.4/documentation/online_help/content/nms-on-prem/aos-cx/g

NEW QUESTION: 4
You need lo 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 OSPF configuration for a separate routing table?
A. Create a new OSPF area, and attach VRF name.
B. Create a new OSPF process ID with vrf name.
C. Attach a new OSFP process ID with a custom routing table
D. Attach OSPF process ID in the VRF configuration.
Answer: B (LEAVE A REPLY)
Explanation
To create a new OSPF configuration for a separate routing table, you need to create a new OSPF process ID with vrf name. This will create a new OSPF instance that is associated with the specified VRF and its routing table. The other options are incorrect because they either do not create a new OSPF instance or do not associate it with a VRF. References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html

NEW QUESTION: 5
A company deployed Dynamic Segmentation with their CX switches and Gateways After performing a security audit on their network, they discovered that the tunnels built between the CX switch and the Aruba Gateway are not encrypted. The company is concerned that bad actors could try to insert spoofed messages on the Gateway to disrupt communications or obtain information about the network.
Which action must the administrator perform to address this situation?
A. Enable Secure Mode Enhanced
B. Enable Enhanced security
C. Enable Enhanced PAPI security
D. Enable GRE security
Answer: (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

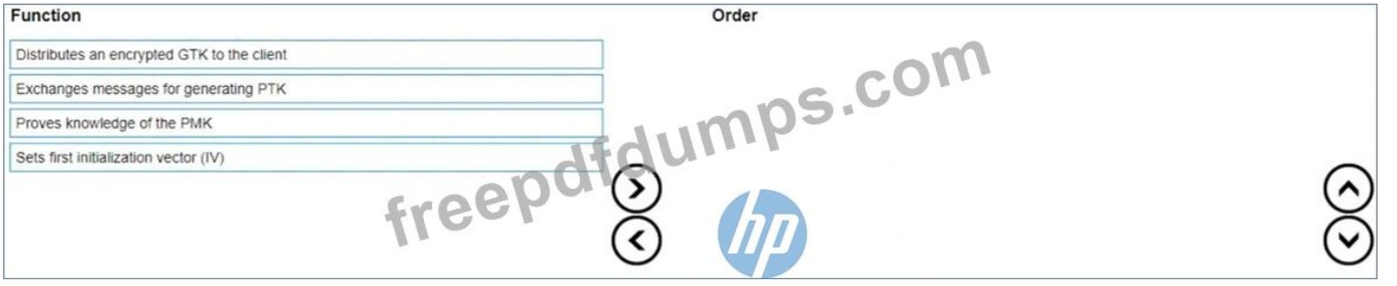
NEW QUESTION: 6

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

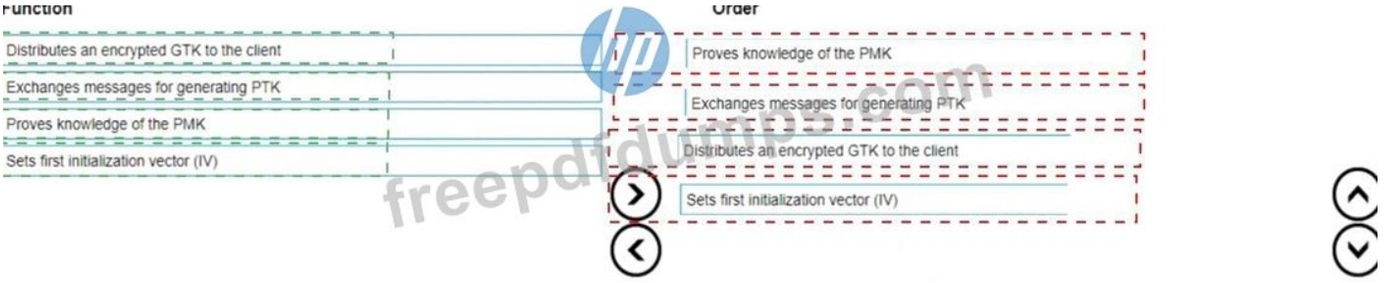
NEW QUESTION: 7
What are two advantages of splitting a larger OSPF area into a number of smaller areas? (Select two)
A. It extends the LSDB
B. It increases stability
C. it simplifies the configuration.
D. It reduces processing overhead.
E. It reduces the total number of LSAs
Answer: B,D (LEAVE A REPLY)
Explanation
Splitting a larger OSPF area into a number of smaller areas has several advantages for network scalability and performance. Some of these advantages are:
* It increases stability by limiting the impact of topology changes within an area. When a link or router fails in an area, only routers within that area need to run the SPF algorithm and update their routing tables. Routers in other areas are not affected by the change and do not need to recalculate their routes.

* It reduces processing overhead by reducing the size and frequency of link-state advertisements (LSAs).
LSAs are packets that contain information about the network topology and are flooded within an area.
By dividing a network into smaller areas, each area has fewer LSAs to generate, store, and process,
* which saves CPU and memory resources on routers.
* It reduces bandwidth consumption by reducing the amount of routing information exchanged between areas. Routers that connect different areas, called area border routers (ABRs), summarize the routing information from one area into a single LSA and advertise it to another area. This reduces the number of LSAs that need to be transmitted across area boundaries and saves network bandwidth.
References: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html

NEW QUESTION: 8
List the WPA 4-Way Handshake functions in the correct order.



Answer:



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

NEW QUESTION: 9
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)
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: 10
You are deploying a bonded 40 MHz wide channel What is the difference in the noise floor perceived by a client using this bonded channel as compared to an unbonded 20MHz wide channel?
A. 2dB
B. 3dB
C. 8dB
D. 4dB
Answer: B (LEAVE A REPLY)
Explanation
The difference in the noise floor perceived by a client using a bonded 40 MHz wide channel as compared to an unbonded 20 MHz wide channel is 3 dB. The noise floor is the level of background noise in a given frequency band. When two adjacent channels are bonded, the noise floor increases by 3 dB because the bandwidth is doubled and more noise is captured. The other options are incorrect because they do not reflect the correct relationship between bandwidth and noise floor. 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/channel-b

NEW QUESTION: 11

In an ArubaOS 10 architecture using an AP and a gateway, what happens when a client attempts to join the network and the WLAN is configured with OWE?

A. Authentication information is not exchanged

B. The Gateway will not respond.

C. No encryption is applied.

D. RADIUS protocol is utilized.

Answer: A (LEAVE A REPLY)

Explanation

This is the correct statement about what happens when a client attempts to join the network and the WLAN is configured with OWE (Opportunistic Wireless Encryption). OWE is a standard that provides encryption for open networks without requiring any authentication or credentials from the client or the network. OWE uses a Diffie-Hellman key exchange mechanism to establish a secure session between the client and the AP without exchanging any authentication information. The other options are incorrect because they either describe scenarios that require authentication or encryption methods that are not used by OWE. References:

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

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

NEW QUESTION: 12

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)

Explanation

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

Authentication survivability enables the Gateway cluster to cache successful authentication requests from the RADIUS server and use them to authenticate clients when the RADIUS server is unreachable. Authentication survivability also allows clients to use MAC caching or MAC authentication bypass (MAB) methods to access the network when the RADIUS server is down. References:

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

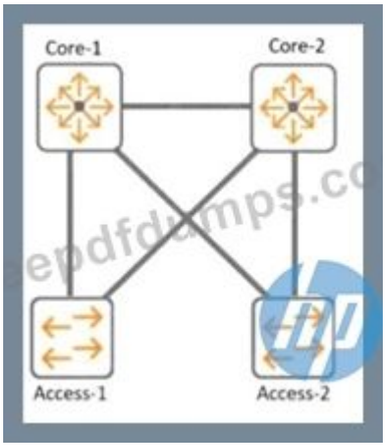
NEW QUESTION: 13

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)
Explanation
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: 14
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: (SHOW ANSWER)

Explanation

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: 15

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)

Explanation

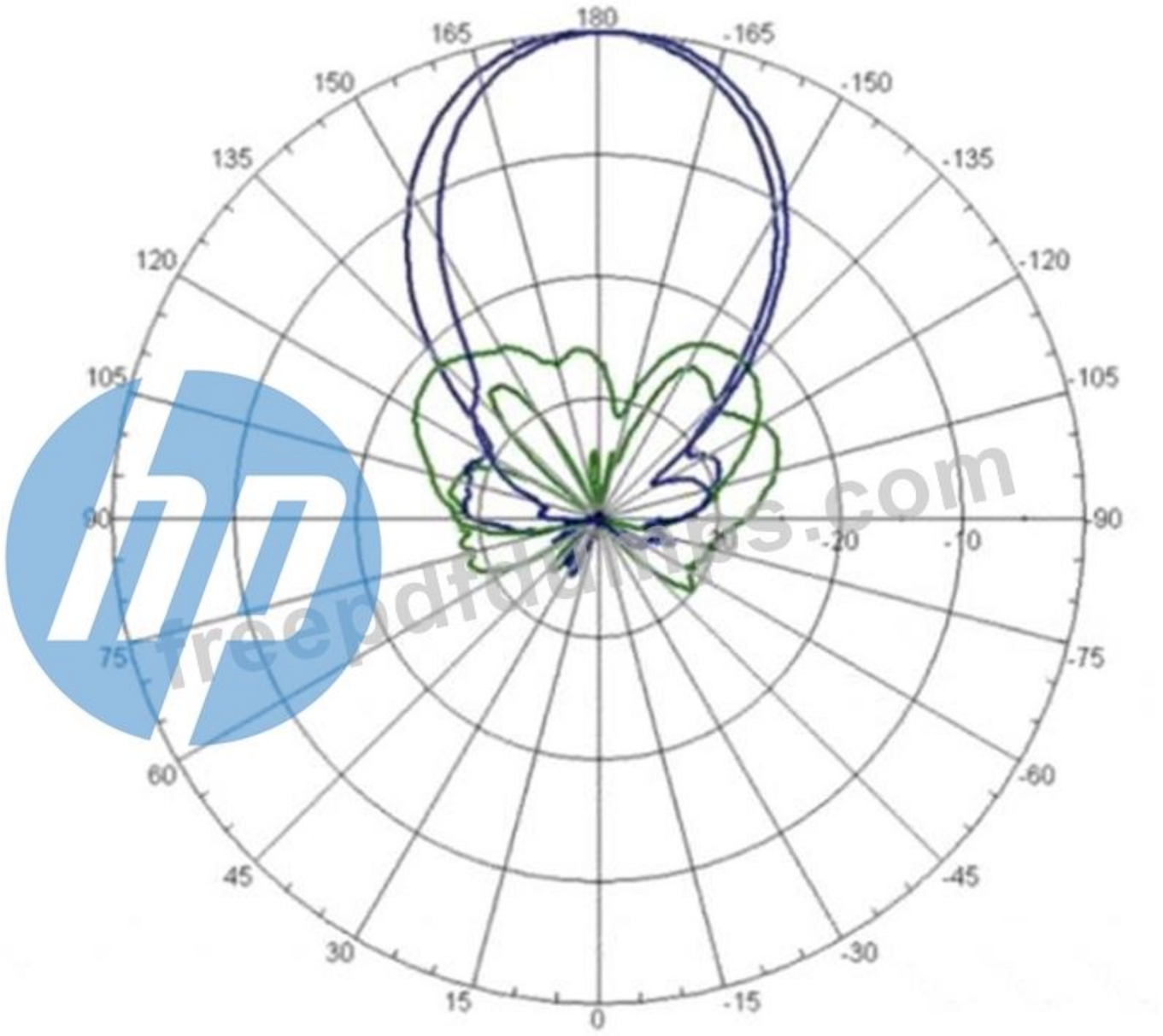
Encryption is a feature supported by SNMPv3 that provides an advantage over SNMPv2c. Encryption protects the confidentiality and integrity of SNMP messages by encrypting them with a secret key. SNMPv2c does not support encryption and relies on community strings for authentication and authorization, which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

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmp.htm

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmpv3.htm

NEW QUESTION: 16

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: 17
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: 18
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)
Explanation
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. 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: 19
In AOS 10. which session-based ACL below will only allow ping from any wired station to wireless clients but will not allow ping from wireless clients to wired stations"? The wired host ingress traffic arrives on a trusted port.
A. ip access-list session pingFromWired any user any permit
B. ip access-list session pingFromWired user any svc-icmp deny any any svc-icmp permit
C. ip access-list session pingFromWired any any svc-icmp permit user any svc-icmp deny
D. ip access-list session pingFromWired any any svc-icmp deny any user svc-icmp permit
Answer: D (LEAVE A REPLY)
Explanation
A session-based ACL is applied to traffic entering or leaving a port or VLAN based on the direction of the session initiation. To allow ping from any wired station to wireless clients but not vice versa, a session-based ACL should be used to deny icmp echo traffic from any source to any destination, and then permit icmp echo-reply traffic from any source to user destination. The user role represents wireless clients in AOS 10.
References:
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D
https://techhub.hpe.com/eginfolib/networking/docs/arubaos-switch/security/GUID-EA0A5B3C-FE4C-4B9B-BE

NEW QUESTION: 20
Which Aruba AP mode is sending captured RF data to Aruba Central for waterfall plot?
A. Hybrid Mode
B. Air Monitor
C. Spectrum Monitor

D. Dual Mode

Answer: C (LEAVE A REPLY)

Explanation

Spectrum Monitor is an Aruba AP mode that is sending captured RF data to Aruba Central for waterfall plot.

Spectrum Monitor is a mode that allows an AP to scan all channels in both 2.4 GHz and 5 GHz bands and collect information about the RF environment, such as interference sources, noise floor, channel utilization, etc. The AP then sends this data to Aruba Central, which is a cloud-based network management platform that can display the data in various formats, including waterfall plot. Waterfall plot is a graphical representation of the RF spectrum over time, showing the frequency, amplitude, and duration of RF signals. The other options are incorrect because they are either not AP modes or not sending RF data to Aruba Central. References:

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/spect

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/water

https://www.arubanetworks.com/products/network-management-operations/aruba-central/

NEW QUESTION: 21

A customer has a large number of food-producing machines

* All machines are connected via Aruba CX6200 switches in VLANs 100.110. and 120
* Several external technicians are maintaining this special equipment

What are the correct commands to ensure that no rogue DHCP server will impact the network?

A.

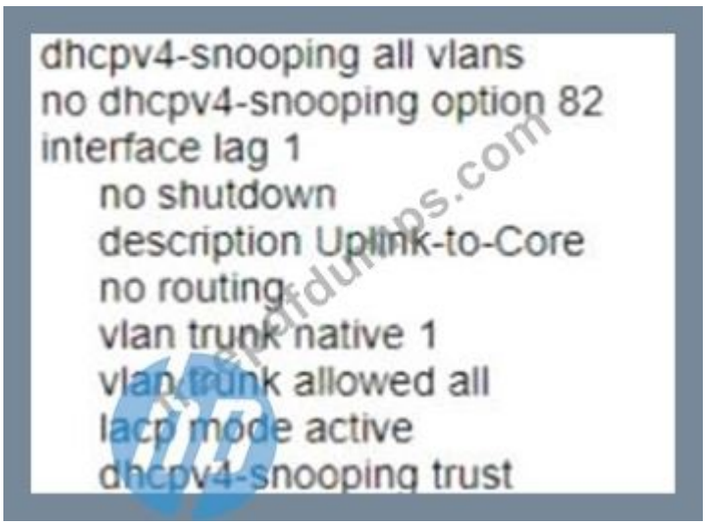
```
dhcp-snooping enable
no dhcp-snooping option 82
dhcp-snooping vlan 100-120
vlan 100
    name cornflakes
vlan 110
    name cornmill
vlan 120
    name packaging

interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcp-snooping trust
```

B.

```
dhcp snooping enable
no dhcp-snooping option 82
vlan 100
    name cornflakes
    dhcp-snooping
vlan 110
    name cornmill
    dhcp-snooping
vlan 120
    name packaging
    dhcp-snooping
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcp snooping trust
```

C.



D.

Answer: A (LEAVE A REPLY)

Explanation

Option A shows the correct commands to ensure that no rogue DHCP server will impact the network. The commands include the following steps:

* Enable DHCP snooping on the switch. DHCP snooping is a feature that prevents rogue DHCP servers from offering IP addresses to clients by filtering DHCP messages based on trusted and untrusted ports1.

* Configure VLANs 100, 110, and 120 as DHCP snooping VLANs. This means that DHCP snooping will be applied to these VLANs and any untrusted DHCP messages received on these VLANs will be dropped1.
* Configure LAG 1 as a trusted port for DHCP snooping. This means that any DHCP messages received on LAG 1 will be allowed and not filtered by DHCP snooping. LAG 1 is assumed to be connected to a legitimate DHCP server or a router that relays DHCP requests to a legitimate DHCP server1.
Option B is incorrect because it does not enable DHCP snooping on the switch or configure VLANs 100, 110, and 120 as DHCP snooping VLANs. Option C is incorrect because it does not configure LAG 1 as a trusted port for DHCP snooping. Option D is incorrect because it does not enable DHCP snooping on the switch or configure LAG 1 as a trusted port for DHCP snooping.
References: 1
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7

NEW QUESTION: 22
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: (SHOW ANSWER)
Explanation
802.11k is a standard that provides mechanisms for APs and clients to dynamically measure the available radio resources in a wireless network. 802.11k defines radio resource management (RRM) functions, such as neighbor reports, link measurement, beacon reports, etc., that allow APs and clients to exchange information about the RF environment and make better roaming decisions. The other options are incorrect because they describe other standards, such as 802.11r, 802.11v, or 802.11ax. References:
https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

NEW QUESTION: 23
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: C (LEAVE A REPLY)

Explanation

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. References: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch01.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch04.html

NEW QUESTION: 24

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: A (LEAVE A REPLY)

Explanation

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: 25
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
```

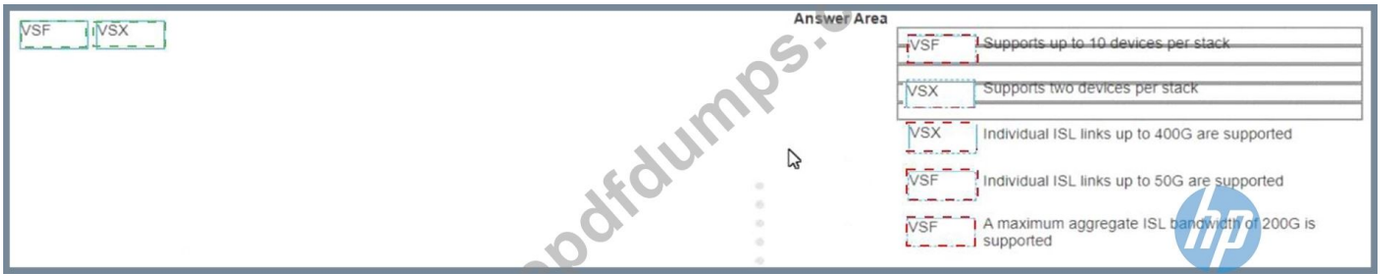
Answer: A,E (LEAVE A REPLY)
Explanation
These are the correct parts of the solution for the requirements of configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network. Option A

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. References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html

NEW QUESTION: 26
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: 27
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

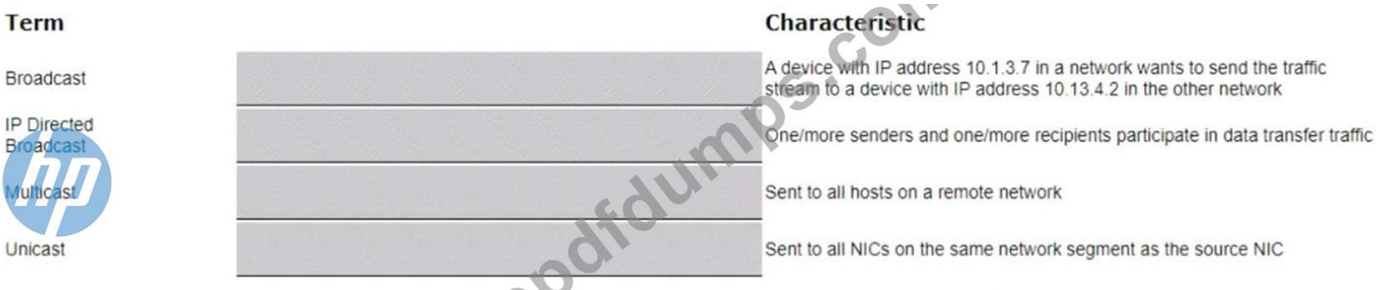
e) A maximum aggregate ISL bandwidth of 200G is supported -> VSF

References: 1

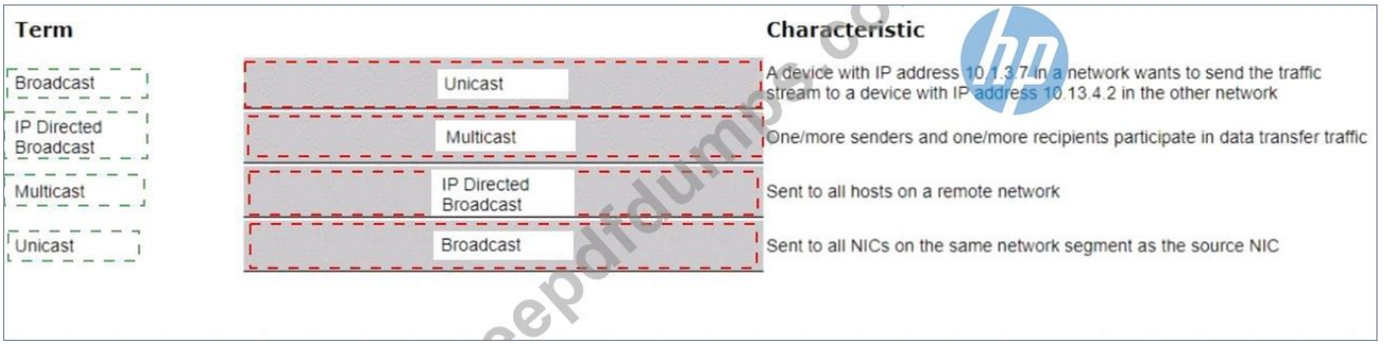
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/GUID-2E425DAE-EC54-4313-9D

NEW QUESTION: 28

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: 29
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.

Answer: (SHOW ANSWER)

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: 30

You are helping an onsite network technician bring up an Aruba 9004 gateway with ZTP for a branch office The technician was to plug in any port for the ZTP process to start Thirty minutes after the gateway was plugged in new users started to complain they were no longer able to get to the internet. One user who reported the issue stated their IP address is 172.16 0.81 However, the branch office network is supposed to be on 10.231 81.0/24.

What should the technician do to alleviate the issue and get the ZTP process started correctly?

A. Turn off the DHCP scope on the gateway, and set DNS correctly on the gateway to reach Aruba Activate

B. Move the cable on the gateway from port G0/0V1 tc port GO 0.0

C. Move the cable on the gateway to G0/0/1. and add the device's MAC and Serial number in Central

D. Factory default and reboot the gateway to restart the process.

Answer: C (LEAVE A REPLY)

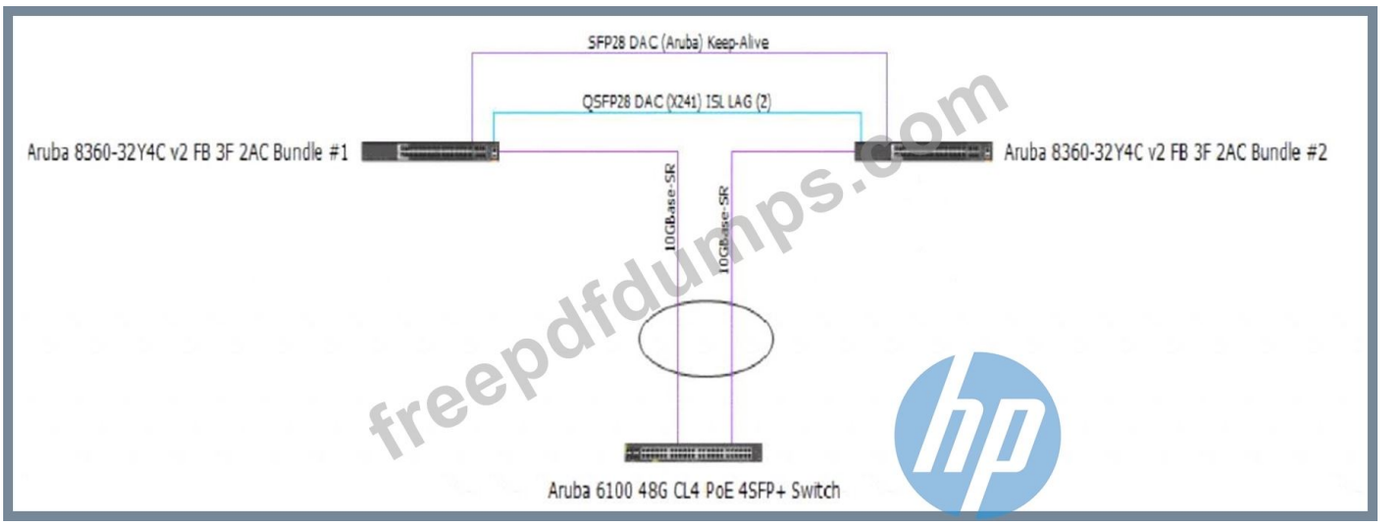
Explanation

This is the correct action to alleviate the issue and get the ZTP (Zero Touch Provisioning) process started correctly for an Aruba 9004 gateway. ZTP is a feature that allows an Aruba gateway to automatically download its configuration from Aruba Central without any manual intervention. To use ZTP, the gateway must be connected to a DHCP-enabled network and have Internet access. The gateway must also be added to Aruba Central using its MAC address and serial number. The default port for ZTP on an Aruba 9004 gateway is G0/0/1, which is labeled as Internet on the

device. The other options are incorrect because they either do not use the correct port for ZTP or do not add the device to Aruba Central. References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/gateways/ztp.htm
https://www.arubanetworks.com/assets/tg/TB_ArubaGateway.pdf

NEW QUESTION: 31
With Aruba CX 6300. how do you configure ip address 10 10 10 1 for the interface in default state for interface 1/1/1?
A. int 1/1/1. switching, ip address 10 10 10 1/24
B. int 1/1/1. no switching, ip address 10 10 10.1/24
C. int 1/1/1. ip address 10.10.10.1/24
D. int 1/1/1. routing, ip address 10.10.10 1/24
Answer: B (LEAVE A REPLY)
Explanation
To configure an IP address for an interface in default state for interface 1/1/1 on Aruba CX 6300 switch, you need to disable switching on the interface first with the command no switching. Then you can assign an IP address with the command ip address. The other options are incorrect because they either do not disable switching or use invalid keywords such as switching or routing. References:
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch01.html
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html

NEW QUESTION: 32
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: B (LEAVE A REPLY)

Explanation

Option B is the correct action that may help fix the issue of sporadic DHCP behavior across clients attached to the CX 6100 switch. Option B enables DHCP relay on VLAN 1000 interface on Core-1 switch, which allows DHCP requests from clients in VLAN 1000 to be forwarded to the DHCP server in a different subnet (10.200.1.100). Without DHCP relay, clients in VLAN 1000 cannot obtain IP addresses from the DHCP server because they are in different broadcast domains. The other options are incorrect because they either do not enable DHCP relay or do not configure it correctly. References:

https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html

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

NEW QUESTION: 33
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)
Explanation
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: 34
You need to ensure that voice traffic sent through an ArubaOS-CX switch arrives with minimal latency What is the best scheduling technology to use for this task?
A. Strict queuing
B. Rate limiting
C. QoS shaping
D. DWRR queuing
Answer: (SHOW ANSWER)
Explanation
Strict queuing is the best scheduling technology to use for voice traffic on an AOS-CX switch. Scheduling is a mechanism that determines how packets are transmitted from different queues on an egress port. Strict queuing is a scheduling method that gives the highest priority queue absolute preference over all other queues, regardless of their size or utilization. Voice traffic should be assigned to the highest priority queue and scheduled with strict queuing to ensure minimal latency and jitter. The other options are incorrect because they are either not scheduling methods or not optimal for voice traffic. References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html

NEW QUESTION: 35

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

A. 802.11ah

B. 802.11mc

C. 802.11be

D. 802.11V

Answer: (SHOW ANSWER)

Explanation

802.11mc is a standard that uses Round Trip Time (RTT) and Fine Time Measurements (FTM) to calculate the distance a client is from an AP. 802.11mc defines a protocol for exchanging FTM frames between an AP and a client, which contain timestamps that indicate when the frames were transmitted and received. By measuring the RTT of these frames, the AP or the client can estimate their distance based on the speed of light. The other options are incorrect because they either do not use RTT or FTM or do not exist as standards. References:

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

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