HP.HPE7-A01.v2024-06-09.q109

Exam Code:	HPE7-A01
Exam Name:	Aruba Certified Campus Access Professional Exam
Certification Provider:	HP
Free Question Number:	109
Version:	v2024-06-09
# of views:	379
# of Questions views:	1090
https://www.freeqas.com/qa/HP/HPE7-A01/HP.HPE7-A01.v2024-06-09.q109.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)
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. Reference:
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html

NEW QUESTION: 2
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. Reference: 2 https://www.arubanetworks.com/assets/ds/DS_CX6400Series.pdf

NEW QUESTION: 3

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

A. hello interval is disabled by default

B. hello interval is based on the value set by dead interval

C. hello interval 100ms by default

D. hello interval is 1s by default

Answer: (SHOW ANSWER)

The reason is that the Inter-Switch Link Protocol (ISLP) is a protocol that enables VSX stack join and synchronization between two VSX peer switches. ISLP uses a hello interval to exchange control messages between the switches.

The hello interval is a parameter that specifies the time interval between sending hello messages. The default value of the hello interval is 1 second. The hello interval can be configured from 1 second to 10 seconds.

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

NEW QUESTION: 4

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: (SHOW ANSWER)

BSS coloring is a mechanism that helps identify the BSS Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients. on the same channel and differentiate them from other BSS on the same channel12. Each BSS is assigned a color code, which is a 6-bit value that is carried in the PHY header of the Wi-Fi frames12. By using BSS coloring, the APs and clients can reduce the threshold for interference detection and avoid unnecessary backoff or retransmissions when they detect frames from other BSS with different colors12. This can improve the spectral efficiency and throughput of the network12. The other options are incorrect because they do not describe the primary benefit of BSS coloring.

NEW QUESTION: 5

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)

Explanation

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

Option C: GRE tunnel

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

Therefore, option C is correct.

1:

https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-849

https://community.arubanetworks.com/discussion/bridge-and-tunnel-mode 3:

https://www.twingate.com/blog/ipsec-tunnel-mode

NEW QUESTION: 6

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: 7
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: 8
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)
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. Reference: 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: 9
You are working on a network where the customer has a dedicated router with redundant Internet connections Tor outbound high-importance real-time audio streams from their datacenter All of this traffic.
* originates from a single subnet
* uses a unique range of UDP ports
* is required to be routed to the dedicated router

All other traffic should route normally The SVI for the subnet containing the servers originating the traffic is located on the core routing switch in the datacenter What should be configured?

A. Configure a new OSPF area including both the core routing switch and the dedicated router

B. Configure a BGP link between the core routing switch and the dedicated router and route filtering.

C. Configure Policy Based Routing (PBR) on the core routing switch for the VRF with the servers' SVI

D. Configure a dedicated VRF on the core routing switch and make the dedicated router the default route.

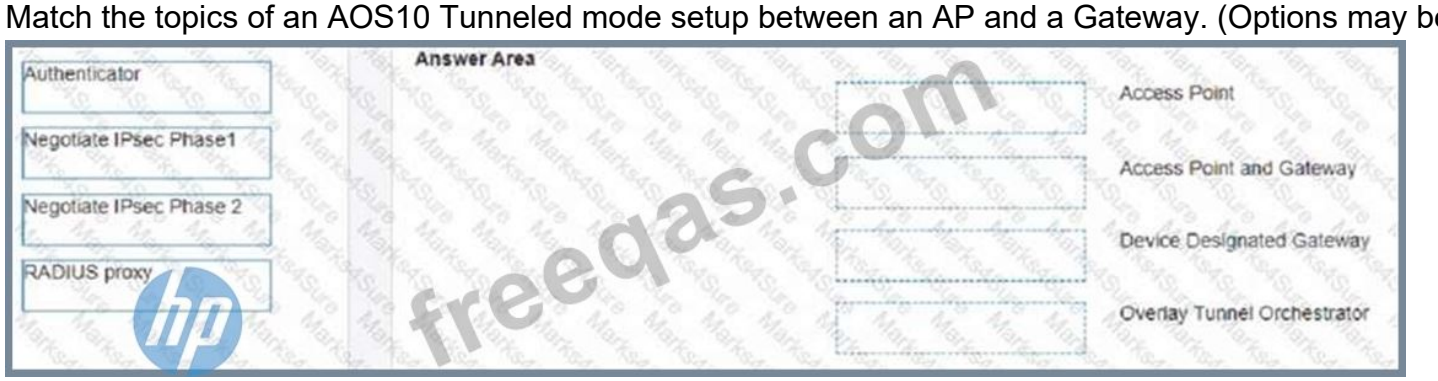
Answer: C (LEAVE A REPLY)

Explanation

The reason is that PBR allows you to route packets based on policies that match certain criteria, such as source or destination IP addresses, ports, protocols, etc. PBR can also be used to set metrics, next-hop addresses, or tag traffic for different routes.

NEW QUESTION: 10

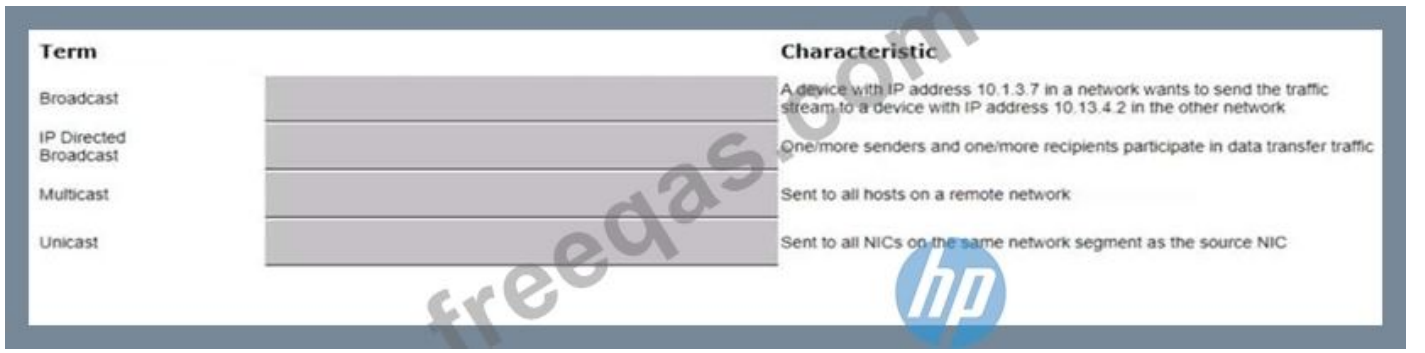
Match the topics of an AOS10 Tunneled mode setup between an AP and a Gateway. (Options may be used more than once or not at all.)



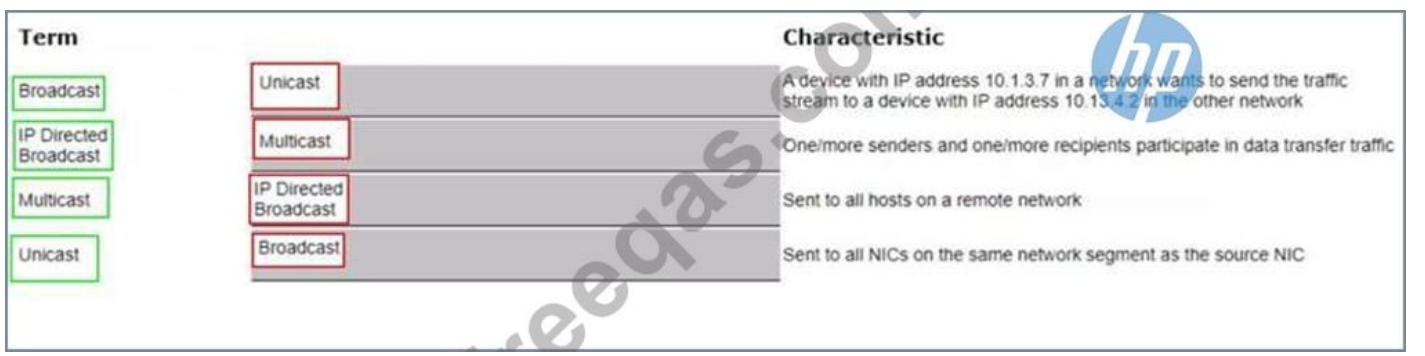
Answer:

NEW QUESTION: 11

Match the terms below to their characteristics (Options may be used more than once or not at all.)



Answer:



Reference:

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:

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: 12

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.

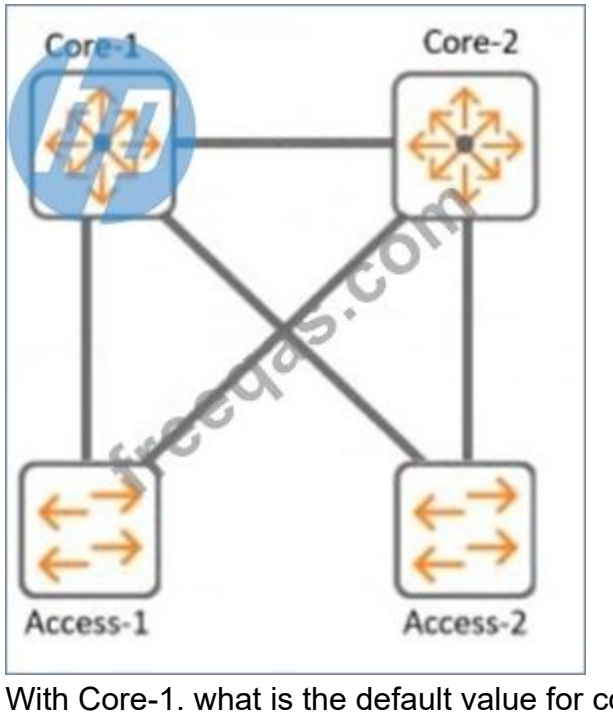
* The antenna cable for AP1 has a 3 dB loss
* The antenna cable forAP2 has a 3 OB loss.
What would be the calculated Equivalent Isotropic Radiated Power (EIRP) for AP1?
A. 2dBm
B. 8 dBm
C. 22 dBm
D. 24 dBm
Answer: B (LEAVE A REPLY)
Explanation
EIRP = 8 dBm
The formula for EIRP is:
EIRP = P - l x Tk + 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 - l x Tk / (1 + Tk) - l 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: 13
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 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)
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. Reference: 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: 14
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)
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: 15
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: B (LEAVE A REPLY)
Explanation
The auditors role is the default AOS-CX user role that meets the requirements of having Web UI access to the System > Log page and having access to the GET method for REST API for the /logs/event resource. The auditors role has a level of 1 and allows read-only access to most commands except those related to security or passwords. It also allows access to the Web UI and REST API with limited permissions. The other options are incorrect because they either have higher levels of access or do not allow access to the Web UI or REST API.
References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch01.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch04.html

NEW QUESTION: 16
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. Reference: 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: 17

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: 18
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: 19
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.

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


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: B (LEAVE A REPLY)

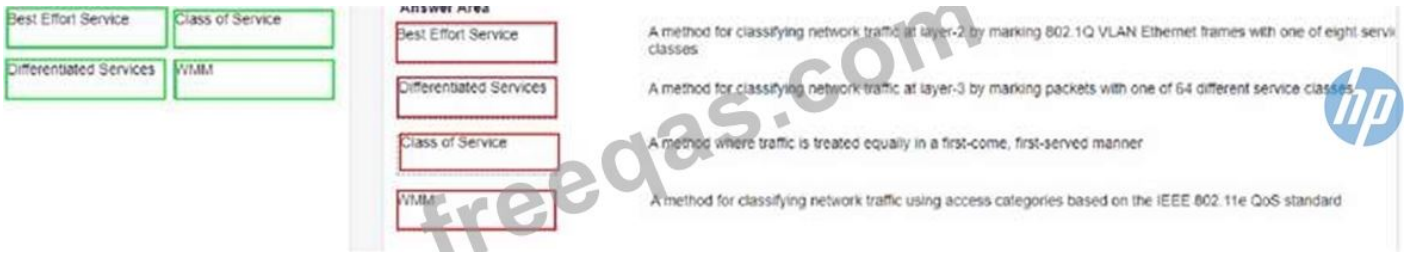
Explanation

configures DHCP snooping on the switch and enables it for VLANs 100, 110, and 120. It also specifies the IP address of the authorized DHCP server and sets the ports connected to the server as trusted. This prevents any unauthorized DHCP server from providing invalid configuration data to the clients on those VLANs. Option B also enables DHCP option-82, which adds information about the switch port and VLAN to the DHCP packets, allowing for more granular control and logging of DHCP transactions.

NEW QUESTION: 20

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

Answer:



NEW QUESTION: 21

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)

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: 22
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: (SHOW ANSWER)
Explanation
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: 23
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: 24
Describe the difference between Class of Service (CoS) and Differentiated Services Code Point (DSCP).
A. CoS has much finer granularity than DSCP
B. CoS is only contained in VLAN Tag fields DSCP is in the IP Header and preserved throughout the IP packet flow
C. They are similar and can be used interchangeably.
D. CoS is only used to determine CLASS of traffic DSCP is only used to differentiate between different Classes.
Answer: B (LEAVE A REPLY)
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. Reference: 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: 25
A system engineer needs to preconfigure several Aruba CX 6300 switches that will be sent to a remote office An untrained local field technician will do the rollout of the switches and the mounting of several AP-515s and AP-575S. Cables running to theAPs are not labeled. The VLANs are already preconfigured to VLAN 100 (mgmt), VLAN 200 (clients), and VLAN 300 (guests) What is the correct configuration to ensure that APs will work properly?
A.

```
port-access lldp-group IAP-Group
   seq 10 match sys-desc AP-515
   seq 20 match sys-desc AP-575
port-access role IAP-Role
   description ARUBA AP
   poe-priority high
   trust-mode dscp vlan trunk native 100
   vlan trunk allowed 100,200,300
   enable
port-access device-profile IAP-Profile
   associate role IAP-Role
   associate lldp-group IAP-Group
```

port-access lldp-group IAP-Group
seq 10 match sys-desc 515
seq 20 match sys-desc 575
port-access role IAP-Role
description ARUBA AP
poe-priority high
trust-mode dscp
vlan trunk native 100
vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
associate role IAP-Role
associate lldp-group IAP-Group
no shutdown

B.

```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

C.

port-access lldp-group IAP-Group
seq 10 match sys-desc 515
seq 20 match sys-desc 575
port-access role IAP-Role
description ARUBA AP
poe-priority high
trust-mode dscp
vlan trunk native 100
vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
enable
associate role IAP-Role
associate lldp-group IAP-Group

D.

Answer: (SHOW ANSWER)

Option C is the correct configuration to ensure that APs will work properly. It uses the ap command to configure a port profile for APs with VLAN 100 as the native VLAN and VLAN 200 and 300 as tagged VLANs. It also enables LLDP on the ports to discover the APs and assign them to the port profile automatically. The other options are incorrect because they either do not use the ap command, do not enable LLDP, or do not configure the VLANs correctly. Reference: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch03.html

NEW QUESTION: 26
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: 27
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 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: 28
Describe the difference between Class of Service (CoS) and Differentiated Services Code Point (DSCP).
A. CoS has much finer granularity than DSCP
B. CoS is only contained in VLAN Tag fields DSCP is in the IP Header and preserved throughout the IP packet flow
C. They are similar and can be used interchangeably.
D. CoS is only used to determine CLASS of traffic DSCP is only used to differentiate between different Classes.
Answer: (SHOW ANSWER)
Explanation

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

NEW QUESTION: 29
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: A,D (LEAVE A REPLY)
The correct answers are A and D.
According to the web search results, VSX LAG is a feature that allows multiple PSKs to be used on a single SSID, providing device-specific or group-specific passphrases for enhanced security and deployment flexibility for headless IoT devices1. VSX LAGs span both aggregation switches and appear as one device to partner downstream or upstream devices or both when forming a LAG with the VSX pair2.
One of the statements that is true about VSX LAG is that the total number of configured links may not exceed 8 for the pair or 4 per switch1. This means that a VSX LAG across a downstream switch can have at most a total of eight member links, and a switch can have a maximum of four member links. When creating a VSX LAG, it is recommended to select an equal number of member links in each segment for load balancing1.
Another statement that is true about VSX LAG is that outgoing traffic is preferentially switched to local members of the LAG2. This means that when active forwarding and active gateway are enabled, north-south and south-north traffic bypasses the ISL link and uses the local ports on the switch. This optimizes the traffic path and reduces the load on the ISL link2.
The other statements are false or not relevant for VSX LAG. Outgoing traffic is not switched to a port based on a hashing algorithm, which may be either switch in the pair. This is a characteristic of MLAG (Multi-Chassis Link Aggregation), which is a different feature from VSX LAG. LAG traffic is not passed over VSX ISL links only while upgrading firmware on the switch pair. This is a scenario that may occur when performing hitless upgrades, which is a feature that allows software updates without impacting network availability. The number of VSX lags that can be configured on all 83xx and 84xx model switches is not 255, but depends on the switch model and firmware version. For example, the AOS-CX 10.04 supports up to 64 VSX lags for 8320 switches and up to 128 VSX lags for 8325 and 8400 switches.

NEW QUESTION: 30
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 correct answer is B. An event log message is created.
The do-not-disable parameter is used to prevent the switch from disabling the port when a loop is detected by the loop-protect feature. Instead, the switch will generate an event log message that indicates the port number and the VLAN ID where the loop was detected. The switch will also send a trap to the SNMP manager, if configured1.
The other options are incorrect because:
A) Port status will not be validated once status is cleared. The port will remain enabled even if a loop is detected, unless the loop-protect action is changed to tx-disable or tx-rx-disable1.
C) The network analytics engine will not be triggered by a loop detection. The network analytics engine is a feature that allows users to monitor and troubleshoot network issues using scripts and agents2.
D) Port status LED will not blink in amber with 100Hz. The port status LED will indicate the normal port status, such as link speed and activity, regardless of the loop detection3.

NEW QUESTION: 31
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)
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: 32
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. Reference:
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 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: C (LEAVE A REPLY)

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.

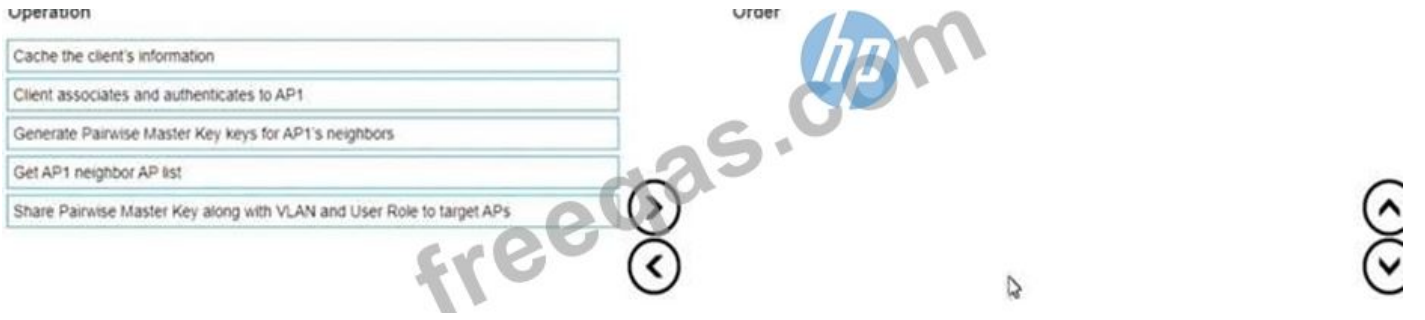
interface vlan 25: This command creates an SVI on VLAN 25 and enters the interface configuration mode3.

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.

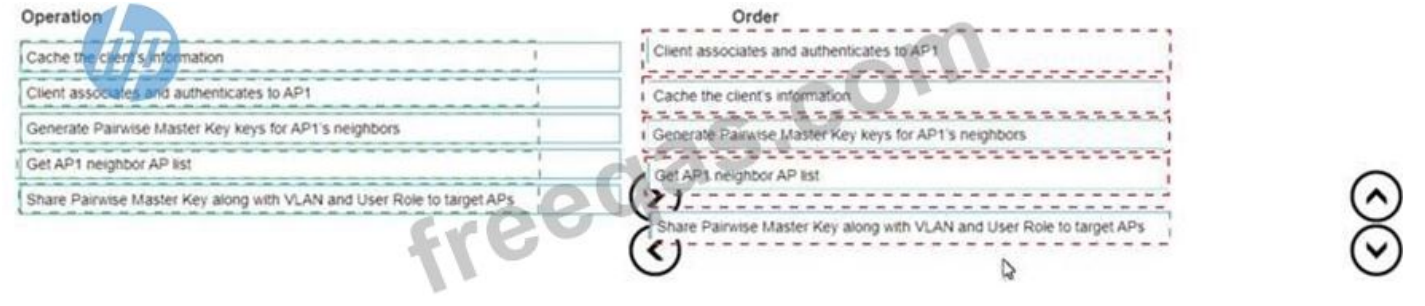
NEW QUESTION: 35
Which standard supported by some Aruba APs can enable a customer to accurately locate wireless client devices within a few meters?
A. 802.11mc
B. 802.11W
C. 802.11k
D. 802.11r
Answer: A (LEAVE A REPLY)
The standard that is supported by some Aruba APs and can enable a customer to accurately locate wireless client devices within a few meters is A) 802.11mc.
802.11mc is an IEEE standard that enables computing devices to measure the distance to nearby Wi-Fi access points using a technique called Fine Timing Measurement (FTM). FTM uses precise timestamps to calculate the round-trip time of Wi-Fi frames between the device and the access point, and then converts it to a distance estimate. By using multiple access points and triangulation methods, the device can determine its location with high accuracy1.
According to the Aruba document 802.11mc Support, this feature is supported on 500 Series, 510 Series, 530 Series, 550 Series, 560 Series and 570 Series access points. These APs act as FTM responders to time measurement queries sent from a client. To configure the AP to send FTM responses, you need to enable the ftm-responder-enable parameter in the WLAN SSID profile1.

NEW QUESTION: 36
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: 37
What is the order of operations tor Key Management service for a wireless client roaming from AP1 to AP2?



Answer:

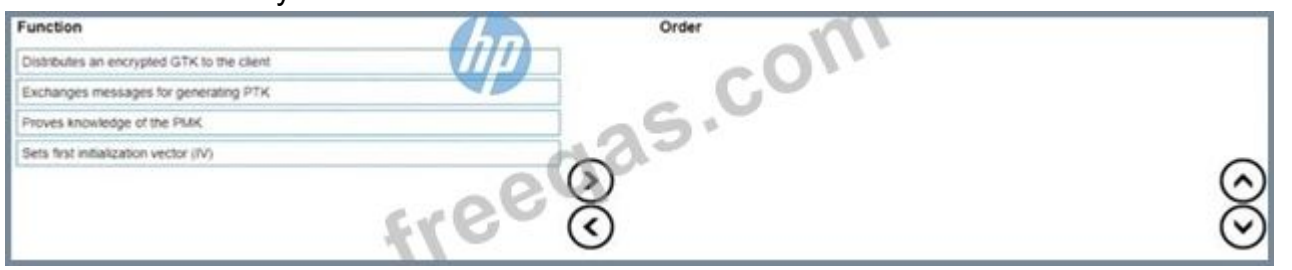


Explanation

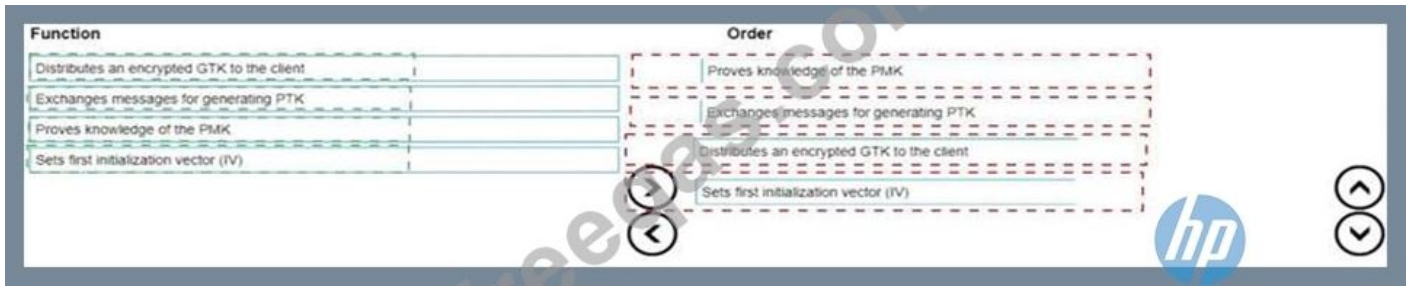
https://www.arubanetworks.com/techdocs/Instant_85_WebHelp/Content/instant-ug/wlan-ssid-conf/conf-fast-roa

NEW QUESTION: 38

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: 39
Your customer has four (4) Aruba 7200 Series Gateways and two (2) 7000 Series Gateways. The customer wants to form a cluster with these Gateways. What design consideration would prevent you from using all of those Gateways?
A. Multiple versions between Gateways in the same cluster profile are not allowed AOS 10.x.
B. A heterogeneous cluster is not supported in AOS 10.x.
C. The AP load should be lowest value of worst-case scenario load.
D. A combination of 7200 series and 7000 series gateways supports up to 4 nodes
Answer: A (LEAVE A REPLY)
The reason is that AOS 10.x does not support clustering gateways with different versions in the same cluster profile. A cluster profile defines the configuration settings for a group of gateways that are managed by Aruba Central.
According to the Aruba documentation2, "You can combine 7200 Series and 7000 Series gateways in the same cluster with a maximum size of four devices with reduced AP client capacity on 7000 Series gateways."

NEW QUESTION: 40
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)
Explanation
This is the correct solution to the problem of devices behind unmanaged switches causing network outages due to loops. Loop protection is a feature that allows an Aruba CX switch to detect and prevent loops by sending loop protection packets on each port, LAG, or VLAN on which loop protection is enabled. If a loop protection packet is received by the same switch that sent it, it indicates a loop exists and an action is taken based on the configuration. Loop protection should be configured on all edge ports of the Aruba CX 6200 and CX 6300 switches, which are the ports that connect to end devices or unmanaged switches. The trap-option should be set up to send a warning to the helpdesk when a loop is detected. The other options are incorrect because they either do not configure loop protection or do not set up the trap-option. References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-99A8B276-0DA3-4458-AF
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-85

NEW QUESTION: 41
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)

Explanation

The correct answer is B. An event log message is created.

The do-not-disable parameter is used to prevent the switch from disabling the port when a loop is detected by the loop-protect feature. Instead, the switch will generate an event log message that indicates the port number and the VLAN ID where the loop was detected. The switch will also send a trap to the SNMP manager, if configured1.

The other options are incorrect because:

A: Port status will not be validated once status is cleared. The port will remain enabled even if a loop is detected, unless the loop-protect action is changed to tx-disable or tx-rx-disable1.

C: The network analytics engine will not be triggered by a loop detection. The network analytics engine is a feature that allows users to monitor and troubleshoot network issues using scripts and agents2.

D: Port status LED will not blink in amber with 100Hz. The port status LED will indicate the normal port status, such as link speed and activity, regardless of the loop detection3.

NEW QUESTION: 42

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

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: 43

Which statements are true regarding a VXLAN implementation on Aruba Switches? (Select two.)

A. MTU size must be increased beyond the default

B. VNIs encapsulate and decapsulate VXLAN traffic

C. VTEPs encapsulate and decapsulate VXLAN traffic
D. They are only available for datacenter switches (CX 8k, 9k,10k)
E. All Aruba CX switches support VXLAN.
Answer: A,B (LEAVE A REPLY)
Explanation
Option A: MTU size must be increased beyond the default
This is because option A shows how to configure the MTU size for VXLAN tunnels on Aruba switches using the interface command and the vxlan command. The MTU size must be increased beyond the default value of
1500 bytes to accommodate the VXLAN header and payload2.
Therefore, option A is true regarding a VXLAN implementation on Aruba switches.
Option B: VNIs encapsulate and decapsulate VXLAN traffic
This is also true regarding a VXLAN implementation on Aruba switches. VNIs are used to encapsulate and decapsulate VXLAN traffic between two devices, such as a switch and a server. VNIs are also used to map VXLAN tunnels to overlay networks3.
Therefore, option B is also true regarding a VXLAN implementation on Aruba switches.
VXLAN is a Layer 2 encapsulation technology that substitutes the usage of VLAN numbers to label Ethernet broadcast domains with VXLAN numbers. VXLAN supports 224 Ethernet broadcast domains or VXLAN numbers. A VXLAN number ID is referred to as VNI. There is a one-to-one relationship between an Ethernet broadcast domain and a VNI. A single Ethernet broadcast domain can't have more than one VNI.

NEW QUESTION: 44
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)
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: 45
Which Aruba AP mode is sending captured RF data to Aruba Central for waterfall plot?
A. Hybrid Mode
B. Air Monitor
C. Spectrum Monitor
D. Dual Mode
Answer: (SHOW ANSWER)
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: 46
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: 47
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: (SHOW ANSWER)
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. Reference: https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

NEW QUESTION: 48
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)

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: 49
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: 50
A system engineer needs to preconfigure several Aruba CX 6300 switches that will be sent to a remote office An untrained local field technician will do the rollout of the switches and the mounting of several AP-515s and AP-575S. Cables running to theAPs are not labeled. The VLANs are already preconfigured to VLAN 100 (mgmt), VLAN 200 (clients), and VLAN 300 (guests) What is the correct configuration to ensure that APs will work properly?

A.
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc AP-515
    seq 20 match sys-desc AP-575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp vlan trunk native 100
    vlan trunk allowed 100,200,300
    enable
port-access device-profile IAP-Profile
    associate role IAP-Role
    associate lldp-group IAP-Group
```

B. e ip="img_94.jpg"></e>

C.
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

D.
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

Answer: C (LEAVE A REPLY)

Explanation

Option C is the correct configuration to ensure that APs will work properly. It uses the ap command to configure a port profile for APs with VLAN 100 as the native VLAN and VLAN 200 and 300 as tagged VLANs. It also enables LLDP on the ports to discover the APs and assign them to the port profile automatically. The other options are incorrect because they either do not use the ap command, do not enable LLDP, or do not configure the VLANs correctly. References:

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch03.html

NEW QUESTION: 51
By default, Best Effort is higher priority than which priority traffic type?
A. All queues
B. Background
C. Internet Control
D. Network Control
Answer: (SHOW ANSWER)
Explanation
This is because Best Effort traffic is all other kinds of non-detrimental traffic that are not sensitive to Quality of Service metrics (jitter, packet loss, latency). A typical example would be peer-to-peer and email applications2. Background traffic is a type of traffic that is used for system maintenance or backup purposes and does not affect the performance or availability of the network3.
Therefore, Best Effort traffic has a higher priority than Background traffic in terms of network resources allocation and management.
1: https://www.arubanetworks.com/techdocs/ArubaDocPortal/content/docportal.htm 2: https://stackoverflow.com/questions/33854306/best-effort-traffic-and-real-time-traffic-difference 3: https://www.informit.com/articles/article.aspx?p=25315&seqNum=4

NEW QUESTION: 52
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.
Reference: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-qos/wmm.htm https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm

NEW QUESTION: 53
What is one advantage of using OCSP vs CRLs for certificate validation?
A. reduces latency between the time a certificate is revoked and validation reflects this status
B. less complex to implement
C. higher availability for certificate validation
D. supports longer certificate validity periods
Answer: (SHOW ANSWER)
Explanation

OCSP is a protocol that allows clients to query the CA or a trusted responder for the status of a specific certificate. OCSP requests and responses are smaller and faster than CRLs, and they can provide real-time information about the revocation status of a certificate12. CRLs are lists of all revoked certificates that are downloaded from the CA. CRLs can present issues, as they can become outdated and have to be downloaded frequently13. Therefore, OCSP reduces latency between the time a certificate is revoked and validation reflects this status. References: 1 https://sectigostore.com/blog/ocsp-vs-crl-whats-the-difference/ 2 https://www.keyfactor.com/blog/what-is-a-certificate-revocation-list-crl-vs-ocsp/ 3 https://www.fortinet.com/resources/cyberglossary/ocsp

NEW QUESTION: 54
Your Director of Security asks you to assign AOS-CX switch management roles to new employees based on their specific job requirements After the configuration was complete, it was noted that a user assigned with the administrators role did not have the appropriate level of access on the switch.
The user was not limited to viewing nonsensitive configuration information and a level of 1 was not assigned to their role Which default management role should have been assigned for the user?
A. sysadmin
B. operators
C. helpdesk
D. config
Answer: B (LEAVE A REPLY)
The default management role that should have been assigned for the user is B. operators.
The operators user role is a predefined role that allows users to view nonsensitive configuration information on the switch, such as interfaces, VLANs, routing protocols, statistics, and more. The operators user role has a privilege level of 1, which is the lowest level of access on the switch1.
The administrators user role is a predefined role that has full access to all switch configuration information and all REST API methods. This role is more than what the Director of Security requires1.

NEW QUESTION: 55
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: 56
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

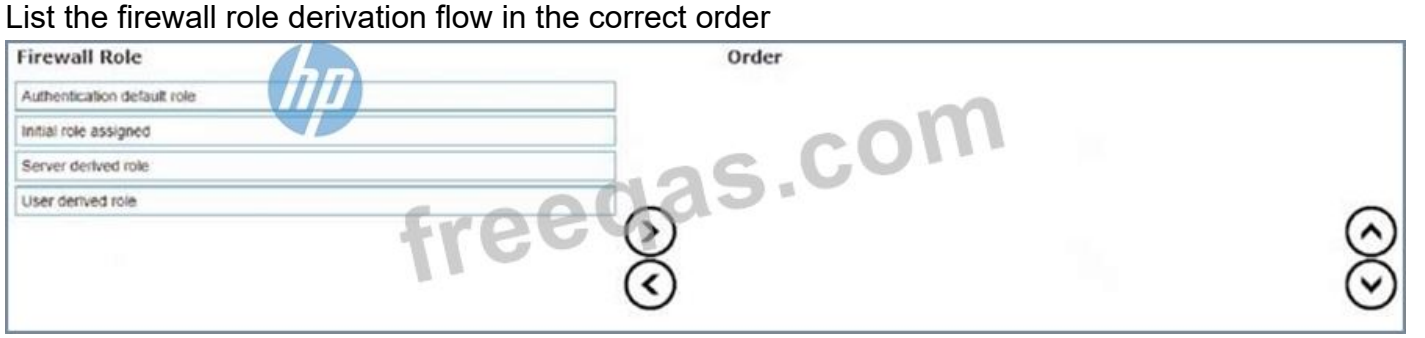
NEW QUESTION: 57
The administrator notices that wired guest users that have exceeded their bandwidth limit are not being disconnected Access Tracker in ClearPass indicates a disconnect CoA message is being sent to the AOS-CX switch.
An administrator has performed the following configuration

```
Access1(config)# ip dns host cppm.arubatraining.com 10.254.1.23 vrf mgmt
Access1(config)# radius-server host cppm.arubatraining.com key plaintext aruba123 vrf mgmt
Access1(config)# aaa group server radius cppm
Access1(config-sg)# server cppm.arubatraining.com vrf mgmt
Access1(config-sg)# exit
Access1(config)# aaa accounting port-access start-stop interim 5 group cppm
Access1(config)# radius dyn-authorization client cppm.arubatraining.com secret-key plaintext aruba123 vrf mgmt
Access1(config)# radius dyn-authorization enable
```

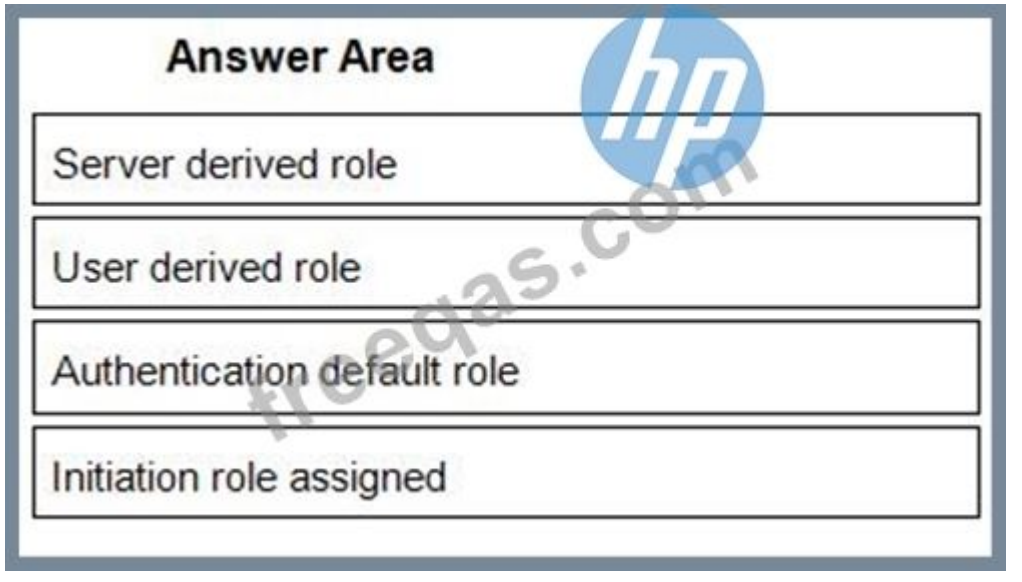
What is the most likely cause of this issue?
A. Change of Authorization has not been globally enabled on the switch
B. The SSL certificate for CPPM has not been added as a trust point on the switch
C. There is a mismatch between the RADIUS secret on the switch and CPPM.
D. There is a time difference between the switch and the ClearPass Policy Manager
Answer: (SHOW ANSWER)
Explanation

Change of Authorization (CoA) is a feature that allows ClearPass Policy Manager (CPPM) to send messages to network devices such as switches to change the authorization state of a user session. CoA requires that both CPPM and the network device support this feature and have it enabled. For AOS-CX switches, CoA must be globally enabled using the command radius-server coa enable. If CoA is not enabled on the switch, the disconnect CoA message from CPPM will be ignored and the user session will not be terminated. References: https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/index.htm#CPPM_UserGuide/Admin/C https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E

NEW QUESTION: 58
How is Dynamic Multicast Optimization (DMO) implemented in an HPE Aruba wireless network?
A. DMO is configured individually tor each SSID in use in the network.
B. The AP uses OOS to provide equal air time for multicast traffic,
C. DMO is configured globally for each SSID in use in the network.
D. The controller converts multicast streams into unicast streams.
Answer: (SHOW ANSWER)
Explanation
The correct answer is A. DMO is configured individually for each SSID in use in the network.
DMO is a feature that allows the AP to convert multicast streams into unicast streams over the wireless link.
This enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. DMO is configured individually for each SSID in use in the network, as different SSIDs may have different multicast requirements.
According to the Aruba document Configuring WLAN Settings for an SSID Profile, one of the steps to configure DMO is:
Dynamic multicast optimization: Select Enabled to allow IAP to convert multicast streams into unicast streams over the wireless link.
Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients.
The other options are incorrect because:
B: The AP does not use QoS to provide equal air time for multicast traffic. QoS is a feature that prioritizes different types of traffic based on their importance and latency sensitivity. QoS does not affect how multicast streams are transmitted over the wireless link.
C; DMO is not configured globally for each SSID in use in the network. DMO is configured individually for each SSID, as different SSIDs may have different multicast requirements.
D: The controller does not convert multicast streams into unicast streams. The AP does the conversion, as it is closer to the wireless clients and can optimize the transmission based on the client capabilities and channel conditions.

NEW QUESTION: 59
List the firewall role derivation flow in the correct order


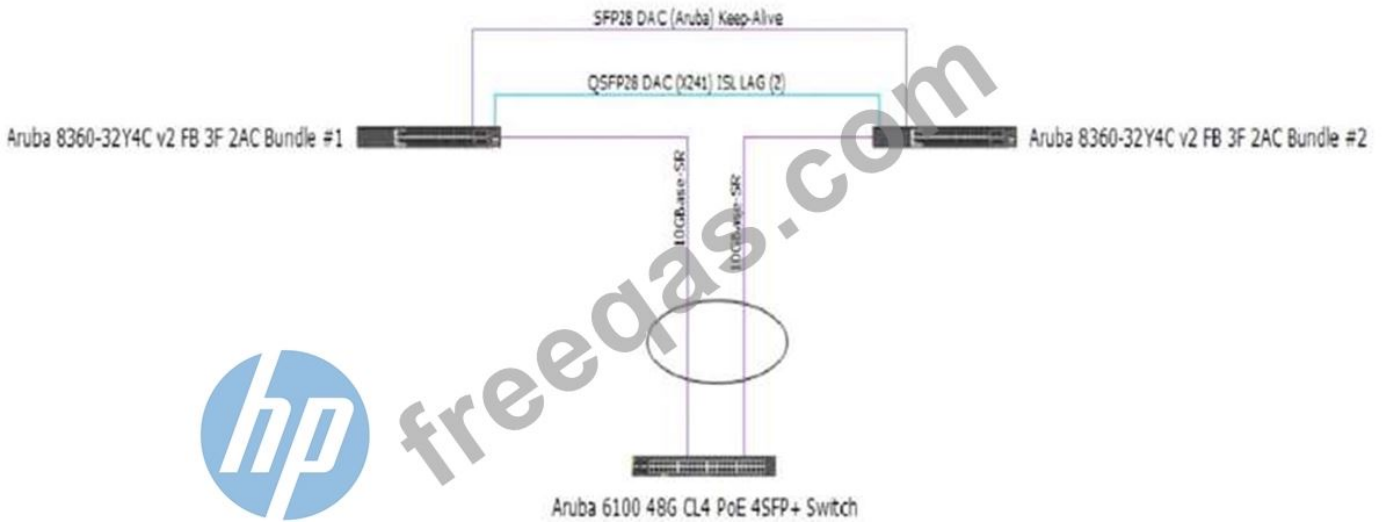
Answer:



1 - Server derived role
2 - User derived role
3 - Authentication default role
4 - Initiation role assigned

NEW QUESTION: 60
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: 61
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: C (LEAVE A REPLY)

Explanation

Option C is the only action that configures the DHCP relay on the SVI of VLAN 1000 on the CX 8360 switches. DHCP relay is a feature that allows a switch to forward DHCP requests from clients in one subnet to a DHCP server in another subnet. DHCP relay is required when the DHCP server and the clients are not in the same broadcast domain1.

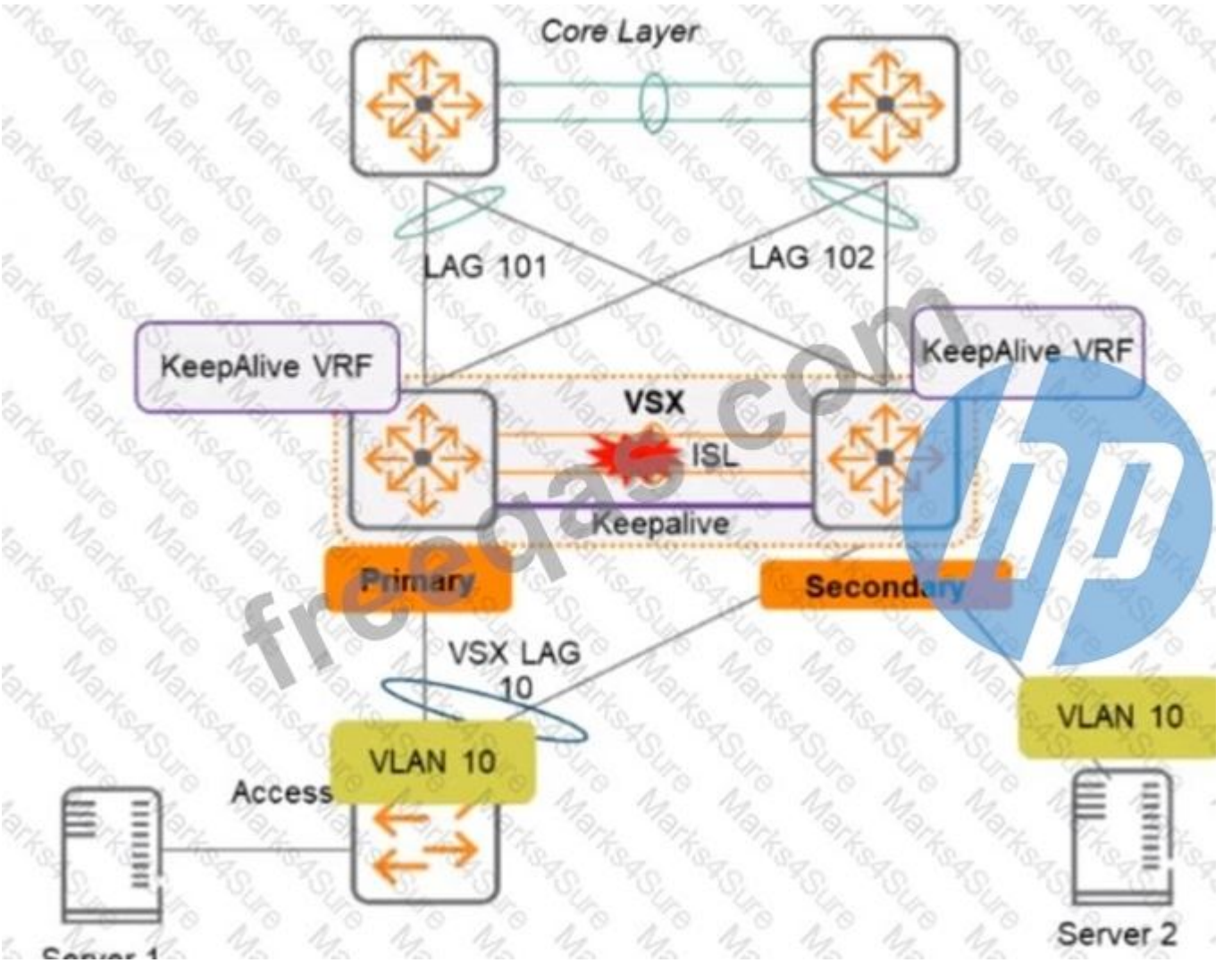
Option C uses the following commands:

interface vlan 1000: This command enters the interface configuration mode for the SVI of VLAN 1000, which has an IP address of 10.102.39.1/24 and is used for wireless clients.

ip helper-address vrf default 10.200.1.100: This command configures the IP address of the DHCP server as a helper address for the SVI, which means that the switch will forward DHCP requests from clients on VLAN 1000 to this address. The vrf default parameter indicates that the SVI and the DHCP server are in the same VRF.

NEW QUESTION: 62
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: 63
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: 64

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

A. "The optimal rate for sending multicast frames is based on the highest broadcast rate across all associated clients

B. When this option is enabled the minimum default rate for multicast traffic is set to 12 Mbps for 5 GHz

C. The optimal rate for sending multicast frames is based on the lowest broadcast rate across all associated clients.

D. The optimal rate for sending multicast frames is based on the lowest unicast rate across all associated clients.

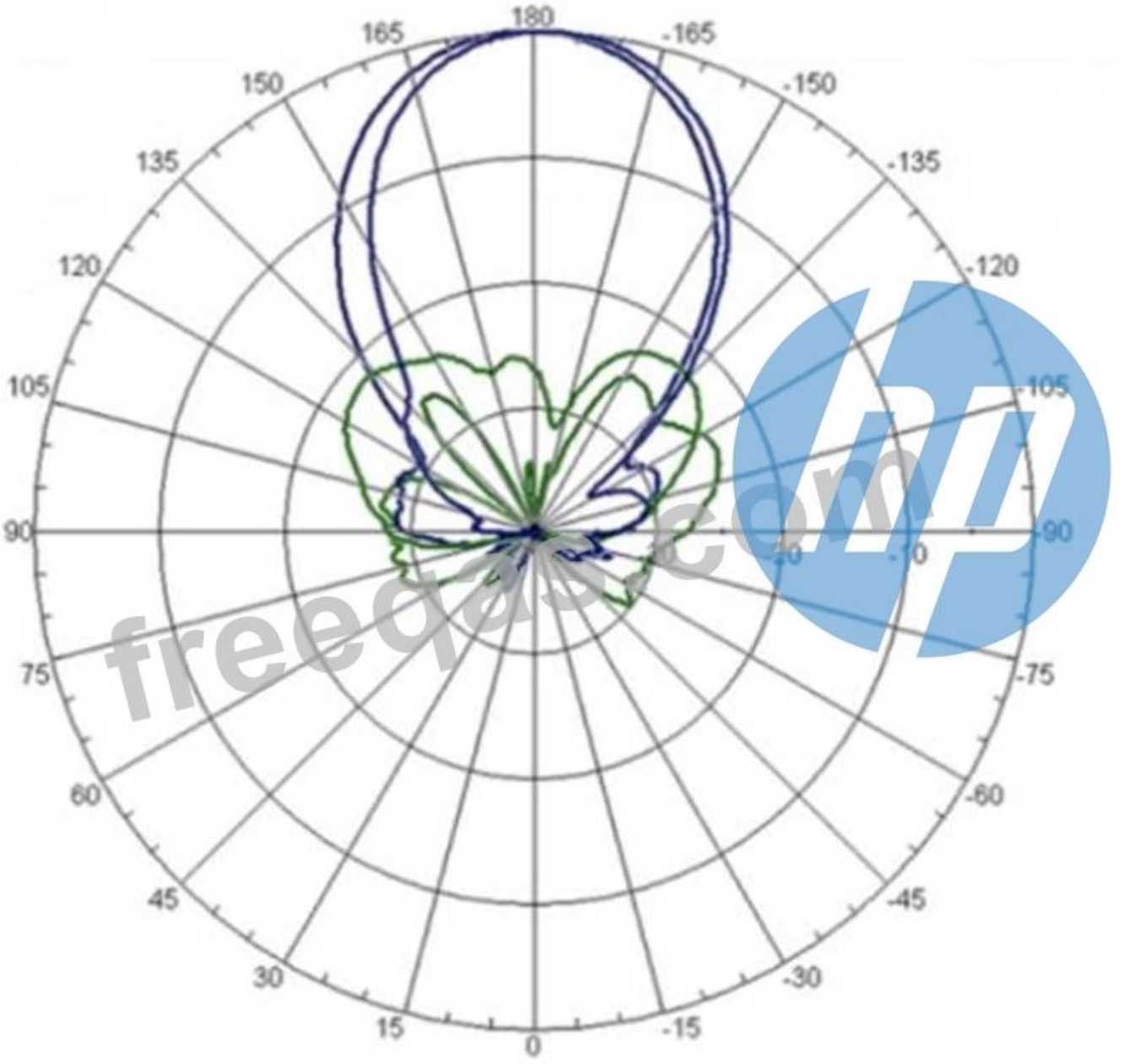
Answer: D (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 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.

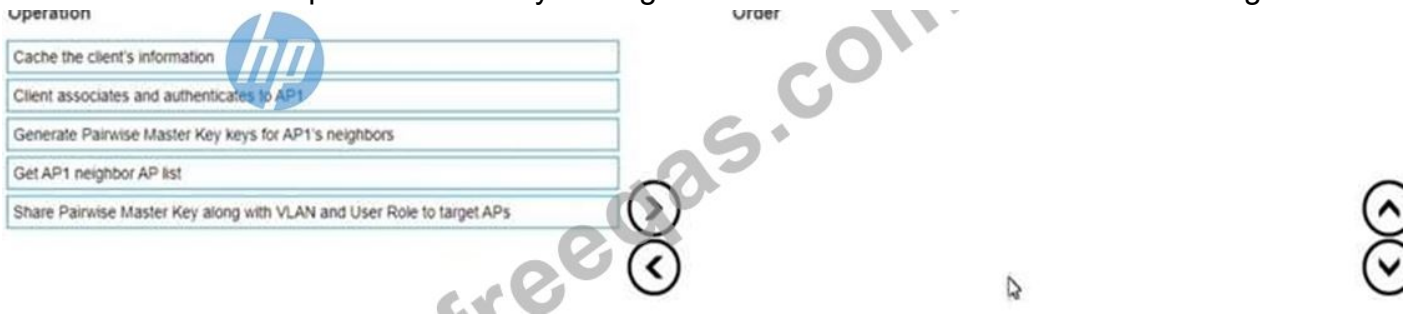
D. The AP is configured in Mesh mode

Answer: B (LEAVE A REPLY)

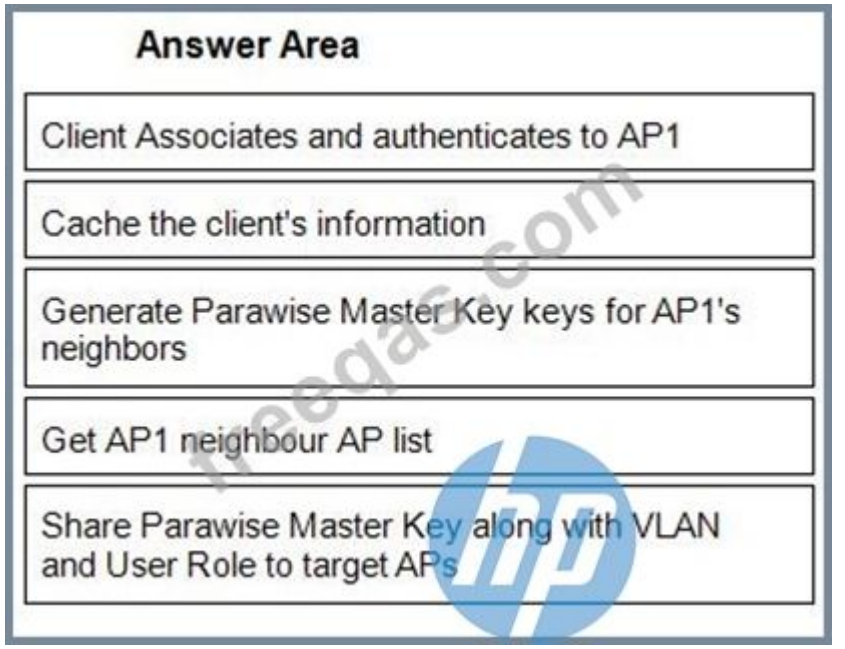
The likely cause of the issue of weak Wi-Fi coverage in the office is that the AP is using a directional antenna. A directional antenna is an antenna that radiates or receives radio waves more strongly in one or more directions, creating a focused beam of signal. A directional antenna can provide better 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 either do not affect the Wi-Fi coverage or do not match the scenario. Reference:

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



Answer:



1 - Client Associates and authenticates to AP1
2 - Cache the client's information
3 - Generate Parawise Master Key keys for AP1's neighbors
4 - Get AP1 neighbour AP list
5 - Share Parawise Master Key along with VLAN and User Role to target APs

NEW QUESTION: 67
What is used to retrieve data stored in a Management Information Base (MIS)?
SNMPv3
DSCP
TLV
CDP
Answer:
SNMPv3.

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.
According to the Aruba Certified Professional - Campus Access document1, one of the skills that this certification validates is:
Implement and Analyze the output from common network monitoring tools
Configure Port Mirroring to collect PCAPs
Configure NAE agents 9.4
Configure UXI sensors for internal and external tests
Describe how API scan be used to configure, manage, monitor, and troubleshoot your network The document also mentions that the candidate should have a distinguished understanding of different protocols across vendors, which implies that they should be familiar with SNMPv3 and how it can be used to access MIB data.
Explanation:
The correct answer is

NEW QUESTION: 68
On AOS10 Gateways, which device persona is only available when configuring a Gateway-only group'?
A. Edge
B. Mobility
C. Branch
D. VPN Concentrator
Answer: B (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-only group, which is a group that contains only one gateway device2 The Mobility persona provides Overlay WLAN and (or) wired LAN functionalities for campus networks1 The Branch persona provides the Aruba Instant OS and SD-Branch (LAN + WAN) functionality for branch and microbranch networks1 The VPN Concentrator persona provides VPN termination and routing functionality for remote access networks3 The Edge persona is not a valid option, as it is not a supported device persona for AOS 10 Gateways.

NEW QUESTION: 69
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
```
B.
```
interface vlan 20,30,40
   ip ospf passive
```
C.
```
router ospf 1
 area 0
 passive-interface
   vlan 20.30.40
```
D.
```
router ospf 1
   area 0
      redistribute local
```

Answer: B (LEAVE A REPLY)

Explanation

OSPF (Open Shortest Path First) is a routing protocol that uses link-state information to calculate the best path to each destination in the network. OSPF establishes adjacencies with neighboring routers to exchange routing information and maintain a consistent view of the network topology1.

To establish an OSPF adjacency, the routers need to have some common parameters, such as the area ID, the network type, the hello interval, the dead interval, and the authentication method2. The routers also need to have a matching subnet mask on the interface that connects them3.

In this case, the Aruba CX 6300 VSF stack has an SVI (Switched Virtual Interface) on VLAN 10 with an IP address of 10.1.1.1/24 and a LAG (Link Aggregation Group) on port 1/1/1 and port 2/1/1 that connects to a neighboring device. The SVI is configured with OSPF area 0 and network type broadcast. The LAG is configured with OSPF passive mode, which means that it will not send or receive OSPF hello packets.

The neighboring device has an interface with an IP address of 10.1.1.2/24 and a LAG on port 1/0/1 and port 2/0/1 that connects to the Aruba CX 6300 VSF stack. The interface is configured with OSPF area 0 and network type broadcast.

Since the Aruba CX 6300 VSF stack and the neighboring device have the same area ID, network type, subnet mask, and default hello and dead intervals on their interfaces, they will be able to establish an OSPF adjacency over SVI 10 with LAG 1. The OSPF passive mode on the LAG will not affect the adjacency, because it only applies to the LAG interface, not the SVI interface.

NEW QUESTION: 70

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

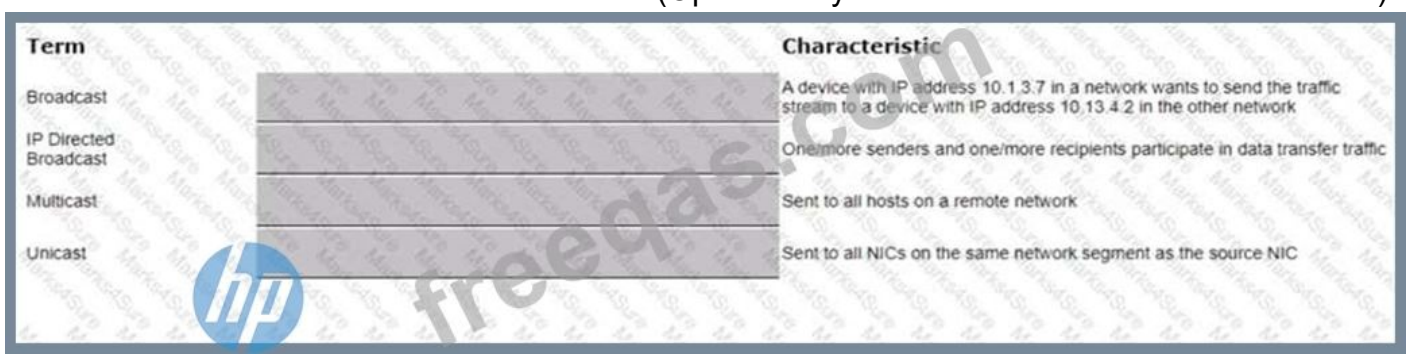
NEW QUESTION: 71
When configuring UBT on a switch what will happen when a gateway role is not specified?
A. The switch will put the client on the access VLAN
B. The gateway will assign a default role to the client
C. The switch will assign the default deny role to the client.
D. The gateway will send back the deny role to the client.
Answer: (SHOW ANSWER)
According to the Aruba Documentation Portal1, user-based tunneling (UBT) is a feature that uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. UBT enables a switch to provide a centralized security policy, using per-user authentication and access control to ensure consistent access and permissions.
Option A: The switch will put the client on the access VLAN
This is because option A shows how UBT works on an Aruba switch. When a device connects to the network, it is authenticated using either MAC Authentication or 802.1X and triggers an enforcement policy from ClearPass, which contains an enforcement profile with a user role configuration. The user role can be assigned locally on the switch or on ClearPass as part of an enforcement profile. The user role determines the VLAN that the device belongs to and the access policies that apply to it23.
Therefore, option A is correct.
1: https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-ubt.htm 2:
https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html 3:
https://community.arubanetworks.com/viewdocument/?
DocumentKey=c740df4e-3e26-4cc5-9126-355a18709c44&CommunityKey=2fd943a6-8898-4dbe-915f-4f09e4d3c317&tab=librarydocuments

NEW QUESTION: 72
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: (SHOW ANSWER)
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.

Reference: 4 https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E6C5B6A7F.html 5 https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-0C3A9D0F-6E5B-4E1A-AF3C-8D8B2F9C1A7B.html

NEW QUESTION: 73

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

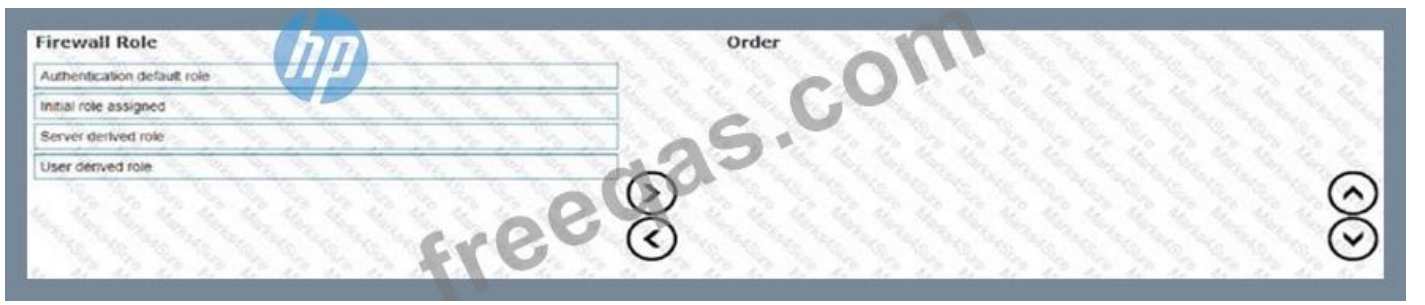
b) One/more senders and one/more recipients participate in data transfer traffic -> Multicast c) Sent to all hosts on a remote network -> IP Directed Broadcast d) Sent to all NICs on the same network segment as the source NIC -> Broadcast References: 1 https://www.thestudygenius.com/unicast-broadcast-multicast/ 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

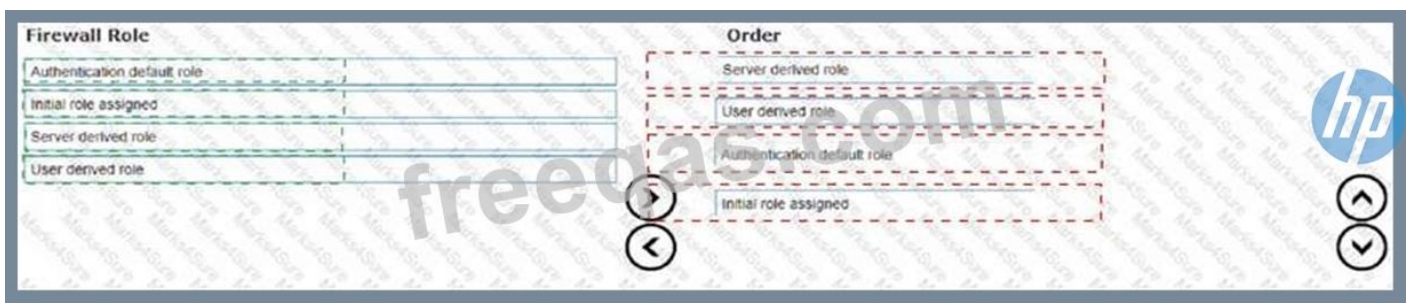
Term	Definition	Example
Broadcast	One-to-all communication, where data is sent to every device on the network	A device with IP address 10.1.3.7 sends a DHCP request to 255.255.255.255
IP Directed Broadcast	One-to-all communication, where data is sent to all hosts on a remote network	A device with IP 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: 74
When configuring UBT on a switch what will happen when a gateway role is not specified?
A. The switch will put the client on the access VLAN
B. The gateway will assign a default role to the client
C. The switch will assign the default deny role to the client.
D. The gateway will send back the deny role to the client.
Answer: A (LEAVE A REPLY)
Explanation
According to the Aruba Documentation Portal1, user-based tunneling (UBT) is a feature that uses GRE to tunnel ingress traffic on a switch interface to a gateway for further processing. UBT enables a switch to provide a centralized security policy, using per-user authentication and access control to ensure consistent access and permissions.
Option A: The switch will put the client on the access VLAN
This is because option A shows how UBT works on an Aruba switch. When a device connects to the network, it is authenticated using either MAC Authentication or 802.1X and triggers an enforcement policy from ClearPass, which contains an enforcement profile with a user role configuration. The user role can be assigned locally on the switch or on ClearPass as part of an enforcement profile. The user role determines the VLAN that the device belongs to and the access policies that apply to it23.
Therefore, option A is correct.
1: https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-ubt.htm 2: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-849
https://community.arubanetworks.com/viewdocument/?DocumentKey=c740df4e-3e26-4cc5-9126-355a18709c4

NEW QUESTION: 75
List the firewall role derivation flow in the correct order



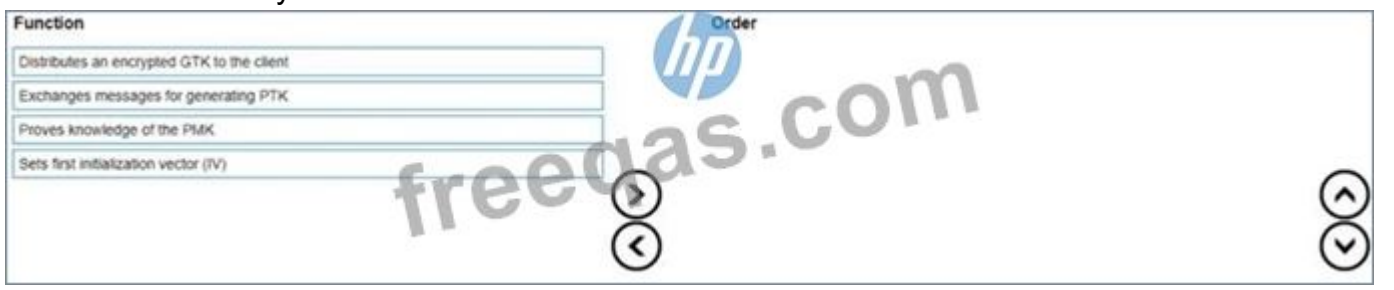
Answer:



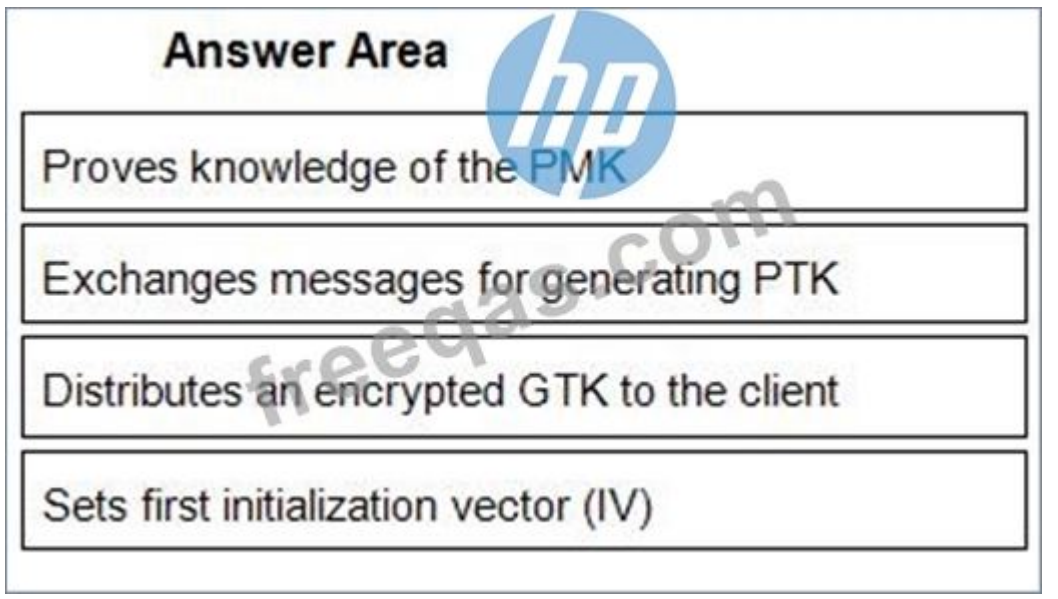
Explanation
According to the Aruba Documentation Portal1, the firewall role derivation flow in the correct order is:
* Server derived role
* User derived role

* Authentication default role
* Initiation role assigned

NEW QUESTION: 76
List the WPA 4-Way Handshake functions in the correct order.



Answer:



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

NEW QUESTION: 77
Match the solution components of NetConductor (Options may be used more than once or not at all.)

Answer:

NEW QUESTION: 78
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. Reference: 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: 79
With the Aruba CX 6200 24G switch with uplinks or 1/1/25 and 1/1/26, how do you protect client ports from forming layer-2 loops?
A. int 1/1/1-1/1/24, loop-protect
B. int 1/1/1-1/1/28. loop-protect
C. int 1/1/1-1/1/28. loop-guard
D. int 1/1/1-1/1/24. loop-guard
Answer: A (LEAVE A REPLY)
The command loop-protect enables loop protection on each layer 2 interface (port, LAG, or VLAN) for which loop protection is needed. Loop protection can find loops in untagged layer 2 links, as well as on tagged VLANs.

NEW QUESTION: 80
you are implementing ClearPass Policy Manager with EAP-TLS for authenticating all corporate-owned devices.

What are two possible solutions to the problem of deploying client certificates to corporate MacBooks that are joined to a Windows domain? (Select two.)

A. ClearPass OnBoard

B. Windows Server PKI and a GPO

C. Apple Configurator and a GPO

D. ClearPass OnGuard

E. Mobile Device Manager

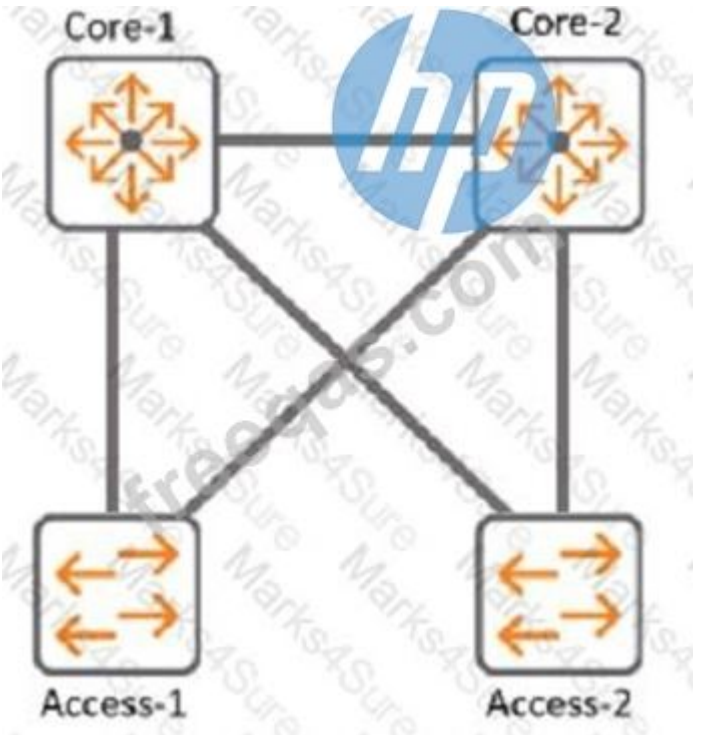
Answer: A,B (LEAVE A REPLY)

The reason is that ClearPass OnBoard is a tool that allows you to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate. This certificate can be obtained from Apple or from a third-party PKI provider.

Apple Configurator is a tool that allows you to configure and deploy Mac computers using a GPO. This tool can also be used to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate.

NEW QUESTION: 81

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)

Explanation

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

To load-balance VLANs with MSTP, you need to configure the same VLAN-to-instance mapping on all switches in the same MST region. This means that you need to assign different VLANs to different MST instances, and then adjust the spanning tree parameters (such as

priority, cost, or port role) for each instance to achieve the desired load balancing. For example, you can make one switch the root for instance 1 and another switch the root for instance 2, and then map half of the VLANs to instance 1 and the other half to instance 2.
According to the Cisco document Understand the Multiple Spanning Tree Protocol (802.1s), one of the steps to configure MST is:
* Split your set of VLANs into more instances and configure different MST settings for each of these instances. In order to easily achieve this, elect Bridge D1 to be the root for VLANs 501 through 1000, and Bridge D2 to be the root for VLANs 1 through 500. These statements are true for this configuration:
Switch D1(config)#spanning-tree mst configuration
Switch D1(config-mst)#instance 1 vlan 501-1000
Switch D1(config-mst)#exit
Switch D1(config)#spanning-tree mst 1 priority 0
Switch D2(config)#spanning-tree mst configuration
Switch D2(config-mst)#instance 2 vlan 1-500
Switch D2(config-mst)#exit
Switch D2(config)#spanning-tree mst 2 priority 0
The above commands create two MST instances, 1 and 2, and map VLANs 501-1000 to instance 1 and VLANs 1-500 to instance 2. Then, they make switch D1 the root for instance 1 and switch D2 the root for instance 2.
The other options are incorrect because:
* A. Spanning-tree bpdu-guard setting is a security feature that disables a port if it receives a BPDU from an unauthorized device. It does not affect load balancing with MSTP.
* C. Spanning-tree CIST mapping is not a valid command. CIST stands for Common and Internal Spanning Tree, which is the spanning tree instance that runs within an MST region and interacts with other regions or non-MST switches.
* D. Spanning-tree root-guard setting is another security feature that prevents a port from becoming a root port if it receives superior BPDUs from another switch. It does not affect load balancing with MSTP.

NEW QUESTION: 82
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: (SHOW ANSWER)
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: 83
A system engineer needs to preconfigure several Aruba CX 6300 switches that will be sent to a remote office An untrained local field technician will do the rollout of the switches and the mounting of several AP-515s and AP-575S. Cables running to theAPs are not labeled. The VLANs are already preconfigured to VLAN 100 (mgmt), VLAN 200 (clients), and VLAN 300 (guests) What is the correct configuration to ensure that APs will work properly?

A.
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc AP-515
    seq 20 match sys-desc AP-575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp vlan trunk native 100
    vlan trunk allowed 100,200,300
    enable
port-access device-profile IAP-Profile
    associate role IAP-Role
    associate lldp-group IAP-Group
```

B.
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    associate role IAP-Role
    associate lldp-group IAP-Group
    no shutdown
```

C.

```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

D.

```
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
```

Answer: C (LEAVE A REPLY)

Explanation

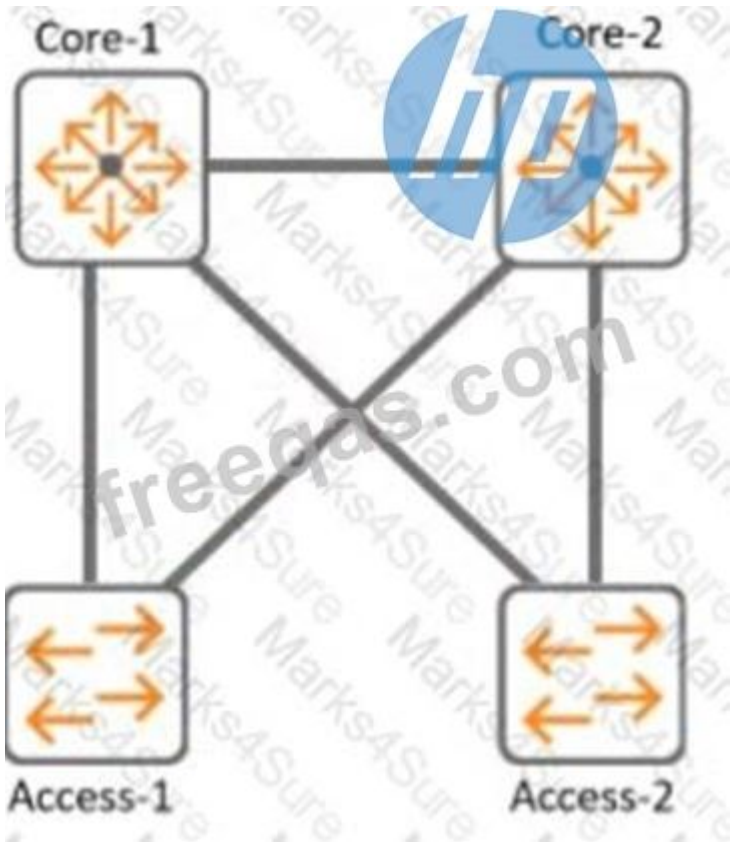
Option C is the correct configuration to ensure that APs will work properly. It uses the ap command to configure a port profile for APs with VLAN 100 as the native VLAN and VLAN 200 and 300 as tagged VLANs. It also enables LLDP on the ports to discover the APs and assign them to the port profile automatically. The other options are incorrect because they either do not use the ap command, do not enable LLDP, or do not configure the VLANs correctly. References:

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch03.html

NEW QUESTION: 84

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: 85

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.

NEW QUESTION: 86
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: A (LEAVE A REPLY)
MAC Caching is a feature that allows a guest user to bypass the captive portal page after the first authentication based on their MAC address1 MAC Caching can be enabled under the splash page settings in Aruba Cloud Guest2 MAC Caching can improve the user experience and reduce the network overhead by eliminating the need for repeated authentication.

NEW QUESTION: 87
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: 88
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 G0 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: B (LEAVE A REPLY)
Aruba 9004 gateway supports ZTP on port G0/0/0 by default1. If the gateway is connected to a different port, such as G0/0/V1, it will not be able to communicate with Aruba Activate and Aruba Central, which are required for ZTP2. Moreover, port G0/0/V1 is configured as a DHCP server by default, which can cause IP address conflicts with the existing network3. Therefore, the technician should move the cable on the gateway to port G0/0/0, which will allow the gateway to obtain an IP address from the network DHCP server and start the ZTP process. The other options are not correct because they will not solve the issue or enable ZTP. For example, option D will not work because factory defaulting and rebooting the gateway will not change the port configuration or behavior3.

NEW QUESTION: 89
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: 90

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: 91
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: 92
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-NETGEAR-Multi-Gigabit-Ethernet-Switches-in-my-network 3: https://arstechnica.com/gadgets/2016/09/5gbps-ethernet-standard-details-8023bz/

NEW QUESTION: 93
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: C,D (LEAVE A REPLY)
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: 94
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: (SHOW ANSWER)
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: 95
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)
Explanation
The active gateway feature is used to provide active-active layer 3 default gateway for hosts on the same subnet. It allows the switch to convert multicast streams into unicast streams over the wireless link, which improves the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. The active gateway feature is unique to VSX configuration because it eliminates the need for VRRP and avoids traffic being pushed over the ISL link, which can cause latency in the network12.
The correct answer to the question is C. Sixteen different VMACs are supported for each IPv4 and IPv6 stack simultaneously. This means that you can have a maximum of eight VMACs for IPv4, and a maximum of eight VMACs for IPv6, on a VSX pair. Only 15 VMACs are supported on 6400 switch series2.
The other options are incorrect because:
A: Sixteen different VMACs are not supported total as shared. They are supported for each IPv4 and IPv6 stack separately.
B: Active gateway can be used without MSTP instances. MSTP is a protocol that allows multiple spanning tree instances to coexist on the same switch, but it does not affect how active gateway works.
D: Active gateway does not copy traffic over the ISL link for an optimized path. It avoids using the ISL link for routed traffic and uses the local switch interface MAC instead of the virtual MAC address (VMAC) for source address1.

NEW QUESTION: 96
With the Aruba CX 6200 24G switch with uplinks or 1/1/25 and 1/1/26, how do you protect client ports from forming layer-2 loops?
A. int 1/1/1-1/1/24, loop-protect
B. int 1/1/1-1/1/28. loop-protect
C. int 1/1/1-1/1/28. loop-guard
D. int 1/1/1-1/1/24. loop-guard
Answer: (SHOW ANSWER)
Explanation
The command loop-protect enables loop protection on each layer 2 interface (port, LAG, or VLAN) for which loop protection is needed. Loop protection can find loops in untagged layer 2 links, as well as on tagged VLANs.

NEW QUESTION: 97

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

A. administrators

B. auditors

C. sysops

D. operators

Answer: A (LEAVE A REPLY)

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. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch01.html https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch04.html

NEW QUESTION: 98

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: 99

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

A. SNMPv3

B. DSCP

C. TLV

D. CDP

Answer: A (LEAVE A REPLY)

Explanation

The correct answer is A. SNMPv3.

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.
According to the Aruba Certified Professional - Campus Access document1, one of the skills that this certification validates is:
Implement and Analyze the output from common network monitoring tools
Configure Port Mirroring to collect PCAPs
Configure NAE agents 9.4
Configure UXI sensors for internal and external tests
Describe how API scan be used to configure, manage, monitor, and troubleshoot your network The document also mentions that the candidate should have a distinguished understanding of different protocols across vendors, which implies that they should be familiar with SNMPv3 and how it can be used to access MIB data.

NEW QUESTION: 100
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: 101
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: (SHOW ANSWER)
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: 102
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: (SHOW ANSWER)
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. Reference: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html https://techhub.hpe.com/eginfolib/networking/docs/arubaos-switch/security/GUID-EA0A5B3C-FE4C-4B9B-BE1D-FE7D2B9F8C3A.html

NEW QUESTION: 103
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. 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. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-99A8B276-0DA3-4458-

AFD8-42BFEC29D4F5.html https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-8561-17DB0311ED8F.html

NEW QUESTION: 104
you are implementing ClearPass Policy Manager with EAP-TLS for authenticating all corporate-owned devices.
What are two possible solutions to the problem of deploying client certificates to corporate MacBooks that are joined to a Windows domain? (Select two.)
A. ClearPass OnBoard
B. Windows Server PKI and a GPO
C. Apple Configurator and a GPO
D. ClearPass OnGuard
E. Mobile Device Manager
Answer: A,B (LEAVE A REPLY)
Explanation
The reason is that ClearPass OnBoard is a tool that allows you to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate. This certificate can be obtained from Apple or from a third-party PKI provider.
Apple Configurator is a tool that allows you to configure and deploy Mac computers using a GPO. This tool can also be used to enroll Mac computers into a ClearPass Policy Manager site using an Apple MDM push certificate.

NEW QUESTION: 105
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
```
B.
```
interface vlan 20,30,40
   ip ospf passive
```
C.
```
router ospf 1
 area 0
 passive-interface
    vlan 20.30.40
```
D.
```
router ospf 1
   area 0
       redistribute local
```
Answer: (SHOW ANSWER)
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: 106
Select the Aruba stacking technology matching each option (Options may be used more than once or not at all.)

Answer:

NEW QUESTION: 107
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: (SHOW ANSWER)

Explanation

Two parts of the solution for these requirements are Option C and Option E.

Option C is a part of the solution because it defines a policy-based routing action list named route_test, which specifies the next hop IP address as 10.1.1.253 for the matching traffic. This is the new default route that the user wants to use for the subnet 10.2.250.0/24. The interface null parameter indicates that the traffic will be routed to the next hop without using a specific interface1.

Option E is a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 250, which has an IP address of 10.2.250.1/24. This is the subnet that the user wants to test the new default route for. The apply policy command enables policy-based routing on the interface and associates it with the action list2.

Option A is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify the next hop IP address as 10.1.1.253, which is the new default route that the user wants to use. Instead, it specifies a next hop IP address of 10.1.1.254, which is different from the requirement.

Option B is not a part of the solution because it defines a policy-based routing action list named route_test, but does not specify any next hop IP address at all, which is necessary for policy-based routing to work. Instead, it specifies an interface null parameter without any IP address, which is invalid.

Option D is not a part of the solution because it applies the policy-based routing action list route_test to the VLAN interface 200, which has an IP address of 10.2.200.1/24. This is not the subnet that the user wants to test the new default route for, but a different subnet that should not be affected by this change.

NEW QUESTION: 108
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)
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: 109
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)
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