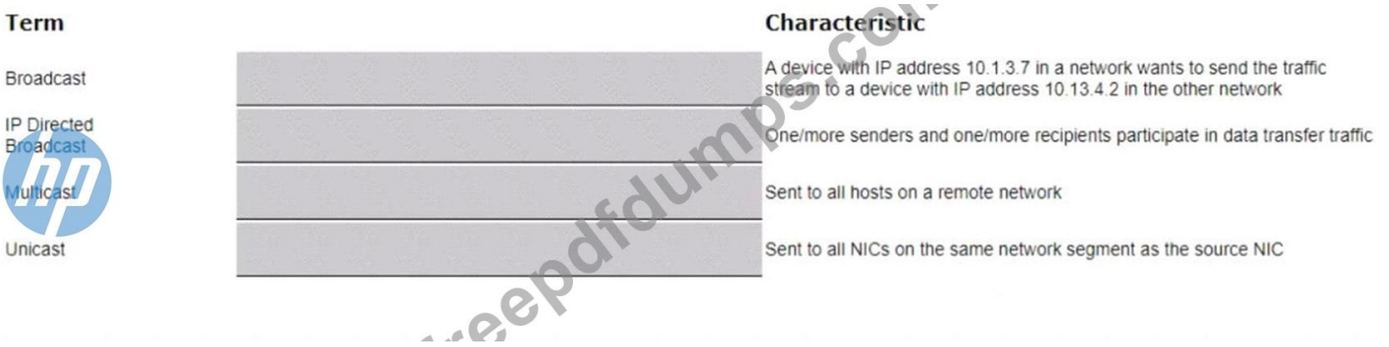
HP.HPE7-A01.v2023-09-15.q32

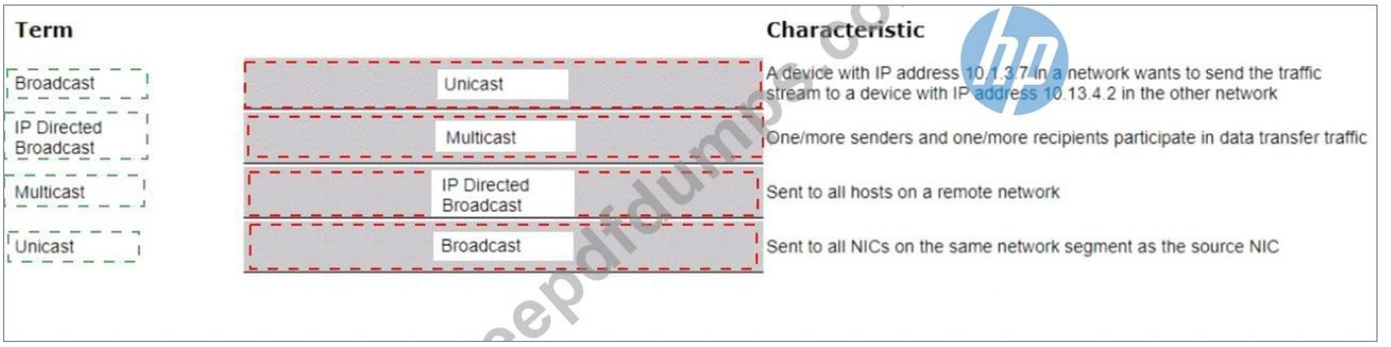
Exam Code:	HPE7-A01
Exam Name:	Aruba Certified Campus Access Professional Exam
Certification Provider:	HP
Free Question Number:	32
Version:	v2023-09-15
# of views:	755
# of Questions views:	320
https://www.freepdfdumps.com/HP.HPE7-A01.v2023-09-15.q32.html	

NEW QUESTION: 1

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: 2
What is a primary benefit of BSS coloring?
A. BSS color tags improve performance by allowing clients on the same channel to share airtime.
B. BSS color tags are applied to client devices and can reduce the threshold for interference
C. BSS color tags are applied to Wi-Fi channels and can reduce the threshold for interference
D. BSS color tags improve security by identifying rogue APs and removing them from the network.
Answer: B (LEAVE A REPLY)
Explanation
This is the correct definition of BSS coloring and its primary benefit. BSS coloring is a mechanism that assigns a color code to each BSS (Basic Service Set), which consists of an AP and its associated clients. The color code is added to the PHY header of each frame transmitted by the AP or the client. BSS coloring helps reduce co-channel interference by allowing devices to differentiate between frames from their own BSS and frames from neighboring BSSs that use the same channel. Devices can then adjust their threshold for interference based on the color code and decide whether to transmit or defer based on the channel status. The other options are incorrect because they either describe different mechanisms or benefits of BSS coloring or use incorrect terms. References:
https://www.commscope.com/blog/2018/wi-fi-6-fundamentals-basic-service-set-coloring-bss-coloring/
https://www.techtarget.com/searchnetworking/answer/How-will-BSS-coloring-boost-Wi-Fi-6-performance

NEW QUESTION: 3
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: 4
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.

```
dhcpv4-snooping all vlans
no dhcpv4-snooping option 82
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcpv4-snooping trust
```

D.

```
dhcpv4-snooping
no dhcpv4-snooping option 82
vlan 100
    name cornflakes
    dhcpv4-snooping
vlan 110
    name cornmill
    dhcpv4-snooping
vlan 120
    name packaging
    dhcpv4-snooping
interface lag 1
    no shutdown
    description Uplink-to-Core
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    dhcpv4-snooping trust
```

Answer: (SHOW ANSWER)

Explanation

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

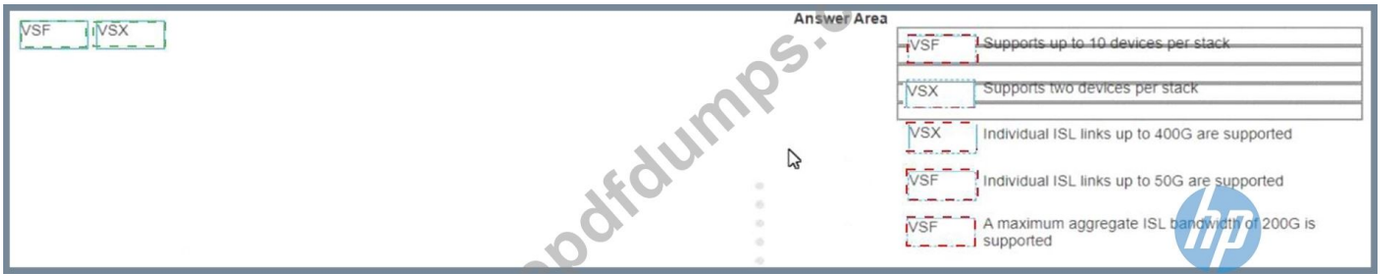
* Enable DHCP snooping on the switch. DHCP snooping is a feature that prevents rogue DHCP servers from offering IP addresses to clients by filtering DHCP messages based on trusted and untrusted ports1.

* 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: 5
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: (SHOW ANSWER)
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: 6
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: 7

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

A. Voice VLANs can be automatically configured for VoIP phones

B. APs can request power as needed from PoE-enabled switch ports

C. iSCSI client devices can request to have flow control enabled

D. GVRP VLAN information can be used to dynamically add VLANs to a trunk

E. iSCSI client devices can set the required MTU setting for the port.

Answer: A,B (LEAVE A REPLY)

Explanation

These are two benefits enabled by LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery).

LLDP-MED is an extension of LLDP that provides additional capabilities for network devices such as VoIP phones and APs. One of the capabilities is to automatically configure voice VLANs for VoIP phones, which allows them to be placed in a separate VLAN from data devices and receive QoS and security policies.

Another capability is to request power as needed from PoE-enabled switch ports, which allows APs to adjust their power consumption and performance based on the available power budget.

The other options are incorrect because they are either not enabled by LLDP-MED or not related to LLDP-MED. References:

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

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

NEW QUESTION: 8
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)
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: 9
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: 10

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: A (LEAVE A REPLY)

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: 11

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: A,D (LEAVE A REPLY)

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: 12
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: 13
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: 14

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: 15
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)
Explanation
These are the correct requirements to ensure that WMM (Wi-Fi Multimedia) is working effectively. WMM is a standard that provides quality of service (QoS) for wireless networks by prioritizing traffic into four categories: voice, video, best effort, and background. To use WMM, both the APs and the controller must be Wi-Fi CERTIFIED for WMM, which means they have passed interoperability tests and comply with the standard. WMM must also be enabled on the APs and the controller, which is usually the default setting. The client device must also be Wi-Fi

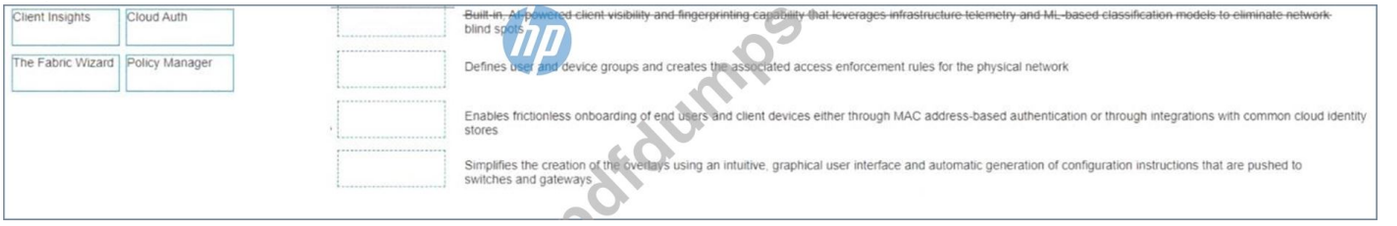
CERTIFIED for WMM and configured for WMM marking, which means it can tag its traffic with the appropriate priority level based on the application type. The other options are incorrect because they are either not related to WMM or not required for WMM to work. References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-qos/wmm.h
https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm

NEW QUESTION: 16
A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working to a remote site connected via layer-3 All legacy devices are connected to a dedicated Aruba CX 6200 switch at each site.
What technology on the Aruba CX 6200 could be used to meet this requirement?
A. Inclusive Multicast Ethernet Tag (IMET)
B. Ethernet over IP (EoIP)
C. Generic Routing Encapsulation (GRE)
D. Static VXLAN
Answer: (SHOW ANSWER)
Explanation
VXLAN is a technology that can be used to meet the requirement of using a legacy application that communicates at layer-2 across a layer-3 network. Static VXLAN is a feature that allows the creation of layer-2 overlay networks over a layer-3 underlay network using VXLAN tunnels. Static VXLAN does not require any control plane protocol or VTEP discovery mechanism, and can be configured manually on the Aruba CX 6200 switches. The other options are incorrect because they either do not support layer-2 communication over layer-3 network or are not supported by Aruba CX 6200 switches. References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html

NEW QUESTION: 17
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: 18
Match the solution components of NetConductor (Options may be used more than once or not at all.)



Answer:

Explanation
Client Insights matches with Built in , AI powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML based classification models to eliminate network bling spots Client Insights is a solution component of NetConductor that provides built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots. Client Insights uses machine learning to automatically detect, identify, and classify devices on the network, such as IoT devices, BYOD devices, or rogue devices. Client Insights also provides behavioral analytics and anomaly detection to monitor device performance and security posture.
Client Insights helps network administrators gain visibility into the device landscape, enforce granular access policies, and troubleshoot issues faster. References:
https://www.arubanetworks.com/products/network-management-operations/central/netconductor/
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf
Cloud Auth matches with Enables fictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity

stores Cloud Auth is a solution component of NetConductor that enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores. Cloud Auth is a cloud-native network access control (NAC) solution that is delivered via Aruba Central. Cloud Auth allows network administrators to define user and device groups, assign roles and policies, and enforce access control across wired and wireless networks. Cloud Auth supports MAC authentication for devices that do not support 802.1X, as well as integrations with cloud identity providers such as Azure AD, Google Workspace, Okta, etc. References:
https://www.arubanetworks.com/products/network-management-operations/central/netconductor/
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf
The Fabric Wizard matches with Simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways The Fabric Wizard is a solution component of NetConductor that simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways. The Fabric Wizard is a tool that allows network administrators to design, deploy, and manage overlay networks using VXLAN and EVPN protocols. The Fabric Wizard provides a graphical representation of the network topology, devices, and links, and allows users to drag and drop virtual components such as VRFs, VLANs, and subnets. The Fabric Wizard also generates the configuration commands for each device based on the user input and pushes them to the switches and gateways via Aruba Central. References:
https://www.arubanetworks.com/products/network-management-operations/central/netconductor/
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf
Policy Manager matches with Defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network Policy Manager is a solution component of NetConductor that defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network. Policy Manager is a tool that allows network administrators to create and manage network policies based on user and device identities, roles, and contexts. Policy Manager uses Group Policy Identifier (GPID) to carry policy information in traffic for in-line enforcement. Policy Manager also integrates with Cloud Auth, ClearPass, or third-party solutions to provide flexible network access control. References:
https://www.arubanetworks.com/products/network-management-operations/central/netconductor/
https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

NEW QUESTION: 19
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+

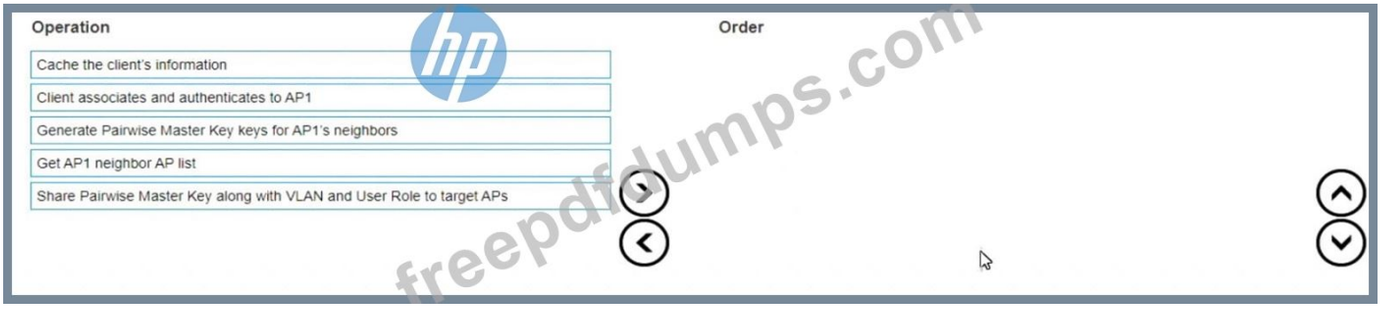
Answer: C (LEAVE A REPLY)
Explanation
UDLD (Unidirectional Link Detection) is the information that the Inter-Switch Link Protocol configuration uses in the configuration created for Aruba CX VSX pair inter-switch-link. UDLD is a protocol that detects unidirectional links between switches and prevents 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: 20
A customer is using Aruba Cloud Guest, but visitors keep complaining that the captive portal page keeps coming up after devices go to sleep Which solution should be enabled to deal with this issue?
A. MAC Caching under the splash page
B. MAC Caching under the user-role
C. Wireless Caching under the splash page
D. MAC Caching under the WLAN
Answer: D (LEAVE A REPLY)
Explanation
This is the correct solution to deal with the issue where visitors keep complaining that the captive portal page keeps coming up after devices go to sleep. MAC Caching is a feature that allows an Aruba Access Point to bypass authentication for devices that have already been authenticated by a captive portal. MAC Caching can be enabled under the WLAN settings in Aruba Cloud Guest by selecting the MAC Caching checkbox and specifying the MAC Caching duration. The other options are incorrect because they either do not exist or do not apply to Aruba Cloud Guest. References:
https://www.arubanetworks.com/techdocs/CloudGuest/Content/Topics/MAC_Caching.htm
https://www.arubanetworks.com/techdocs/CloudGuest/Content/Topics/WLAN.htm

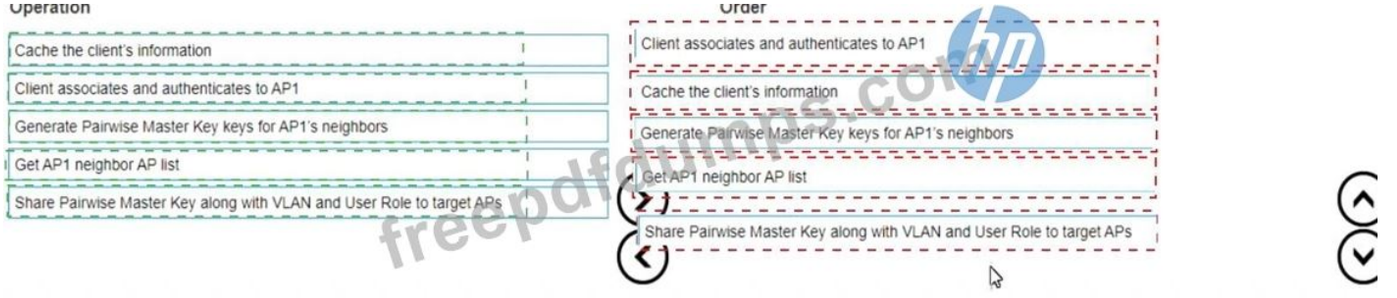
NEW QUESTION: 21
Describe the difference between Class of Service (CoS) and Differentiated Services Code Point (DSCP).
A. CoS is only used to determine CLASS of traffic DSCP is only used to differentiate between different Classes.
B. CoS is only contained in VLAN Tag fields DSCP is in the IP Header and preserved throughout the IP packet flow
C. They are similar and can be used interchangeably.
D. CoS has much finer granularity than DSCP
Answer: B (LEAVE A REPLY)

Explanation
CoS and DSCP are both methods of marking packets for quality of service (QoS) purposes. QoS is a mechanism that allows network devices to prioritize and differentiate traffic based on certain criteria, such as application type, source, destination, etc. CoS stands for Class of Service and is a 3-bit field in the 802.1Q VLAN tag header. CoS can only be used on Ethernet frames that have a VLAN tag, and it can only be preserved within a single VLAN domain. DSCP stands for Differentiated Services Code Point and is a 6-bit field in the IP header. DSCP can be used on any IP packet, regardless of the underlying layer 2 technology, and it can be preserved throughout the IP packet flow, unless it is modified by intermediate devices.
References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mt-book/qos-overview.html
https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html

NEW QUESTION: 22
What is the order of operations tor Key Management service for a wireless client roaming from AP1 to AP2?



Answer:

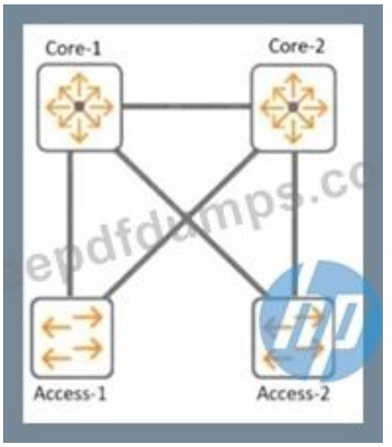


Explanation

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

NEW QUESTION: 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: (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: 24

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: 25

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: (SHOW ANSWER)

Explanation

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.

References: 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: 26

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)

Explanation

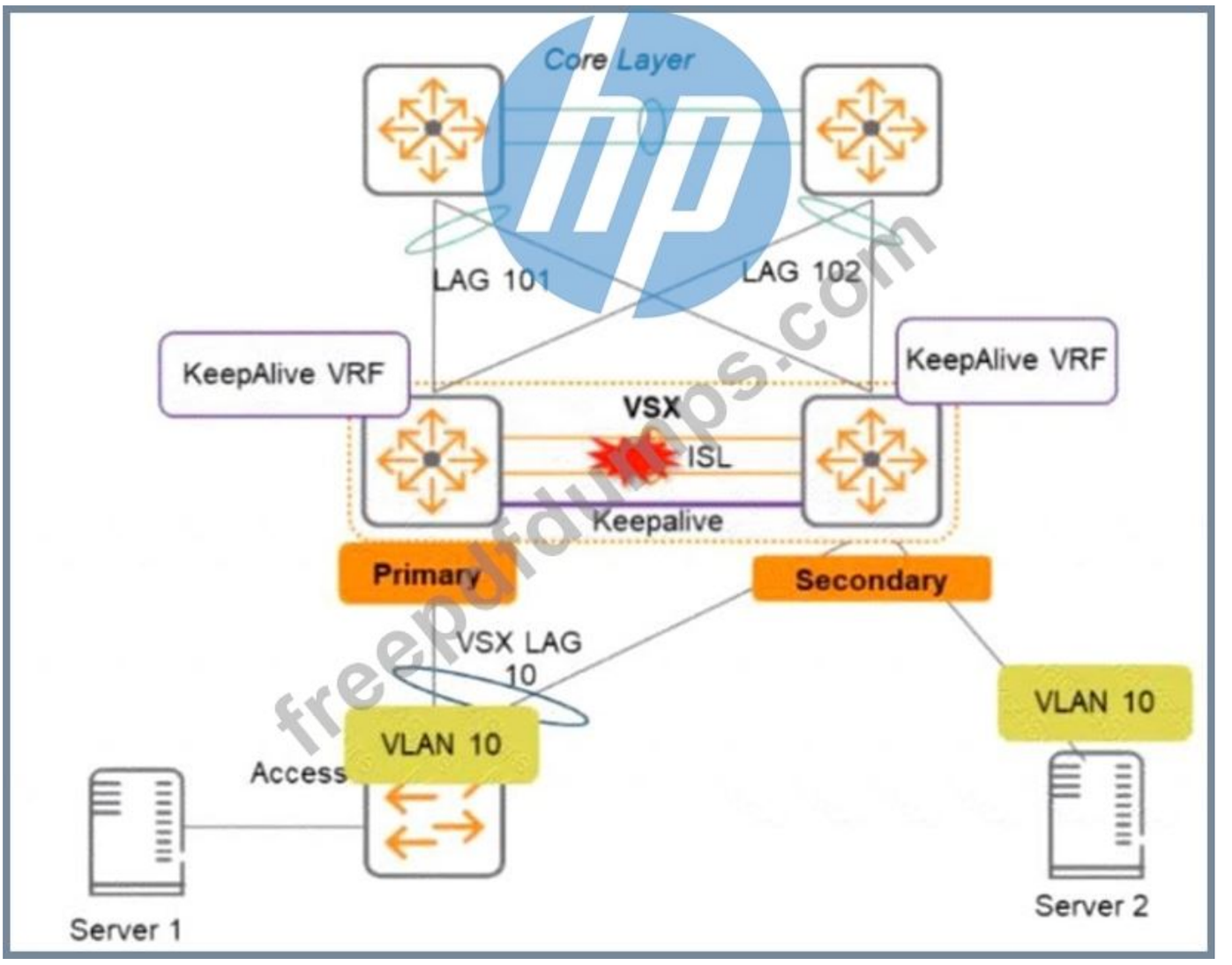
To onboard a new UXI in an existing environment with 802.1X authentication, you need to use the UXI app on your smartphone and connect the UXI via Bluetooth. The UXI app allows you to scan the QR code on the UXI sensor and configure its network settings, such as SSID, password, IP address, etc. The Bluetooth 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: 27

Two AOS-CX switches are configured with VSX at the the Access-Aggregation layer where servers attach to them An SVI interface is configured for VLAN 10 and serves as the default gateway for VLAN 10. The ISL link between the switches fails, but the keepalive interface functions. Active gateway has been configured on the VSX switches.



What is correct about access from the servers to the Core? (Select two.)

A. Server 1 can access the core layer via the keepalrve link

B. Server 2 can access the core layer via the keepalive link

C. Server 2 cannot access the core layer.

D. Server 1 can access the core layer via both uplinks

E. Server 1 and Server 2 can communicate with each other via the core layer

F. Server 1 can access the core layer on only one uplink

Answer: D,E (LEAVE A REPLY)

Explanation

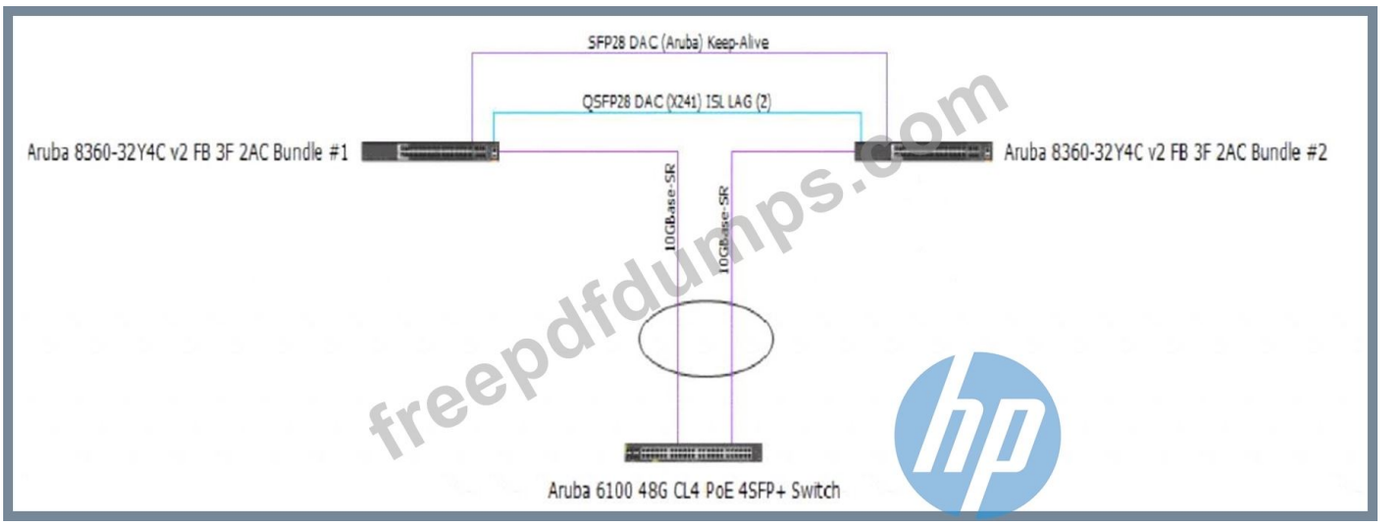
These are the correct statements about access from the servers to the Core when the ISL link between the switches fails, but the keepalive interface functions. Server 1 can access the core layer via both uplinks because it is connected to VSX-A, which is still active for VLAN 10. Server 2 can also access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

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

NEW QUESTION: 28
You need to create a keepalive network between two Aruba CX 8325 switches for VSX configuration How should you establish the keepalive connection?
A. SVI, VLAN trunk allowed all on ISL in default VRF
B. routed port in custom VRF
C. loopback 0 and OSPF area 0 in default VRF
D. SVI, VLAN trunk allowed all on ISL in custom VRF
Answer: B (LEAVE A REPLY)
Explanation
To establish a keepalive connection between two Aruba CX 8325 switches for VSX configuration, you need to use a routed port in custom VRF. A routed port is a physical port that acts as a layer 3 interface and does not belong to any VLAN. A custom VRF is a virtual routing and forwarding instance that provides logical separation of routing tables. By using a routed port in custom VRF, you can isolate the keepalive traffic from other traffic and prevent routing loops or conflicts. The other options are incorrect because they either do not use a routed port or do not use a custom VRF. 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: 29
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)
Explanation
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. 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: 30
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: 31
How is Multicast Transmission Optimization implemented in an HPE Aruba wireless network?
A. "The optimal rate for sending multicast frames is based on the highest broadcast rate across all associated clients
B. When this option is enabled the minimum default rate for multicast traffic is set to 12 Mbps for 5 GHz
C. The optimal rate for sending multicast frames is based on the lowest broadcast rate across all associated clients.
D. The optimal rate for sending multicast frames is based on the lowest unicast rate across all associated clients.
Answer: A (LEAVE A REPLY)
Explanation
This is the correct definition of Multicast Transmission Optimization in an HPE Aruba wireless network.
Multicast Transmission Optimization is a feature that improves the performance and reliability of multicast traffic by dynamically adjusting the transmission rate based on the highest broadcast rate across all associated clients. This ensures that multicast frames are sent at the optimal rate for each client and reduces retransmissions and packet loss. The other options are incorrect because they either describe different features or use incorrect terms. References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/multicast/multica
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/multicast/multica

NEW QUESTION: 32
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: (SHOW ANSWER)
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