HP.HPE7-A07.v2026-07-28.q58

Exam Code:	HPE7-A07
Exam Name:	Aruba Certified Campus Access Mobility Expert Written Exam
Certification Provider:	HP
Free Question Number:	58
Version:	v2026-07-28
# of views:	120
# of Questions views:	580
https://www.freeqas.com/qa/HP/HPE7-A07/HP.HPE7-A07.v2026-07-28.q58.html	

NEW QUESTION: 1
A network technician racked up two 9240 mobility gateways in a single cluster that will be terminating 1700 APs in a medium-sized branch office Next, the technician cabled the gateways with two SFP28 Direct Attach Copper (DAC) cables, distributed between a two-member core switching stack and powered them up.
What must the network administrator do next regarding the gateway configuration to ensure maximum wired bandwidth utilization?
A. Map two physical ports to a port channel on each gateway.
B. Make an ports trunk interfaces and permit data VLANs
C. Disable the spanning tree and allocate unique VLANs to each port.
D. Manually set 25Gbps speeds on all ports.
Answer: A (LEAVE A REPLY)
To maximize wired bandwidth utilization, especially when multiple APs are terminating on mobility gateways, it's best practice to aggregate physical ports into a port channel. This provides redundancy and increased bandwidth by combining the throughput of multiple ports.

NEW QUESTION: 2
You want to configure an MTU of 9198 for a routed lag interface on a CX 6300 switch. Which configuration achieves this?
A.
```
interface lag 11 multi-chassis
    no shutdown
    ip mtu 9198
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```
B.
```
interface lag 11
    no shutdown
    ip address 10.1.1.1/24
    lacp mode active
    exit
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

C.

D.

Answer: A (LEAVE A REPLY)

In the context of ArubaOS-CX, particularly with the 6300 series switches, setting the MTU on a routed Link Aggregation Group (LAG) interface requires the interface lag id command in the configuration, specifying the LAG interface you're configuring. The ip mtu command is then used to set the desired MTU size for that LAG. Option A correctly shows this configuration process, where the MTU is set to 9198 for the LAG interface, in line with the requirements for routing larger frames, which could be necessary for certain applications or data flows that require jumbo frames.

The information related to the configuration of Aruba switches is consistent with the principles and guidelines found in the technical documentation for the ArubaOS-CX 6300 series switches, which emphasizes the importance of correct MTU settings for network performance and stability.

NEW QUESTION: 3

What should be defined on the Edge-1 to establish valid BGP routing between agg-sw1 and agg-sw2 using BGP protocol using the IP addresses above?

A. OPTION A

B. OPTION B

C. OPTION C

D. OPTION D

Answer: D (LEAVE A REPLY)

In the design shown:

* The BGP peering between agg-sw1 and agg-sw2 is being established using loopback interfaces as the BGP neighbor addresses (10.0.0.2 and 10.0.0.4)
* When BGP peering uses loopbacks, you must configure the BGP session to originate updates from the same loopback interface that the neighbor's address resolves to Otherwise, the TCP session fails because:
The source IP does not match the configured neighbor remote-IP which is based on the loopback address Aruba AOS-CX requirement:
"When configuring eBGP or iBGP neighbors using loopback interfaces, apply update-source <loopback> under the IPv4 unicast address family so BGP uses the correct source interface for peering."

NEW QUESTION: 4
You configured" a bridgedmode SSID with WPA3-Enterprise and EAP-TLS security. When you connect an Active Directory joined client that has valid client certificates. ClearPass shows the following error.

What is needed to resolve this issue?
A. Enable authorization in your Authentication Method.
B. Recreate the SSID m tunneled mode.
C. Modify your ACX-AD authentication source to include the UPN in the search.
D. Configure ClearPass to trust the client certificate.
Answer: C (LEAVE A REPLY)
The error message "User not found" indicates that the authentication source, in this case, Active Directory (AD), is not able to locate the user account based on the current search parameters. This often occurs when the User Principal Name (UPN) that the client is using to authenticate is not included in the search parameters of the AD authentication source within ClearPass. By modifying the AD authentication source to include the UPN in the search, ClearPass will be able to correctly locate the user account and proceed with the authentication using the valid client certificates.

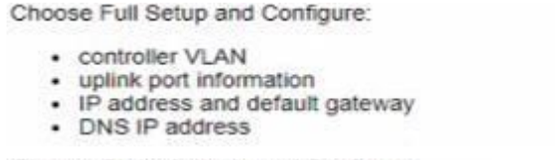
NEW QUESTION: 5
A customer is running out of IP addresses in a network segment. What will happen if they add an additional IP subnet to the same VLAN?
A. This would result in a single SVI using two subinterfaces
B. Users can reach each other and establish PTP traffic without passing an L3 point in the same VLAN
C. Broadcasts for the two subnets will arrive on all ports in the same VLAN
D. IGMP will not work in both of the subnets in the same VLAN
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract of HPE Aruba Networking Switching:

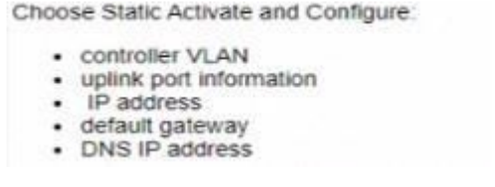
On Aruba switches (AOS-CX/AOS-S), multiple IPv4 networks can be configured on the same VLAN interface (SVI) by assigning a primary address and one or more secondary addresses. The VLAN remains one Layer-2 broadcast domain; adding more IP subnets does not create subinterfaces and does not split the broadcast domain.
Exact extract:
* "A VLAN interface may be configured with a primary IP address and additional secondary IP addresses to host multiple subnets on the same Layer-2 broadcast domain."
* "A VLAN is a single broadcast domain. Broadcast and unknown unicast frames are flooded to all ports belonging to the VLAN."
* "Hosts in different IP subnets on the same VLAN still require Layer-3 routing to communicate; sharing the VLAN only means they share the same L2 broadcast domain." Therefore, when a second subnet is added to the same VLAN, broadcasts (ARP, DHCP, etc.) from devices in either subnet will be flooded to all member ports of that VLAN, making option C correct.
Options A (subinterfaces) are not used here; B is incorrect because inter-subnet traffic still needs routing; D is not categorically true-IGMP operates per VLAN with multicast routing configuration and is not inherently disabled by multiple subnets.
References of HPE Aruba Networking Switching documents or Study Guide:
* Aruba AOS-CX Interface and VLAN Configuration Guide - "Primary and secondary IP addressing on VLAN interfaces; VLANs as broadcast domains."
* Aruba AOS-CX Layer 2 Fundamentals - "Flooding behavior for broadcast/unknown frames within a VLAN."
* Aruba Campus Wired Design Fundamentals - "Multiple IP subnets on one VLAN and routing implications."

NEW QUESTION: 6
You are deploying a new AOS 10 mobility gateway cluster. Due to customer requirements, the gateways must be configured with static IP addresses and are restricted from communicating using port 443 to any URLs except tor "central arubanetworks.com How would you onboard these gateways successfully into HPE Aruba Networking Central?

A.


B.

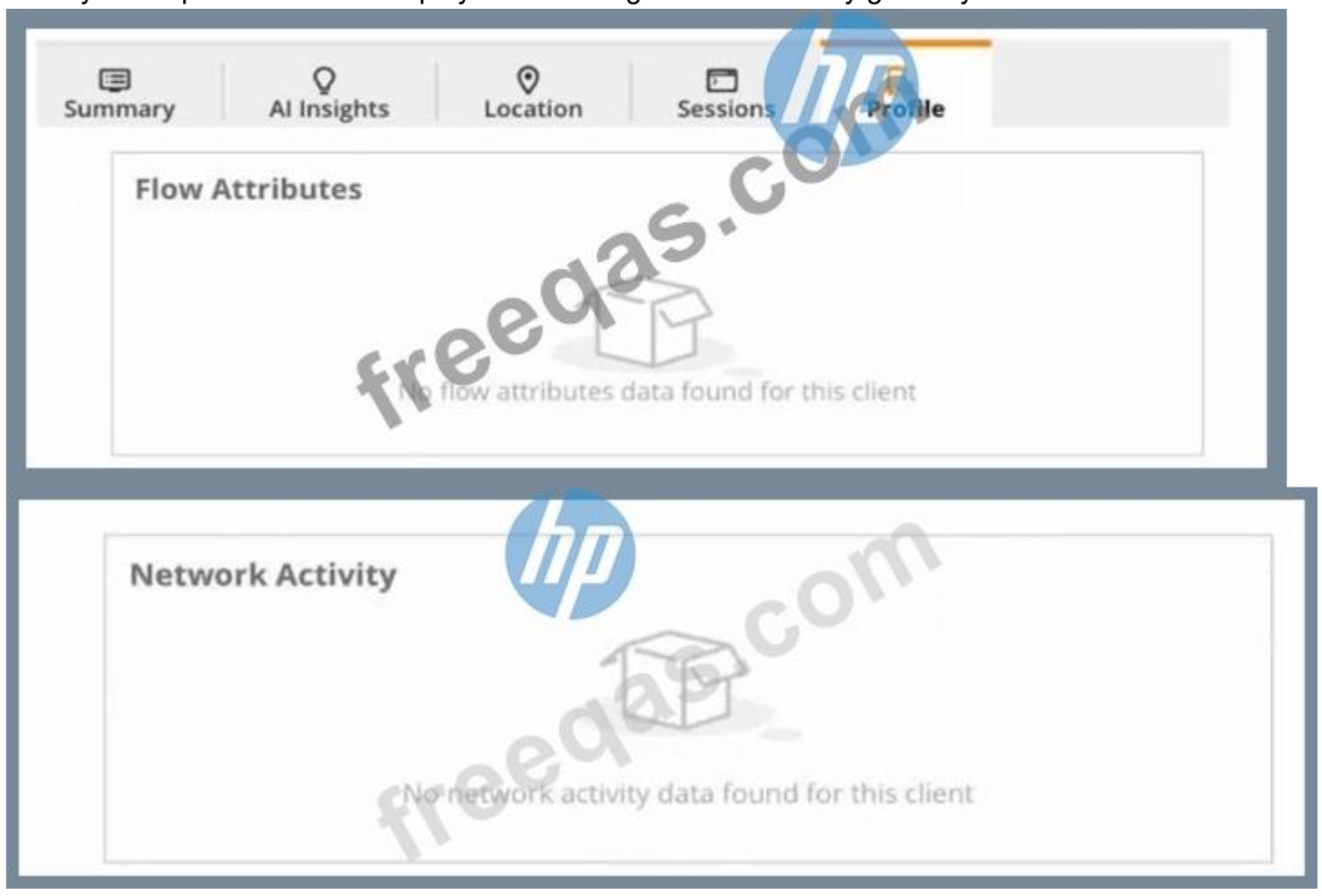

C.


D.


Answer: A (LEAVE A REPLY)

Option A includes all necessary steps for a full setup of an AOS 10 mobility gateway cluster, including setting the system name, switch role, ACP FQDN address, uplink port information, IP address and default gateway, DNS IP address, controller country code, timezone and clock, andadmin password. Since the gateways must have static IP addresses and can only communicate on port 443 for a specific URL, this configuration would need to allow for static IP configuration and restrict communication to the required URL.

NEW QUESTION: 7
A customer is reviewing HPE Aruba Networking Central's Client Insights and notices that several wireless clients are not displaying flow attributes and network activity in the profile tab. This deployment is using AOS-10 mobility gateways.



What are the possible reasons why this data is not visible in HPE Aruba Networking Central? (Select two)
A. The client's SSID is configured as mixed mode, and the clients experiencing the issue are tunneled out of the APs
B. The wireless client VLANs on the gateways are marked as trusted
C. The client's SSID is configured as bridged
D. The client's SSID is configured as mixed mode, and the clients experiencing the issue are bridged out of the APs
E. The wireless client VLANs on the gateways are marked as untrusted
Answer: C,D (LEAVE A REPLY)
* Why C and D are correct (bridged traffic):
"In AOS 10 deployments that use mobility gateways, application/flow visibility and Client Insights for wireless clients are derived from gateway DPI and firewall session state. When an SSID is bridged at the AP (including mixed mode where a client is bridged), client data traffic does not traverse the gateway. Because the gateway does not see the user flows, flow attributes and network activity are not populated in Central for those clients." This applies to:
* C - SSID is bridged (all clients bypass the gateway).

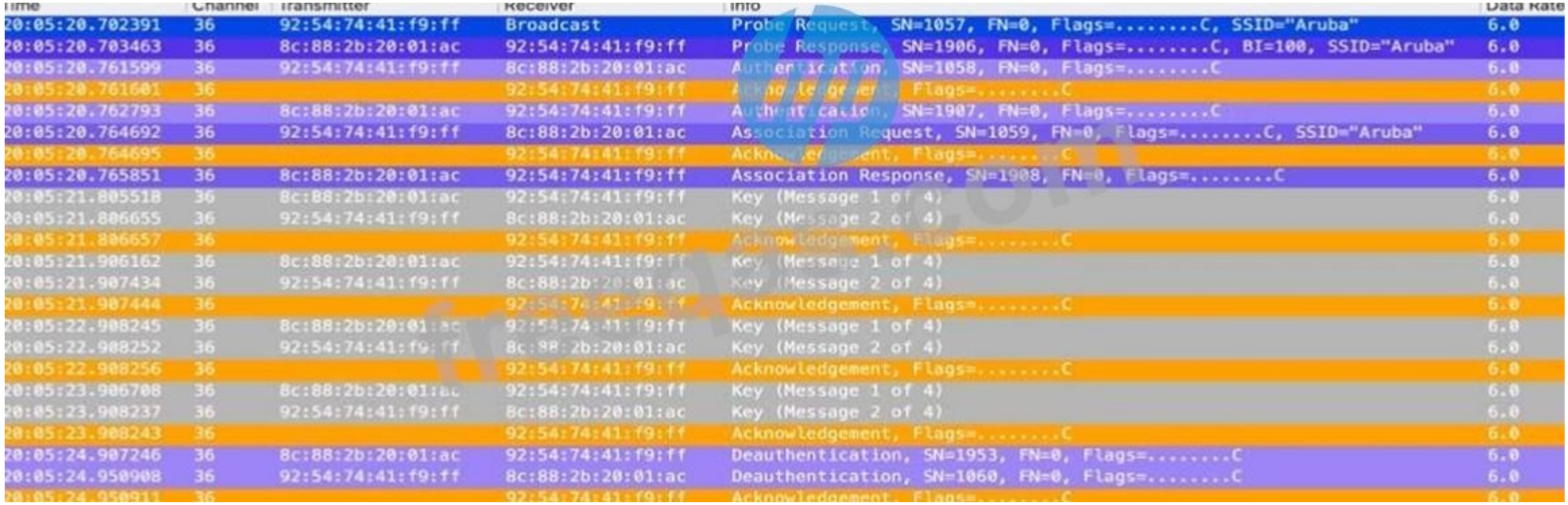
* D - SSID is mixed mode but the affected clients are bridged (those clients bypass the gateway).
* Why A, B, and E are not the best answers:
"When clients are tunneled (including mixed-mode clients that are tunneled) to the gateway, the gateway's stateful firewall and DPI engine observe the sessions and export flow/app data to Central." Thus A is not a reason for missing data.
"Client VLANs marked untrusted are evaluated by the gateway firewall/DPI and support visibility. Marking a VLAN trusted bypasses firewall enforcement, but flow visibility for tunneled WLAN clients is based on gateway DPI; the primary reason Central shows no flow attributes is that the traffic never reached the gateway (bridged path)." Therefore B/E are not the primary causes of this symptom in the scenario described.
References of HPE Aruba Networking Switching documents or Study Guide:
* Aruba AOS 10 Gateway and WLAN Configuration Guides - "Tunneled vs Bridged SSIDs and impact on gateway DPI/visibility."
* Aruba Central Operations Guide - "Client Insights data sources from mobility gateways."
* Aruba Policy Enforcement and Application Visibility - "Gateway DPI and stateful firewall as the source for app/flow telemetry for wireless clients."

NEW QUESTION: 8
You recently added ClearPass as an authentication server to an HPE Aruba Networking Central group.
RADIUS authentication with Local User Roles (LUR) works fine Out the same access points cannot use Downloadable User Roles (DUR).
What should he corrected in this configuration to fa the issue with DUR?
A. Add a new Enforcement Policy of type "WEBAUTH"on ClearPass and associate it with the matching service on ClearPass
B. Add the correct IP addresses or IP subnets of the Network Access Devices(NADs) under the "Devices" tabon ClearPass
C. Replace the AP's expiree digital certificate using the "crypto pki-import pem serverCert" command.
D. Add the correct values for "CPPM username" and "CPPM Password" m the authentication server configuration on HPEAruba Networking Central
Answer: B (LEAVE A REPLY)
For Downloadable User Roles (DUR) to function correctly with ClearPass, the Network Access Devices (NADs) need to be correctly defined in ClearPass under the "Devices" tab. This ensures that ClearPass can identify and communicate with the NADs to deliver the appropriate user roles. If the NADs are not correctly defined, ClearPass will not be able to provide the DURs to the access points for enforcement. This is a common configuration step that is required to integrate ClearPass with network devices for advanced role-based access control.

NEW QUESTION: 9
A university owns a campus with several buildings segmented into east and west wings, which are L3 separated. The east wing has 1600 APs. and the west wing has 1200 Aps. Each wing has a single gateway cluster managed by HPE Aruba Networking Central. Each cluster contains one 7210 mobility gateway The gateways are configured with DHCP relay and route all client VLANs. A new business-critical facultyreal-time application requires users to roam within wings but not across wings without disconnections or delay increments.
Which changes must the network administrator make lo successfully meet the requirement without performance degradation matching best practices? (Select two.)
A. Replace the 7210 mobility gateway in the west wing with a pair of 7030 mobility gateways.
B. Add a single 7210 mobility gateway to each cluster.
C. Remove the DHCP relay from the gateways and enable the DHCP server instead
D. Replace me 7210 mobility gateway in the east wing with a pair or 9012 mobility gateways
E. Run L2 for all SSIDs and permit the users' VLANs in the gateway's uplinks.
Answer: B,E (LEAVE A REPLY)
To support a business-critical faculty real-time application that requires seamless roaming within wings without cross-wing roaming, it's essential to ensure high availability and sufficient capacity. Adding an additional 7210 mobility gateway to each cluster would provide the required redundancy and capacity.

Running L2 for all SSIDs and permitting user VLANs on gateway uplinks would facilitate the necessary traffic flow without L3 segmentation issues, thus supporting seamless roaming within each wing.

NEW QUESTION: 10
Refer to the exhibit.



Time	Channel	Transmitter	Receiver	Info	Data Rate
20:05:20.702391	36	92:54:74:41:f9:ff	Broadcast	Probe Request, SN=1057, FN=0, Flags=........C, SSID="Aruba"	6.0
20:05:20.703463	36	8c:88:2b:20:01:ac	92:54:74:41:f9:ff	Probe Response, SN=1906, FN=0, Flags=........C, BI=100, SSID="Aruba"	6.0
20:05:20.761599	36	92:54:74:41:f9:ff	8c:88:2b:20:01:ac	Authentication, SN=1058, FN=0, Flags=........C	6.0
20:05:20.761601	36		92:54:74:41:f9:ff	Acknowledgement, Flags=........C	6.0
20:05:20.762793	36	8c:88:2b:20:01:ac	92:54:74:41:f9:ff	Authentication, SN=1907, FN=0, Flags=........C	6.0
20:05:20.764692	36	92:54:74:41:f9:ff	8c:88:2b:20:01:ac	Association Request, SN=1059, FN=0, Flags=........C, SSID="Aruba"	6.0
20:05:20.764695	36		92:54:74:41:f9:ff	Acknowledgement, Flags=........C	6.0
20:05:20.765851	36	8c:88:2b:20:01:ac	92:54:74:41:f9:ff	Association Response, SN=1908, FN=0, Flags=........C	6.0
20:05:21.805518	36	8c:88:2b:20:01:ac	92:54:74:41:f9:ff	Key (Message 1 of 4)	6.0
20:05:21.806655	36	92:54:74:41:f9:ff	8c:88:2b:20:01:ac	Key (Message 2 of 4)	6.0
20:05:21.806657	36		92:54:74:41:f9:ff	Acknowledgement, Flags=........C	6.0
20:05:21.906162	36	8c:88:2b:20:01:ac	92:54:74:41:f9:ff	Key (Message 1 of 4)	6.0
20:05:21.907434	36	92:54:74:41:f9:ff	8c:88:2b:20:01:ac	Key (Message 2 of 4)	6.0
20:05:21.907444	36		92:54:74:41:f9:ff	Acknowledgement, Flags=........C	6.0
20:05:22.908245	36	8c:88:2b:20:01:ac	92:54:74:41:f9:ff	Key (Message 1 of 4)	6.0
20:05:22.908252	36	92:54:74:41:f9:ff	8c:88:2b:20:01:ac	Key (Message 2 of 4)	6.0
20:05:22.908256	36		92:54:74:41:f9:ff	Acknowledgement, Flags=........C	6.0
20:05:23.906708	36	8c:88:2b:20:01:ac	92:54:74:41:f9:ff	Key (Message 1 of 4)	6.0
20:05:23.908237	36	92:54:74:41:f9:ff	8c:88:2b:20:01:ac	Key (Message 2 of 4)	6.0
20:05:23.908243	36		92:54:74:41:f9:ff	Acknowledgement, Flags=........C	6.0
20:05:24.907246	36	8c:88:2b:20:01:ac	92:54:74:41:f9:ff	Deauthentication, SN=1953, FN=0, Flags=........C	6.0
20:05:24.950908	36	92:54:74:41:f9:ff	8c:88:2b:20:01:ac	Deauthentication, SN=1060, FN=0, Flags=........C	6.0
20:05:24.950911	36		92:54:74:41:f9:ff	Acknowledgement, Flags=........C	6.0

Which statement is true?
A. The client performed passive scanning
B. The client is using BSS Fast Transition
C. The client is failing 802.1X authentication
D. The client used an incorrect passphrase
Answer: C (LEAVE A REPLY)
The exhibit shows a series of 802.1X authentication steps with multiple "Deauthentication" frames, which indicate that the client is not successfully completing the authentication process. Since the frames show repeated attempts at authentication followed by deauthentication, this suggests that the client is failing the 802.1X authentication process, which is required for network access in a WPA2/WPA3-Enterprise security environment.

NEW QUESTION: 11
An AOS 10 multi-site deployment has sites with AP-only bridged SSIDs and other sites with APs and gateways operating tunneled SSiDs. Client session state sync errors exist between secure lab environments and public -facing areas at several sites.
What is causing the issues?
A. The DTLS connections are down between APs in the lab and APs in public areas
B. The affected clients are associated with an SSID with 11r and 11k disabled.
C. The sites with issues are the overlay AP with gateway sites because the connection to HPE Aruba Networking central is interrupted
D. The sites with issues are the AP-only deployments because the connection to HPE Aruba Networking Central is interrupted
Answer: C (LEAVE A REPLY)

In a multi-site deployment with a mix of bridged and tunneled SSIDs, if there are session sync errors between different areas, it could be due to connectivity issues with the central management platform, which in the case of Aruba, is likely HPE Aruba Networking Central. This interruption could cause inconsistencies in session states across the network.

NEW QUESTION: 12

Which statement is true given the following CLI output from a CX 6300?

```
Central-3-Edge# show bgp l2 evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 172.21.10.3

     Network                                          Nexthop          Metric     LocPrf     Weight
-------------------------------------------------------------------------------------------------
Route Distinguisher: 172.21.11.2:200      (L2VNI 200)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]      172.21.11.2      0          100        0
*>i [3]:[0]:[172.21.11.2]                             172.21.11.2      0          100        0

Route Distinguisher: 172.21.11.3:200      (L2VNI 200)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]      172.21.11.3      0          100        0
*>  [3]:[0]:[172.21.11.3]                             172.21.11.3      0          100        0

Route Distinguisher: 172.21.11.2:201      (L2VNI 201)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.201.1.1]      172.21.11.2      0          100        0
*>i [2]:[0]:[0]:[78:98:e8:c0:c7:f2]:[10.201.1.100]    172.21.11.2      0          100        0
*>i [2]:[0]:[0]:[78:98:e8:c0:c7:f2]:[]                172.21.11.2      0          100        0
*>i [3]:[0]:[172.21.11.2]                             172.21.11.2      0          100        0

Route Distinguisher: 172.21.10.1:10010    (L3VNI 10010)
*>i [5]:[0]:[0]:[0]:[0.0.0.0]                         172.21.11.1      0          100        0
*>i [5]:[0]:[0]:[24]:[172.21.111.0]                   172.21.11.1      0          100        0

Route Distinguisher: 172.21.10.2:10010    (L3VNI 10010)
*>i [5]:[0]:[0]:[24]:[10.200.1.0]                     172.21.11.2      0          100        0
*>i [5]:[0]:[0]:[24]:[10.201.1.0]                     172.21.11.2      0          100        0

Route Distinguisher: 172.21.10.3:10010    (L3VNI 10010)
*>  [5]:[0]:[0]:[24]:[10.200.1.0]                     172.21.11.3      0          100        0
*>  [5]:[0]:[0]:[24]:[10.201.1.0]                     172.21.11.3      0          100        0

Route Distinguisher: 172.21.11.2:200      (L3VNI 10010)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]      172.21.11.2      0          100        0

*>i [2]:[0]:[0]:her: 172.21.11.2:201      (L3VNI 10010)   172.21.11.2   0   100   0
*>i [2]:[0]:[0]:[78:98:e8:c0:c7:f2]:[]                172.21.11.2      0          100        0

Route Distinguisher: 172.21.11.3:200      (L3VNI 10010)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]      172.21.11.3      0          100        0

Route Distinguisher: 172.21.11.3:201      (L3VNI 10010)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.201.1.1]      172.21.11.3      0          100        0
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[10.201.1.101]    172.21.11.3      0          100        0
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[]                172.21.11.3      0          100        0
Total number of entries 26
```

A. The underlay loopback addresses are in the 172 21 11 x range.

B. There are two anycast addresses m me overlay fabric.

C. Duplicate MAC addresses were detected in the overlay fabric

D. There are three active client overlay VLANs in the overlay fabric

Answer: (SHOW ANSWER)

The CLI output displays EVPN routes and their corresponding next hops. The "Route Distinguisher" entries followed by IP addresses in the 172.21.11.x range indicate these are loopback addresses used by the underlay network. The underlay network provides the basic routing and forwarding plane for the overlay network that EVPN is part of. These loopback addresses are crucial for the proper functioning of the EVPN control plane.

NEW QUESTION: 13
Anetworkadministrator accesses HPE Aruba Networking Central and notices that visitors consume too much internet bandwidth starving employee traffic when accessing an external service.Therefore,the administrator wants to limitwireless bandwidth to 60 Mops in both directions among all users in the voice rote and no more than 10 Mops in both directions for YouTube traffic. Deep packet inspection, web contentclassification, andfirewall visibility are enabled.
Which configurations are required to accomplish this task? (Select two.)

A.

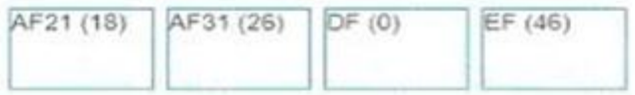
B.

C.

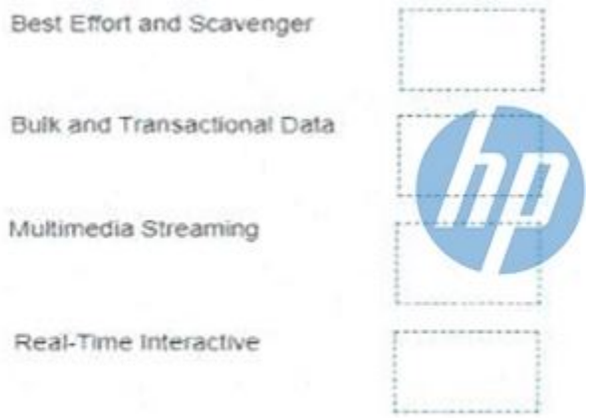
D.

Answer: B,D (LEAVE A REPLY)
To achieve the bandwidth limits set by the network administrator, both per-application and total limits need to be configured. Option B shows the configuration for setting a per-application bandwidth limit, which can restrict YouTube traffic to 10 Mbps in both directions. Option D shows the configuration for setting a total bandwidth limit for all users within the voice role to 50000 Kbps (or 50 Mbps), satisfying the requirement to restrict total wireless bandwidth. By applying these configurations in HPE Aruba Networking Central, the administrator will successfully implement the necessary controls to ensure that visitor traffic does not impede the network performance for employee traffic, aligning with the capabilities of Aruba solutions to manage and prioritize network resources effectively.

NEW QUESTION: 14
Your customer is requesting a 4-ciass LAN queuing model tor QoS. Following best practices, match the PHB /DSCP values to the application types.



Answer Area



Answer:

Explanation:
Best Effort and Scavenger = DF (0)
Bulk and Transactional Data = AF21 (18)
Multimedia Streaming = AF31 (26)
Real-Time Interactive = EF (46)

NEW QUESTION: 15
Exhibit.

```
(MC2) #show auth-tracebuf mac 70:4d:7b:10:9e:c6 count 27

Warning: user-debug is enabled on one or more specific MAC addresses;
         only those MAC addresses appear in the trace buffer.

Auth Trace Buffer
-----------------


Jun 29 20:56:51  station-up              *   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -     -    wpa2 aes
Jun 29 20:56:51  eap-id-req             <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1     5
Jun 29 20:56:51  eap-start              ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -     -
Jun 29 20:56:51  eap-id-req             <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1     5
Jun 29 20:56:51  eap-id-resp            ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1     7    it
Jun 29 20:56:51  rad-req                ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          42    174  10.1.140.101
Jun 29 20:56:51  eap-id-resp            ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1     7    it
Jun 29 20:56:51  rad-resp               <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  42    88
Jun 29 20:56:51  eap-req                <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          2     6
Jun 29 20:56:51  eap-resp               ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          2     214
Jun 29 20:56:51  rad-req                ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  43    423  10.1.140.101
Jun 29 20:56:51  rad-resp               <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  43    228
Jun 29 20:56:51  eap-req                <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          3     146
Jun 29 20:56:51  eap-resp               ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          3     61
Jun 29 20:56:51  rad-req                ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  44    270  10.1.140.101
Jun 29 20:56:51  rad-resp               <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  44    128
Jun 29 20:56:51  eap-req                <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          4     46
Jun 29 20:56:51  eap-resp               ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          4     46
Jun 29 20:56:51  rad-req                ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  45    255  10.1.140.101
Jun 29 20:56:51  rad-accept             <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  45    231
Jun 29 20:56:51  eap-success            <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          4     4
Jun 29 20:56:51  user repkey change     *   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          65535 -    204c0306e790000000170008
Jun 29 20:56:51  macuser repkey change  *   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          65535 -    70:4d:7b:10:9e:c6
Jun 29 20:56:51  wpa2-key1              <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -     117
Jun 29 20:56:51  wpa2-key2              ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -     117
Jun 29 20:56:51  wpa2-key3              <-   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -     151
Jun 29 20:56:51  wpa2-key4              ->   70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -     95
```

Which wireless connection phase has Just been completed?

A. MAC Authentication and 4-way handshake

B. L3 authentication and encryption

C. 802.11 enhanced open association

D. L2 authentication and encryption

Answer: D (LEAVE A REPLY)

The wireless connection phase that has just been completed is L2 authentication and encryption. This phase includes processes such as the Extensible Authentication Protocol (EAP) exchange, RADIUS requests and responses, and the 4-way handshake which is characteristic of WPA2-AES encryption.

NEW QUESTION: 16

The ACME company has an AOS-CX 6200 switch stack with an uplink oversubscription ratio of 9.6:1. They are considering adding two more nodes to the stack without adding any additional uplinks due to cabling constraints One of their architects has expressed concerns that their critical UDP traffic from both wired and bridged AP clients will encounter packet drops. They have already applied the following configuration:

```
vsf1(config)# qos threshold-profile acmethreshold
vsf1(config-threshold)# queue 0 action wred-resp yellow min-threshold 40 percent max-threshold 80 percent
vsf1(config)# int lag 1
vsf1(config-if)# description uplink-to-collapsed-core
vsf1(config-if)# apply qos threshold-profile acmethreshold
```

```
vsf1# show qos dscp-map default
DSCP     code_point local_priority cos color   name
-------- ---------- -------------- --- ------- ----
000000   0          1                  green   CS0
000001   1          1                  green
000010   2          1                  green
000011   3          1                  green
000100   4          1                  green
000101   5          1                  green
000110   6          1                  green
000111   7          1                  green
001000   8          0                  green   CS1
001001   9          0                  green
001010   10         0                  green   AF11
001011   11         0                  green
001100   12         0                  yellow  AF12
001101   13         0                  green
001110   14         0                  yellow  AF13
001111   15         0                  green
010000   16         2                  green   CS2
010001   17         2                  green
010010   18         2                  green   AF21
010011   19         2                  green
010100   20         2                  yellow  AF22
010101   21         2                  green
010110   22         2                  yellow  AF23
010111   23         2                  green
011000   24         3                  green   CS3
011001   25         3                  green
011010   26         3                  green   AF31
011011   27         3                  green
011100   28         3                  yellow  AF32
011101   29         3                  green
011110   30         3                  yellow  AF33
011111   31         3                  green
100000   32         4                  green   CS4
100001   33         4                  green
100010   34         4                  green   AF41
100011   35         4                  green
100100   36         4                  yellow  AF42
100101   37         4                  green
100110   38         4                  yellow  AF43
100111   39         4                  green
101000   40         5                  green   CS5
101001   41         5                  green
101010   42         5                  green
101011   43         5                  green
101100   44         5                  green
101101   45         5                  green
101110   46         5                  green   EF
101111   47         5                  green
110000   48         6                  green   CS6
110001   49         6                  green
110010   50         6                  green
110011   51         6                  green
110100   52         6                  green
110101   53         6                  green
110110   54         6                  green
110111   55         6                  green
111000   56         7                  green   CS7
111001   57         7                  green
111010   58         7                  green
111011   59         7                  green
111100   60         7                  green
111101   61         7                  green
111110   62         7                  green
111111   63         7                  green
```

Which strategy will complement this solution to achieve their objective?

A. edge mark lower priority TCP traffic with AF12

B. edge mark critical UDP Traffic with CSS

C. edge mark lower priority TCP traffic with AF11

D. edge mark critical UDP traffic with AF42

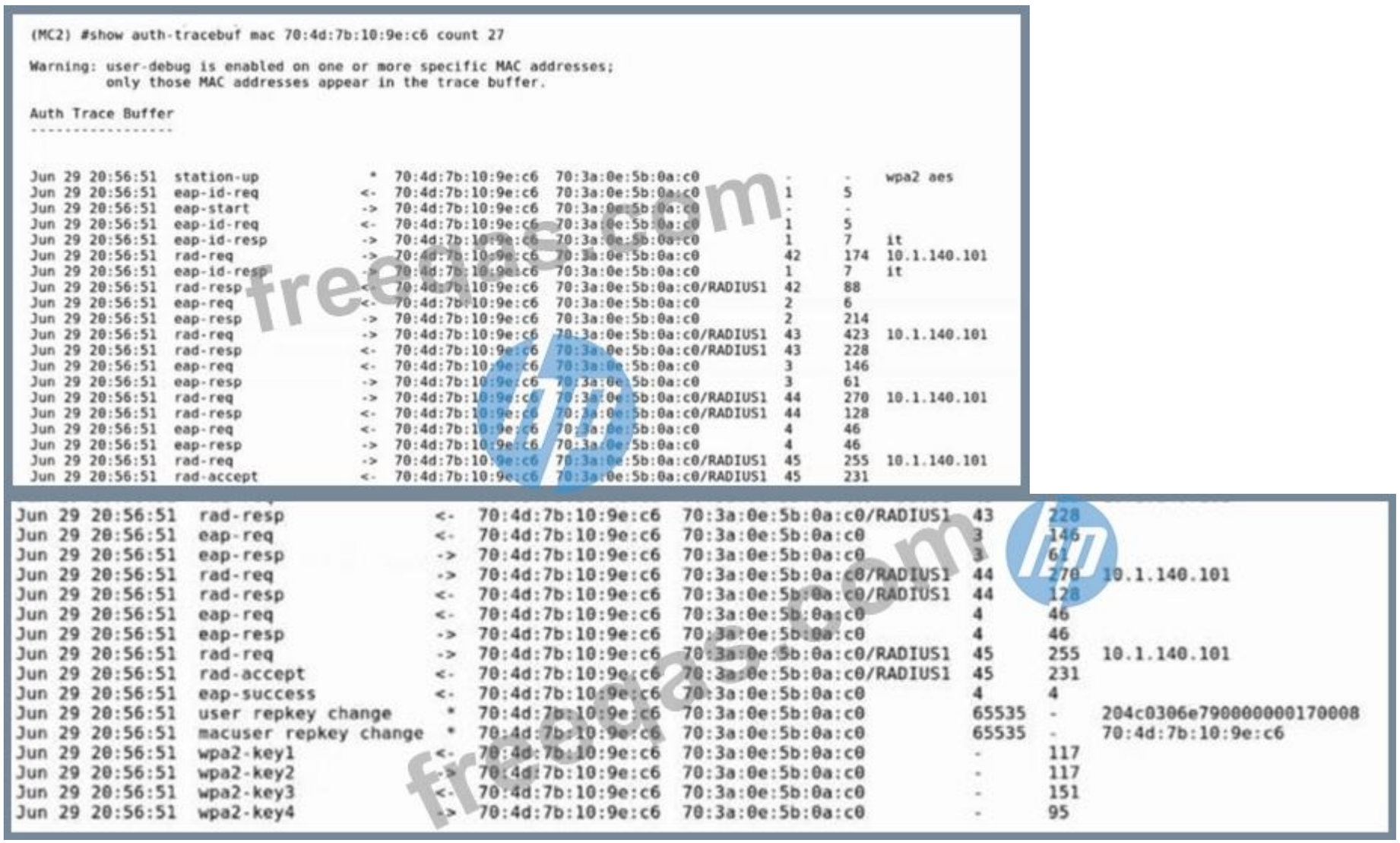
Answer: (SHOW ANSWER)

Given that the ACME company's concern is about UDP traffic potentially encountering packet drops due to uplink oversubscription, they need a strategy that prioritizes critical UDP traffic to minimize loss.

Option D, edge mark critical UDP traffic with AF42, is the correct answer. Assured Forwarding (AF) classes provide a way to assign different levels of delivery assurance for IP packets. AF42 is typically used for traffic that requires low latency and low loss, such as voice and video, which often use UDP. Marking critical UDP traffic with AF42 will help ensure that this traffic is treated with higher priority over the network.

Option A (edge mark lower priority TCP traffic with AF12) and Option C (edge mark lower priority TCP traffic with AF11) suggest marking lower priority TCP traffic, which does not directly address the concern for critical UDP traffic.
Option B (edge mark critical UDP Traffic with CS5) suggests using Class Selector 5 for critical UDP traffic, which is also a valid approach but does not match the existing configuration that is focused on Assured Forwarding (AF) classes.

NEW QUESTION: 17
Refer to the exhibit.



```
(MC2) #show auth-tracebuf mac 70:4d:7b:10:9e:c6 count 27

Warning: user-debug is enabled on one or more specific MAC addresses;
         only those MAC addresses appear in the trace buffer.

Auth Trace Buffer
-----------------

Jun 29 20:56:51  station-up            *  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -     -    wpa2 aes
Jun 29 20:56:51  eap-id-req           <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1     5
Jun 29 20:56:51  eap-start            ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -     -
Jun 29 20:56:51  eap-id-req           <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1     5
Jun 29 20:56:51  eap-id-resp          ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1     7    it
Jun 29 20:56:51  rad-req              ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          42    174  10.1.140.101
Jun 29 20:56:51  eap-id-resp          ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1     7    it
Jun 29 20:56:51  rad-resp             <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  42    88
Jun 29 20:56:51  eap-req              <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          2     6
Jun 29 20:56:51  eap-resp             ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          2     214
Jun 29 20:56:51  rad-req              ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  43    423  10.1.140.101
Jun 29 20:56:51  rad-resp             <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  43    228
Jun 29 20:56:51  eap-req              <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          3     146
Jun 29 20:56:51  eap-resp             ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          3     61
Jun 29 20:56:51  rad-req              ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  44    270  10.1.140.101
Jun 29 20:56:51  rad-resp             <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  44    128
Jun 29 20:56:51  eap-req              <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          4     46
Jun 29 20:56:51  eap-resp             ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          4     46
Jun 29 20:56:51  rad-req              ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  45    255  10.1.140.101
Jun 29 20:56:51  rad-accept           <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  45    231
```

A network administrator is validating client connectivity and executes the show command shown in the exhibit. Which authentication method was used by the wireless station?

A. MAC authentication
B. 802.1X user authentication
C. WEBauth authentication

D. 802.1X machine authentication

Answer: B (LEAVE A REPLY)

The provided output is from the command:

(MC2) #show auth-tracebuf mac <MAC>

This command traces the authentication exchange between the access point (or mobility controller) and the RADIUS server for a specific client. The trace provides insight into the 802.1X authentication sequence and RADIUS responses.

From the exhibit:

* EAPOL (Extensible Authentication Protocol over LAN) Messages Observed:
* eap-id-req
* eap-id-resp
* eap-req
* eap-resp
* eap-success

These messages clearly indicate that an 802.1X (EAP-based) authentication took place. MAC authentication (MAB) or WebAuth would not include multiple EAP identity and response messages.

* RADIUS Messages:
* rad-req, rad-resp, rad-accept from /RADIUS1
* The presence of rad-accept indicates successful authentication.

Exact extract from ArubaOS (AOS-S/AOS 10 WLAN Authentication Guide):

"When the trace output shows EAP identity requests, EAP responses, and a RADIUS Access-Accept message, the authentication method in use is 802.1X (EAP-based user authentication). The presence of EAP-Success following the Access-Accept confirms successful 802.1X authentication."

* Follow-on WPA2 Key Exchange:
* Lines show wpa2-key1, wpa2-key2, wpa2-key3, and wpa2-key4.
* This sequence occurs after 802.1X authentication completes and is used to establish encryption keys for a WPA2 Enterprise session.

Exact extract from Aruba WLAN Troubleshooting Guide:

"After successful 802.1X authentication (EAP-Success), the controller exchanges four WPA2 keys with the station to derive the session keys used for data encryption. This confirms WPA2-Enterprise with 802.1X was used."

* No Indication of MAC or WebAuth:
* MAC authentication would show mac-auth or macauth messages instead of eap-id-req/resp.
* WebAuth involves HTTP-based redirection and is not visible in auth-tracebuf as EAP transactions.

Exact extract:

"MAC authentication shows 'macauth start' and 'macauth accept' entries, not EAPOL frames. WebAuth authentication uses a web redirect and does not appear as EAP frames in the trace buffer." Therefore, the trace confirms a WPA2-Enterprise 802.1X user authentication, where the user's credentials were validated by the RADIUS server, followed by the WPA2 key handshake.

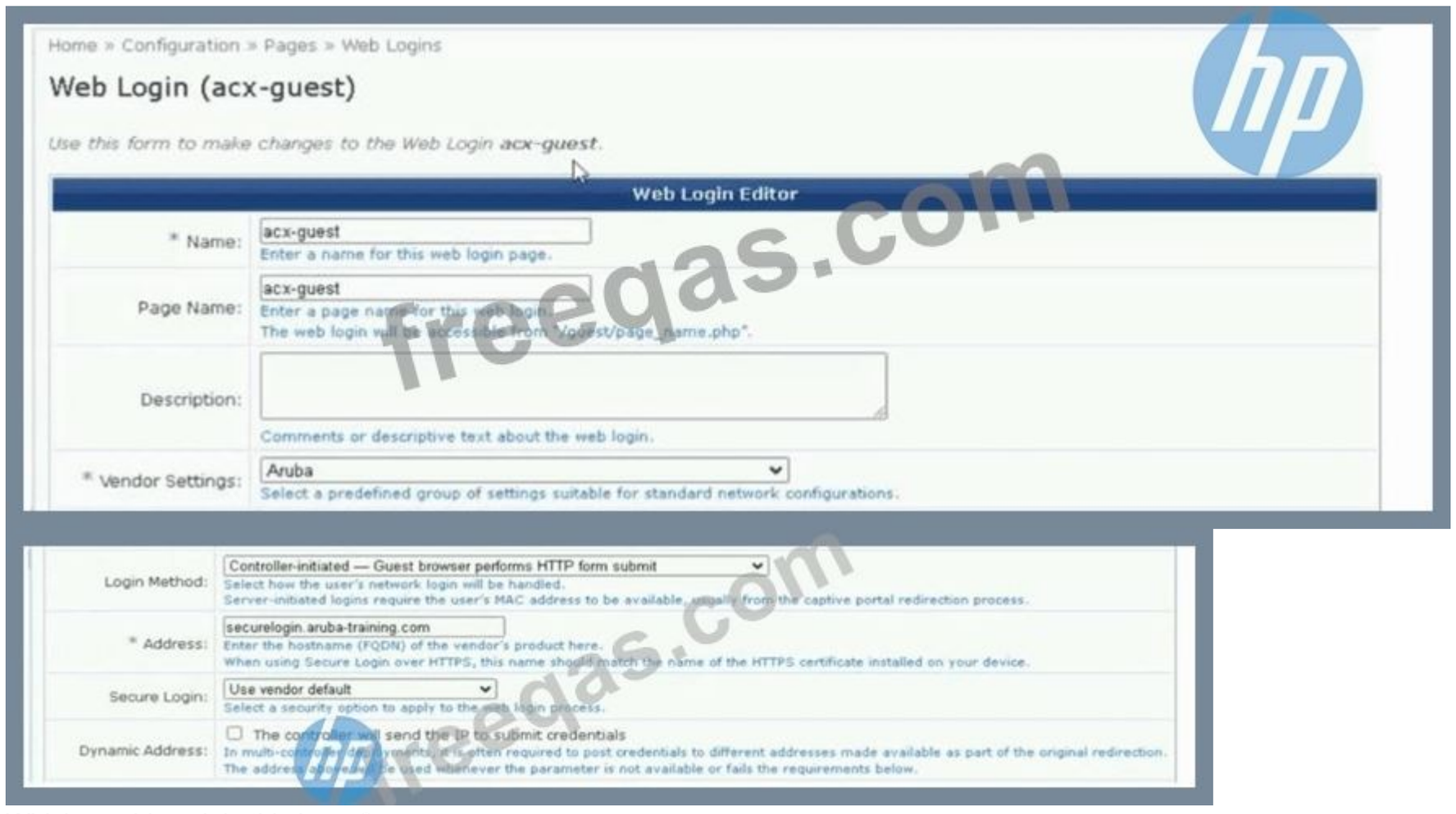
Why the Other Options Are Incorrect:

* A. MAC authentication:Would show MAC-based request/response entries (macauth), not eap-id-req /resp.
* C. WEBauth authentication:WebAuth occurs over HTTP/HTTPS and does not involve EAP messages; thus, no eap-id or eap-success would be seen.
* D. 802.1X machine authentication:Machine authentication occurs before user logon and is typically identified in logs by a computer account (e.g., host/computername$). Here, the username and context indicate a user-level session.

References of HPE Aruba Networking Switching Documents or Study Guide:

* ArubaOS 8/10 WLAN Authentication and Security Configuration Guide - "802.1X EAP Authentication and Trace Analysis."
* Aruba WLAN Troubleshooting Guide - "Using show auth-tracebuf to validate EAP authentication."
* Aruba Campus Wireless Design Fundamentals - "Understanding WPA2-Enterprise authentication flow (EAPOL, RADIUS, WPA2 4-Way Handshake)."
* Aruba Access Security and AAA Implementation Guide - "Distinguishing between MAC, WebAuth, and 802.1X authentication in debug outputs."

NEW QUESTION: 18
A customer reports that their HPE Aruba Networking ClearPass Guest captive portal is not functioning. The page loads but they are unable to browse after pressing connect. They have uploaded a valid and publicly trusted *. aruba-training.com certificate.
Refer to the exhibit.



Which would explain this issue?
A. aruba-training.com needs to be entered in the Address field for the ClearPass Guest
B. captiveportal-login.aruba-training.com needs to be entered in the Address field for the ClearPass Guest
C. HTTPS certificate is not required in ClearPass Guest
D. HTTPS wildcard certificates are not supported
Answer: (SHOW ANSWER)
In HPE Aruba ClearPass Guest configuration, the "Address" field defines the Fully Qualified Domain Name (FQDN) of the captive portal server that users are redirected to when accessing the guest network.
When a wildcard certificate is used, such as *.aruba-training.com, the derived FQDN for the captive portal redirection automatically becomes: captiveportal-login.aruba-training.com

This naming convention is required so that the Common Name (CN) or Subject Alternative Name (SAN) in the SSL certificate matches the domain presented to the client browser during HTTPS redirection.
If the "Address" field is incorrectly configured with just aruba-training.com, the certificate and the redirection URL will not match, causing the browser to block or fail the authentication process. This results in users being unable to browse after pressing Connect on the portal page.
HPE Aruba documentation states:
"When using a wildcard certificate (for example CN = *.domain.com) on ClearPass Guest, the web login redirection address must be configured as captiveportal-login.domain.com to ensure the HTTPS certificate name matches the redirection hostname."
"If the address field does not match the derived hostname of the certificate, browser trust validation fails and users cannot proceed beyond the captive portal page." Additionally, the ArubaOS and ClearPass Guest deployment guide clarifies that wildcard certificates are fully supported for guest portals, provided that the Address field follows the proper naming pattern.
Incorrect Configurations:
* Setting "Address" to aruba-training.com causes SSL mismatch errors.
* Leaving the "Address" blank defaults to a local IP or hostname mismatch.
Correct Configuration:
* "Address" should be set to captiveportal-login.aruba-training.com when the wildcard certificate is *.
aruba-training.com.
Option Explanations:
* A. Incorrect - this does not follow the certificate's derived FQDN format.
* B. Correct - matches the expected derived FQDN for wildcard certificates.
* C. Incorrect - HTTPS certificates are required for secure guest portals.
* D. Incorrect - Wildcard certificates are supported by ClearPass Guest and ArubaOS.
Final Verified answer: B
Reference Sources (HPE Aruba Networking Official Materials):
* Aruba ClearPass Guest Configuration and Deployment Guide
* ArubaOS 8.x User Guide - Captive Portal and Authentication Configuration
* HPE Aruba ClearPass Certificates 101 Technical Note
* ArubaOS-Switch and ClearPass Integration Guide

NEW QUESTION: 19
A BGP routing table contains multiple routes to the same destination prefix.
Referring to the table below which route would be marked with a ">" symbol?

Route	Distance	Metric	Origin Code	Local Preference
A		200	i	0
B		0	?	100
C		20	?	0
D	200	0	i	100
E	20	0	i	100

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

E. Option E

Answer: E (LEAVE A REPLY)

In BGP, the route marked with a ">" symbol is the best route that is chosen based on BGP attributes in the following order: highest weight (Cisco-specific), highest local preference, originated by BGP running on the local router, shortest AS path, lowest origin type, lowest MED, eBGP over iBGP, closest IGP neighbor, and lowest BGP router ID. Based on the table provided, Option E would be marked with a ">" symbol as it has the highest local preference of 100 which is a decisive factor in the BGP best path selection process.

NEW QUESTION: 20

You configured" a bridged mode SSID with WPA3-Enterprise and EAP-TLS security. When you connect an Active Directory joined client that has valid client certificates. ClearPass shows the following error.

What is needed to resolve this issue?

A. Enable authorization in your Authentication Method.

B. Recreate the SSID m tunneled mode.

C. Modify your ACX-AD authentication source to include the UPN in the search.

D. Configure ClearPass to trust the client certificate.

Answer: C (LEAVE A REPLY)

The error message "User not found" indicates that the authentication source, in this case, Active Directory (AD), is not able to locate the user account based on the current search parameters. This often occurs when the User Principal Name (UPN) that the client is using to authenticate is not included in the search parameters of the AD authentication source within ClearPass. By modifying the AD authentication source to include the UPN in the search, ClearPass will be able to correctly locate the user account and proceed with the authentication using the valid client certificates.

NEW QUESTION: 21

What is the recommended configuration to ensure link aggregation is consistent in a campus topology using VSX with two aggregation switches and downlinks to access switches?

A. Use the command "vsx-sync active-gateways" under the VSX context.

B. Use a custom LACP hash algorithm for improved load balancing.

C. Use the command "vsx-sync mclag-interfaces" from the global context.

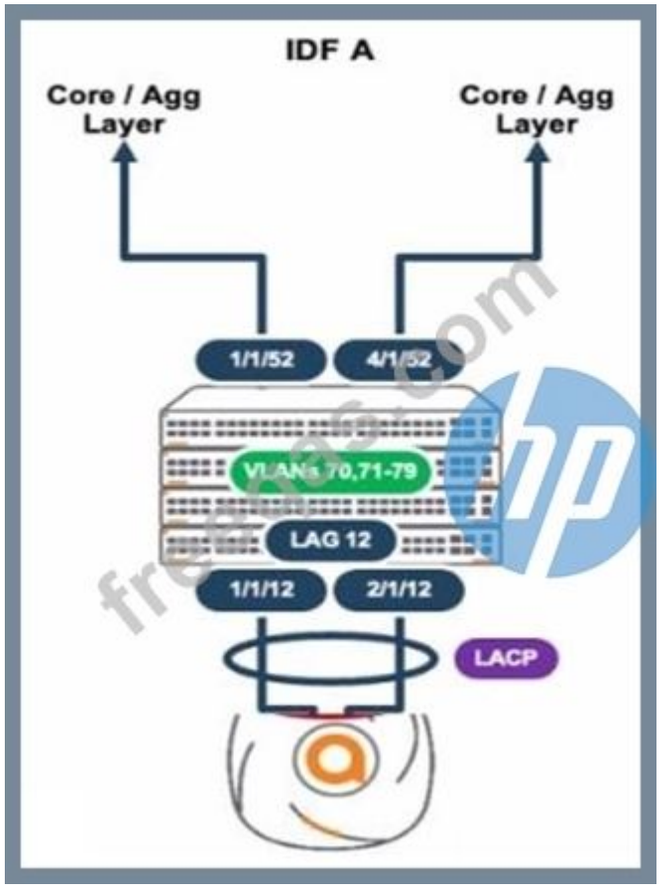
D. Use the command "vsx-sync mclag-interfaces" under the VSX context.

Answer: D (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract of HPE Aruba Networking Switching:

The VSX synchronization feature provides per-feature synchronization from the primary to the secondary VSX peer. For multi-chassis LAGs (MC-LAGs), the command that ensures both VSX peers maintain consistent LAG interface associations and attributes is entered under the VSX configuration context:
* Command syntax: vsx-sync mclag-interfaces
* Command context: config-vsx
Description (extract): Enables VSX synchronization of VSX LAG interface associations and attributes from the primary VSX switch to the secondary peer switch.
In a campus design with two aggregation switches in a VSX pair and access switches dual-homed using MC- LAG, enabling vsx-sync mclag-interfaces under the VSX context ensures consistent LAG membership, attributes, and behavior across the pair-avoiding configuration drift and aggregation inconsistencies.
References:* ArubaOS-CX VSX Command Reference; "vsx-sync mclag-interfaces" (syntax, command context, and description).* Aruba Campus Switching Best Practices with VSX; MC-LAG consistency and VSX feature synchronization guidelines.

NEW QUESTION: 22
A deployment using AP-635S is connected to a stack of CX 6300s as shown.



The output of the snow LACP interfaces shews the following:

```
SW-IDF-A# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
-------------------------------------------------------------------------------
Intf       Aggr      Port  Port  State   System-ID          System Aggr Forwarding
           Name      Id    Pri                              Pri    Key  State
-------------------------------------------------------------------------------
1/1/12     lag12     13    1     ALFNCD  88:3a:30:99:ac:40 65534  12   up
2/1/12     lag12     77    1     ALFO    88:3a:30:99:ac:40 65534  12   lacp-block
```

What is causing this issue?

A. e0 is connected to a smart rate interface, and e1 is connected to a non-smart rate interface.

B. Spanning tree and loop protect are enabled on both AP uplink ports.

C. Each AP interface is connected to a routed-only interlace on different networks

D. The AP is configured with LACP active

Answer: D (LEAVE A REPLY)

In an Aruba deployment, if an AP's interfaces show different LACP states, it often indicates a configuration mismatch. If one interface is up and the other is blocked as shown in the output, it's likely due to both interfaces on the AP being set to LACP active mode, which is a correct setting for establishing an LACP channel with Aruba switches like the CX 6300 series.

NEW QUESTION: 23

Your customer added third-party USB dongles to the USB ports of their AOS 10 access points. The customer uses AP-615 and AP-635 Each AP is connected with a Cat 6A cable to a CX 6300F Class 4 PoE switch All APs are in the same group in HPE Aruba Networking Central and share the same configuration However, many of the dongles do not come up.

Which option will solve this issue?

A. Replace the Class a PoE switches with Class 6 PoE switches.

B. Create two separate service profiles in the loT tab of the Central configuration settings.

C. Perform a "poe disable" followed by a "poe enable" for the switch ports which connect to the APs so that the APs reboot.

D. Move the AP-635 access points to a different group in Central to configure the dongles separately from the AP-615.

Answer: A (LEAVE A REPLY)

USB dongles often require additional power, which may exceed the power delivery capabilities of Class 4 PoE switches. Aruba AP-615 and AP-635 are designed to work with USB dongles that require additional power for proper operation. Since the Cat 6A cable can support higher power levels, replacing the Class 4 PoE switches with Class 6 PoE switches, which can deliver higher power, should resolve the issue with the dongles not powering up.

NEW QUESTION: 24

A BGP routing tablecontains multiple routes to the same destination prefix.

Referring to the table below whichroutewould be marked with a ">" symbol?

Route	Distance	Metric	Origin Code	Local Preference
A		200	i	0
B		0	?	100
C		20	?	0
D	200	0	i	100
E	20	0	i	100

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Answer: (SHOW ANSWER)

In BGP, the route marked with a ">" symbol is the best route that is chosen based on BGP attributes in the following order: highest weight (Cisco-specific), highest local preference, originated by BGP running on the local router, shortest AS path, lowest origin type, lowest MED, eBGP over iBGP, closest IGP neighbor, and lowest BGP router ID. Based on the table provided, Option E would be marked with a ">" symbol as it has the highest local preference of 100 which is a decisive factor in the BGP best path selection process.

NEW QUESTION: 25

A customer's infrastructure is set up to use both primary and secondary gateway clusters on the SSID profile based on best practices What is a valid cause tor having an equal spirt in APs connected to the primary and secondary gateway clusters?

A. The secondary gateway cluster is heterogeneous

B. The secondary gateway cluster is homogeneous

C. The primary gateway cluster is up. out some APs are unable to reach the primary gateway cluster. These APs would connect to the secondary gateway cluster

D. The primary gateway cluster is up. out some APs cannot reach the secondary gateway cluster. These APs would connect to the secondary gateway cluster

Answer: C (LEAVE A REPLY)

In a high availability setup where both primary and secondary gateway clusters are present, APs are typically designed to connect to the primary cluster. If the APs are equally split between the primary and secondary, this may indicate that some APs cannot reach the primary cluster due to connectivity issues or reachability constraints, thus falling back to the secondary cluster.

NEW QUESTION: 26

A customer's infrastructure is set up to use both primary and secondary gateway clusters on the SSID profile based on best practices. Why do they have an equal split of their 260 APs across the primary and secondary gateway clusters?

A. The primary gateway cluster is up, but some APs cannot reach the secondary gateway cluster. These APs would connect to the secondary gateway cluster

B. The secondary gateway cluster is homogeneous

C. The secondary gateway cluster is heterogeneous

D. The primary gateway cluster is up, but some APs cannot reach the primary gateway cluster. These APs would connect to the secondary gateway cluster

Answer: D (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract of HPE Aruba Networking Switching:

In AOS-10 wireless deployments, HPE Aruba Networking supports the configuration of Primary and Secondary Gateway Clusters in the SSID profile to ensure high availability, redundancy, and load distribution. This configuration follows Aruba's gateway clustering best practices, where access points (APs) attempt to establish tunnels with their Primary Gateway Cluster first. If the AP cannot reach the primary cluster (due to reachability, latency, or network topology), it automatically connects to the Secondary Gateway Cluster.

When both gateway clusters are active and reachable but some APs cannot reach the primary cluster-for example, due to Layer 3 routing, firewall restrictions, or network segmentation-those APs will associate with the secondary cluster instead. This results in an approximately equal split of APs across both clusters, even though the primary cluster is operational.

Exact Extract from HPE Aruba Networking Switching and AOS-10 Gateway Documentation:

"Access Points attempt to form tunnels with the Primary Gateway Cluster first. If the primary cluster is unreachable or fails to respond within the defined timeout, the AP establishes a tunnel with the Secondary Gateway Cluster."

"When the primary and secondary gateway clusters are both up but APs are distributed across separate routed networks or VLANs, APs may select the gateway cluster that is most reachable at that time, resulting in an even or partial split of AP distribution."

"This is expected behavior when APs in different subnets cannot reach the same primary cluster due to network topology. The secondary cluster provides redundancy and connectivity continuity." Therefore, the equal split of 260 APs is explained by the fact that while the primary cluster is active, a subset of APs cannot reach it due to routing or segmentation and thus join the secondary cluster-this behavior aligns with Aruba's gateway redundancy mechanism.

Why the Other Options Are Incorrect:

* A. The statement reverses the cause: APs that cannot reach the primary connect to the secondary- not the other way around. The secondary cluster's reachability does not affect AP selection when the primary is available and reachable.

"APs first attempt the primary cluster; only failure to reach it triggers fallback to secondary."

* B. Secondary cluster is homogeneous:Cluster homogeneity refers to identical hardware/software versions between gateways; it does not influence AP distribution or equal load split.

"Homogeneity is a software version consideration, not an AP load-balancing factor."
* C. Secondary cluster is heterogeneous:Heterogeneity (mixed hardware types) is unsupported or discouraged; it does not cause AP distribution behavior. "Heterogeneous gateway clusters are not a cause of AP distribution variation; cluster type does not dictate AP split." References of HPE Aruba Networking Switching Documents or Study Guide:
* ArubaOS 10 Gateway and AP Deployment Guide - "Primary and Secondary Gateway Cluster Configuration and AP Association Logic."
* Aruba High Availability and Clustering Best Practices Guide - "Gateway Cluster Failover, Redundancy, and AP Selection."
* Aruba Central Cloud Management and Monitoring Guide - "SSID Profile Configuration: Primary and Secondary Gateway Clusters."
* Aruba Campus Wireless Design Guide (AOS 10.x) - "Cluster Reachability, Redundancy, and Role Propagation Across Gateways."

NEW QUESTION: 27
In a campus topology using VSX with two aggregation switches and downlinks to access switches, which LAG interface configuration at the aggregation layer is correct based on the parameters below?
* ZTP VLAN 1001
* access switch MGMT VLAN 2002
* access switch MGMT VLAN is tagged
* connectivity to the access switch should be maintained before and after the ZTP operation is complete

A.
```
interface lag 150 multi-chassis
    no shutdown
    description ZTP2ACCESS_SW
    no routing
    vlan trunk native 1001
    vlan trunk allowed all
    lacp mode active
    lacp fallback
```

B.
```
interface lag 150 multi-chassis
    no shutdown
    description ZTP2ACCESS_SW
    no routing
    vlan trunk native 1001
    vlan trunk allowed all
    lacp mode passive
```

C.
```
interface lag 150 multi-chassis
    no shutdown
    description ZTP2ACCESS_SW
    no routing
    vlan trunk native 2002
    vlan trunk allowed 1001,2002
    lacp mode active
    lacp fallback
```

D.
```
interface lag 150
    no shutdown
    description ZTP2ACCESS_SW
    no routing
    vlan trunk native 1001
    vlan trunk allowed 1001,2002
    lacp mode active
    lacp fallback
```

Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
Exhibit.

An engineer has applied the above configuration to R1 and R2 However the routers OSPF adjacency never progresses past the "EXSTART-DR" slate as shown below.

```
R2(config)# show ip ospf neighbors
VRF : default                              Process : 1
=================================================

Total Number of Neighbors : 1

Neighbor ID      Priority  State            Nbr Address       Interface
-------------------------------------------------------------------------
10.255.1.0       1         EXSTART/DR       10.255.1.0         1/1/1
```

Which configuration action on either router will allow R1 and R2 to progress past the "EXSTART/DR" state?

A. Change R1 and R2 to a network type of point-to-point.

B. Remove the layer 3 MTU configuration.

C. Ensure the OSPF process is not configured with passive-interface default.

D. Change the IP address and mask applied to interface 1/1/1.

Answer: (SHOW ANSWER)

In OSPF, the "EXSTART/DR" state indicates that the routers are trying to establish an adjacency but are unable to progress. This can happen if the OSPF network type is incorrectly configured for the type of connection between the routers. Given that R1 and R2 are connected via a point-to-point link (as suggested by the /31 subnet), setting the network type to point-to-point on both routers will remove the need for DR/BDR election, which is unnecessary on a point-to-point link, and allow OSPF to progress past the "EXSTART" state and form a full adjacency.

NEW QUESTION: 29

A campus topology uses VSX with a collapsed core topology. The customer added redundant SFP+ transceivers and reconfigured their mobility gateways from a single link to an aggregate Link. You are asked to verify the CLI output for the link aggregation configuration for one of the mobility gateway cluster members below.

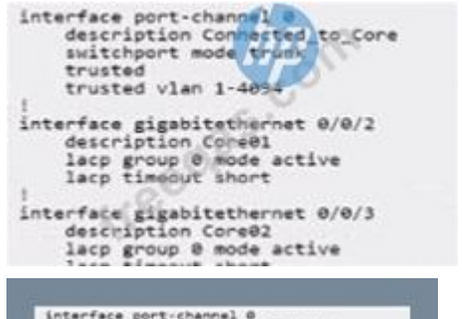
```
interface lag 100 multi-chassis
    no shutdown
    description ArubaGWY_01
    no routing
    vlan trunk native 100
    vlan trunk allowed all
    lacp mode active
    lacp rate fast
```

What is a valid configuration?

A.

B.

C.



D.

Answer: A (LEAVE A REPLY)

The configuration shown in Option A is a valid configuration for a multi-chassis link aggregation (MC-LAG) setup. It specifies the use of LACP (Link Aggregation Control Protocol) with a fast rate of LACP PDUs exchange, which is appropriate for creating a resilient and high-throughput link aggregation. The 'vlan trunk allowed all' command allows all VLANs across the trunk, and 'vlan trunk native 100' sets VLAN 100 as the native VLAN for untagged traffic.

NEW QUESTION: 30

Based on best practices if an SSID is configured Tor a primary and secondary gateway cluster with cluster preemption enabled, which will decide if the APs move to the secondary gateway cluster if all of the nodes in the primary gateway cluster are down?

A. tunnel orchestrator for LAN tunnel service in HPE Aruba Networking Central

B. every AP individually

C. cluster leader in the primary gateway cluster

D. cluster leader in the secondary gateway cluster

Answer: B (LEAVE A REPLY)

In an Aruba network, if an SSID is configured for a primary and secondary gateway cluster with cluster preemption enabled, each AP individually will decide to move to the secondary gateway cluster if all of the nodes in the primary gateway cluster are down. This decentralized decision-making process enhances network resilience and ensures uninterrupted service for clients connected to the APs.

NEW QUESTION: 31

Exhibit.

:0d:b0:41:5d:b6	b8:3a:5a:84:24:30	Association Request, SN=1, FN=0, Flags=....	12.0	Association Request	-54 dBm	802.11a (OFDM)
8:3a:5a:84:24:30	20:0d:b0:41:5d:b6	Association Response, SN=1294, FN=0, Flags…	12.0	Association Response	-54 dBm	802.11a (OFDM)
	b8:3a:5a:84:24:30	Acknowledgement, Flags=.....C	12.0	Ack	-54 dBm	802.11a (OFDM)
8:3a:5a:84:24:30	20:0d:b0:41:5d:b6	Key (Message 1 of 4)	12.0	WPA KEYS	-54 dBm	802.11a (OFDM)
	b8:3a:5a:84:24:30	Acknowledgement, Flags=.....C	12.0	Ack	-54 dBm	802.11a (OFDM)
:0d:b0:41:5d:b6	b8:3a:5a:84:24:30	Key (Message 2 of 4)	24.0	WPA KEYS	-54 dBm	802.11a (OFDM)
8:3a:5a:84:24:30	20:0d:b0:41:5d:b6	Key (Message 3 of 4)	12.0	WPA KEYS	-54 dBm	802.11a (OFDM)
8:3a:5a:84:24:30	20:0d:b0:41:5d:b6	Key (Message 3 of 4)	12.0	WPA KEYS	-54 dBm	802.11a (OFDM)
	b8:3a:5a:84:24:30	Acknowledgement, Flags=.....C	12.0	Ack	-54 dBm	802.11a (OFDM)
:0d:b0:41:5d:b6	b8:3a:5a:84:24:30	Key (Message 4 of 4)	24.0	WPA KEYS	-54 dBm	802.11a (OFDM)
8:3a:5a:84:24:30	80:32:53:62:d6:df	VHT/HE NDP Announcement, Sounding Dialog T…	6.0	Other Control Frame	-53 dBm	802.11a (OFDM)
:32:53:62:d6:df	b8:3a:5a:84:24:30	Action No Ack, SN=72, FN=0, Flags=.....C	65.0	Other Management Fra…	-46 dBm	802.11ac (VHT)
8:3a:5a:84:24:30	80:32:53:62:d6:df	VHT/HE NDP Announcement, Sounding Dialog T…	6.0	Other Control Frame	-52 dBm	802.11a (OFDM)
:32:53:62:d6:df	b8:3a:5a:84:24:30	Action No Ack, SN=73, FN=0, Flags=.....C	32.5	Other Management Fra…	-46 dBm	802.11ac (VHT)
8:3a:5a:84:24:30	80:32:53:62:d6:df	VHT/HE NDP Announcement, Sounding Dialog T…	6.0	Other Control Frame	-52 dBm	802.11a (OFDM)
:32:53:62:d6:df	b8:3a:5a:84:24:30	Action No Ack, SN=74, FN=0, Flags=.....C	32.5	Other Management Fra…	-46 dBm	802.11ac (VHT)
:0d:b0:41:5d:b6	b8:3a:5a:84:24:30	DHCP Request Transaction ID 0xd3da6e2f	24.0	QoS Data	-54 dBm	802.11a (OFDM)
8:3a:5a:84:24:30	ff:ff:ff:ff:ff:ff	DHCP ACK Transaction ID 0xd3da6e2f	12.0	Data	-54 dBm	802.11a (OFDM)
:0d:b0:41:5d:b6	b8:3a:5a:84:24:30	Who has 192.168.10.1? Tell 192.168.10.158	24.0	QoS Data	-54 dBm	802.11a (OFDM)
	b8:3a:5a:84:24:30	Acknowledgement, Flags=.....C	12.0	Ack	-54 dBm	802.11a (OFDM)
:0d:b0:41:5d:b6	b8:3a:5a:84:24:30	Action, SN=2, FN=0, Flags=.p.....C, Dialo…	12.0	Action	-54 dBm	802.11a (OFDM)
8:3a:5a:84:24:30	20:0d:b0:41:5d:b6	802.11 Block Ack Req, Flags=.....C	12.0	Block Ack Request	-54 dBm	802.11a (OFDM)
:0d:b0:41:5d:b6	b8:3a:5a:84:24:30	802.11 Block Ack, Flags=.....C	12.0	Block Ack	-54 dBm	802.11a (OFDM)
8:3a:5a:84:24:30	20:0d:b0:41:5d:b6	192.168.10.1 is at 00:1c:7f:7b:d2:4d	585.0	QoS Data	-51 dBm	802.11ac (VHT)
8:3a:5a:84:24:30	20:0d:b0:41:5d:b6	192.168.10.1 is at 00:1c:7f:7b:d2:4d	585.0	QoS Data (Retry)	-51 dBm	802.11ac (VHT)

A customer is reporting mat connectivity is Tailing for some wireless client Devices. What are your conclusions from the capture? (Select two.)

A. The client does not have an ARP entry for me default gateway.

B. The network is using WPA2-PSK key management.

C. The network is using WPA3-SAE key management.

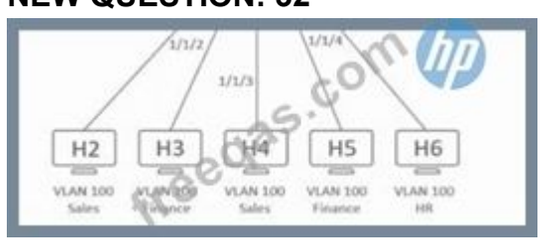
D. The client is not receiving an IP address.

E. The client does not support beamforming.

Answer: (SHOW ANSWER)

The capture shows messages related to WPA key management, indicating WPA2-PSK is being used. Also, the capture includes a DHCP request from the client but no corresponding DHCP ACK, suggesting the client is not receiving an IP address, which could explain the connectivity failure.

NEW QUESTION: 32



Source	Destination	Action
Marketing	HR	Deny
Marketing	Sales	Permit
Marketing	Finance	Deny

What is the expected behavior for ARP traffic sent from H1?

A. A2 will send the ARP traffic out of ports 1/1/1 and 1/1/3.

B. A2 will send the ARP traffic out of ports 1/1/1-1/1/4.

C. A2 will drop the ARP traffic.

D. A2 will flood the ARP traffic out of all interfaces.

Answer: (SHOW ANSWER)

In this scenario:

* All hosts are in VLAN 100

* Group-Based Policy (GBP) is applied

* H1 belongs to the Marketing role

* Policy table for Marketing:

Source

Destination

Action

Marketing

HR

Deny

Marketing

Sales

Permit

Marketing

Finance

Deny

Role Mapping:

* Sales: H2, H4

* Finance: H3, H5

* HR: H6

Key Aruba GBP Behavior for ARP

Aruba AOS-CX GBP enforces policy at L3 and L2, and ARP is not treated as unconditional broadcast when GBP roles restrict communication.

Aruba documentation states:

"ARP requests are only forwarded to ports associated with permitted roles.

ARP behavior follows the GBP access-policy rules."

Since Marketing is only permitted to communicate with Sales, ARP from H1 must only be forwarded toward:

H2 (Sales)

H4 (Sales)

Interfaces:

* H2 # port 1/1/1

* H4 # port 1/1/3

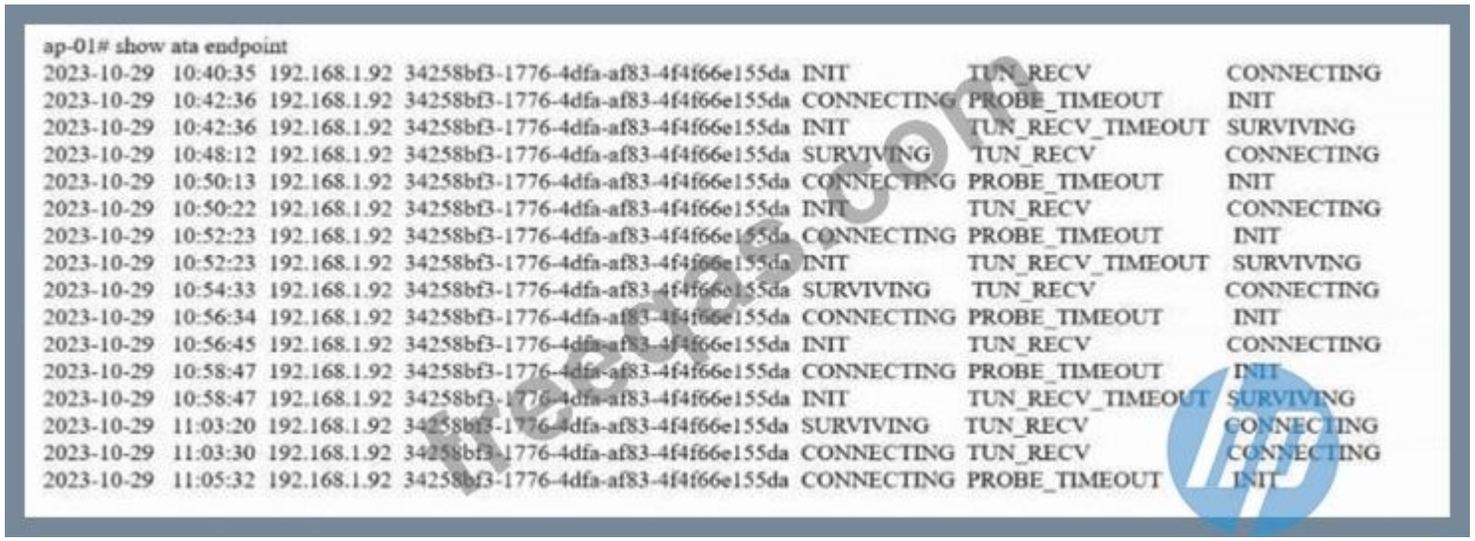
Therefore, the ARP request is NOT flooded to Finance (H3/H5) or HR (H6), where communication is denied.
Why Other Options Are Incorrect
Option
Why Wrong
B
Would ignore GBP enforcement; too wide of a flood
C
Not dropped - allowed paths exist to Sales
D
ARP is not broadcasted when GBP denies connectivity

NEW QUESTION: 33
A customer is planning to add IoT devices that connect wirelessly to the existing 802.1X SSID. The customer will use HPE Aruba Networking ClearPass to authenticate the IoT devices by MAC address but other devices will still need to authenticate by only 802.1X.
Refer to the exhibit.

The customer provided the current configuration and reported their non-IoT 802.1X devices are no longer able to connect. Which configuration change can be made to fix the issue?
A. Remove mac-authentication from the WLAN configuration
B. Modify max-authentication failures to 0
C. Add 12-auth-failthrough to the WLAN configuration
D. Modify opmode wpa3-aes-gcm-256 to opmode wpa2-aes
Answer: C (LEAVE A REPLY)
In ArubaOS WLAN SSID profiles, the command mac-authentication enables MAC-based authentication on the SSID. When MAC authentication is enabled and l2-auth-failthrough is not configured, the AP treats MAC authentication as the decisive Layer-2 method: if the MAC check does not return an accept, the client is not allowed to proceed to another Layer-2 method (such as 802.1X). Aruba documentation states that l2-auth- failthrough allows a client to fall through to the next Layer-2 authentication method when the first method fails or is not matched.
Therefore, with IoT devices using MAC authentication and non-IoT devices using 802.1X on the same SSID, you must enable l2-auth-failthrough so that clients that do not match MAC authentication are allowed to attempt 802.1X.
* mac-authentication: enables MAC-auth on the SSID.
* l2-auth-failthrough: permits clients to continue to 802.1X when MAC-auth is not accepted.
* Changing opmode (WPA2 vs WPA3) or max-authentication-failures does not resolve the Layer-2 method selection behavior.
* Removing mac-authentication would prevent the IoT MAC-auth use case.

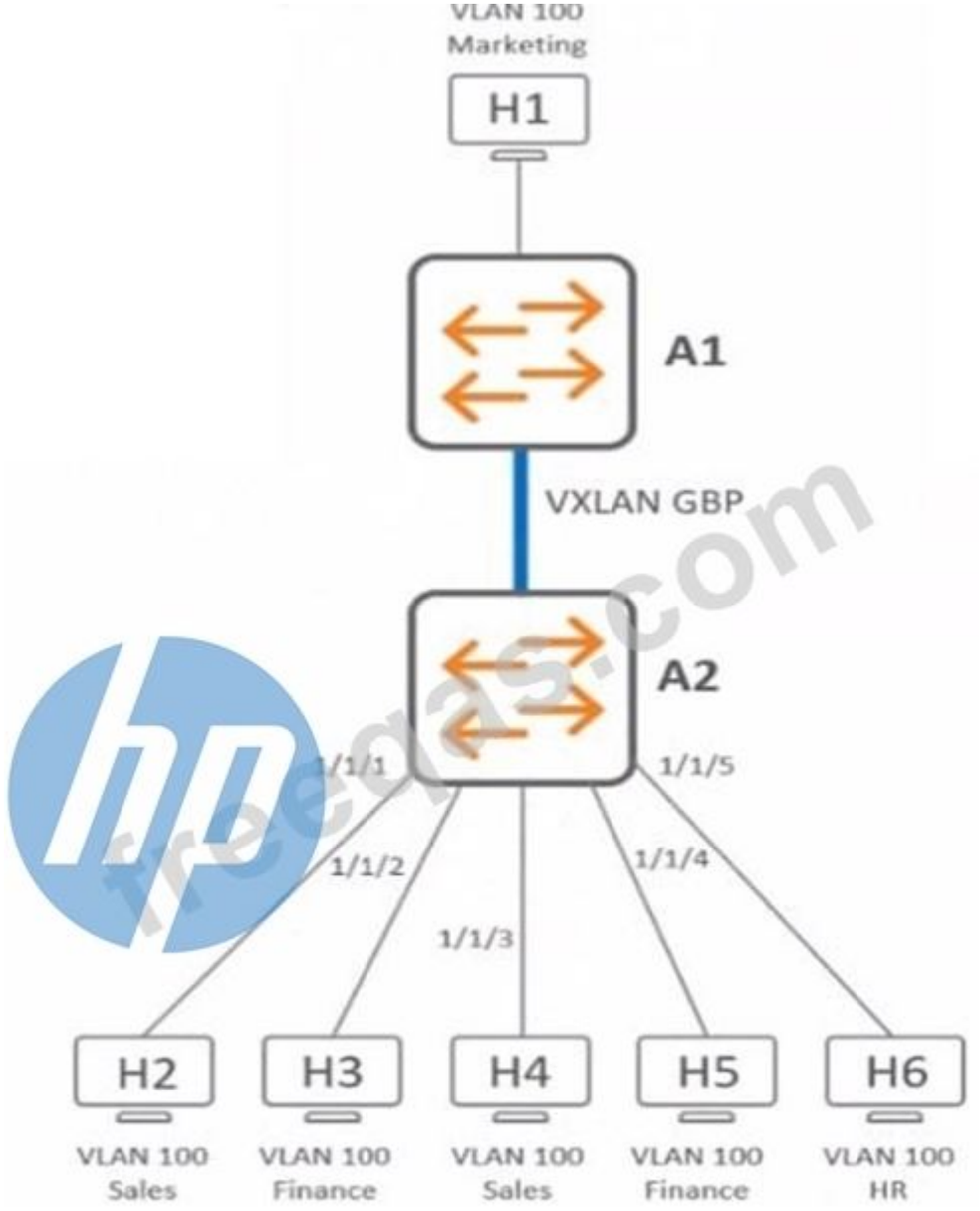
References (HPE Aruba Networking official guides):
* ArubaOS WLAN SSID Profile-Layer-2 Authentication Methods: mac-authentication and l2-auth- failthrough behavior and sequencing.
* Aruba ClearPass and ArubaOS Integration-MAC Authentication with 802.1X coexistence on a single SSID using fail-through.

NEW QUESTION: 34
Refer to the exhibit.



Given the log output, which statement is true?
A. AP-01's tunnel to 192.168.1.92 is in a survived state.
B. The gateway with IP address 192.168.1.92 is offline.
C. AP-01 cannot communicate with the HPE Aruba Networking Central tunnel orchestrator.
D. The gateway tunnel to the AP has a path MTU issue.
Answer: B (LEAVE A REPLY)
* The show ata endpoint output lists the AP's AP Tunnel Agent (ATA) state transitions with a given gateway.
* Key state/result fields:
* CONNECTING # PROBE_TIMEOUT # INIT: the AP tries to bring up the IPSec tunnel, health probes to the gateway time out, then the state resets to INIT and retries.
* TUN_RECV_TIMEOUT: the AP stops receiving tunnel keepalives/packets from the gateway within the expected interval.
* SURVIVING indicates the AP is maintaining service with an already-up tunnel while control connectivity is impaired; it is not the state shown at the end here.
In the log, AP-01 repeatedly cycles through CONNECTING # PROBE_TIMEOUT # INIT, with intermittent TUN_RECV_TIMEOUT. This pattern is the documented symptom of the gateway being unreachable or down (no response to probes/keepalives), rather than a Central/orchestrator outage or PMTU problem.
Therefore, the correct conclusion is that the gateway at 192.168.1.92 is offline or not reachable.
* A is incorrect: the final/recurring state is not SURVIVING.
* C is incorrect: a Central/orchestrator issue would show SURVIVING (existing tunnel continues) rather than repeated probe timeouts to the gateway.
* D is incorrect: PMTU issues do not generate recurring PROBE_TIMEOUT/TUN_RECV_TIMEOUT cycles; they appear as ESP/IKE negotiation problems, not persistent probe loss.

NEW QUESTION: 35
Exhibit.



Source	Destination	Action
Marketing	HR	Deny
Marketing	Sales	Permit
Marketing	Finance	Deny

What is me expected behavior for ARP traffic sent from H1?

A. A2 will drop the ARP traffic.

B. A2 will send the ARP traffic out of ports 1/1/1-1/1/4.

C. A2 will flood the ARP traffic out of all interfaces.

D. A2 will send the ARP traffic out of ports 1/1/1 and 1/1/3.

Answer: C (LEAVE A REPLY)

In a VXLAN environment, unknown unicast traffic, such as ARP requests from H1, which does not have a specific destination MAC address learned by the switch A2, will be flooded out of all interfaces. This flooding behavior is necessary because A2 needs to ensure that the ARP request reaches its intended destination, which might be on any of the interfaces. It's a part of the standard behavior of switches to handle ARP traffic when the destination hardware address is unknown.

NEW QUESTION: 36

Exhibit.

Which would explain this issue?

A. HTTPS wildcard certificates are not supported

B. HTTPS certificate is not required in ClearPass Guest.

C. captiveportal-login aruba-training com needs to be entered m the Address field for the ClearPass Guest

D. ".aruba-training com needs to be entered in the Address field for the ClearPass Guest

Answer: D (LEAVE A REPLY)

The correct address for the ClearPass Guest should match the FQDN of the HTTPS certificate installed on the device, which is often the FQDN of the vendor's product. This ensures secureand proper redirection to the captive portal during the authentication process. The FQDN should be entered in the Address field for ClearPass Guest configuration.

NEW QUESTION: 37

An OSPF router has learned a path to an external network by both an E1 and an E2 advertisement. Both routes have the same path cost. Which path will the router prefer?

A. The router will use both paths equally utilizing ECMP.

B. Both routes will be suppressed until the path conflict has been resolved.

C. The router will prefer the E1 path.

D. The router will prefer the E2 path.

Answer: C (LEAVE A REPLY)

In HPE Aruba Networking (AOS-CX and AOS-Switch) OSPF implementation, the routing behavior for external routes (Type 5 LSAs) distinguishes between two types of external advertisements:

* E1 (Type-1 external) - The total path cost is calculated as the sum of the internal cost to reach the ASBR (Autonomous System Boundary Router) plus the external cost as advertised in the LSA.

* E2 (Type-2 external) - The external cost is considered independent of the internal OSPF path cost to reach the ASBR. Thus, the metric used is only the external cost from the LSA.

When both an E1 and an E2 route exist to the same external destination, OSPF gives preference to the E1 route, regardless of metric values, because the E1 route represents a more accurate total cost to the destination (including internal OSPF cost).
Extract (as per HPE Aruba OSPF Technical Overview and AOS-CX Routing Guide):
"When both Type-1 (E1) and Type-2 (E2) external LSAs for the same destination are present, the router always prefers the Type-1 route. Type-1 routes include both internal and external costs in the total metric, while Type-2 routes use only the external cost. The E1 path is therefore considered more precise and is selected as the preferred route." This is consistent across Aruba's OSPF implementation and follows standard OSPF behavior as defined by the protocol (RFC 2328).
Therefore, when both E1 and E2 routes are available and have the same overall cost, the router will always prefer the E1 path.
References:* HPE Aruba Networking AOS-CX Routing Configuration Guide - OSPF External Route Preference (Section: OSPF External LSAs).* HPE Aruba Certified Switching Professional (ACSP) Study Guide - OSPF Route Selection and External Type Behavior.* HPE ArubaOS-Switch Management and Configuration Guide - OSPF External Route Types (E1 vs E2).

NEW QUESTION: 38
Which statements accurately describe OSPF Graceful Restart (when the restarting router is able to Keep its forwarding tables across the restart)? (Select two.)
A. The GR helper role is supported on AOX-CX 6100 switches.
B. VSF Failover and Graceful-Restart require a VSF secondary member in the VSF stack
C. Bidirectional Forwarding Detection for OSPF and GR are mutually exclusive features.
D. OSPF Routers listen for Grace-LSAs on each network segment where there is an OSFP adjacency.
E. You must ensure your VSF stack has a secondary member when acting as a GR helper
Answer: (SHOW ANSWER)
Graceful Restart (GR) allows a router to continue forwarding packets while it restarts its OSPF process. The GR helper role on AOS-CX switches supports routers during this process. OSPFrouters listen for Grace-LSAs to identify neighbors undergoing a graceful restart, maintaining adjacencies with those routers to allow uninterrupted forwarding.

NEW QUESTION: 39
A customer would like to allow their IT Helpdesk to configure IoT devices to connect to a single SSID using a unique PSK that other devices cannot use.
Which solution would you recommend?
A. MPSK AES with HPE Aruba Networking ClearPass
B. MPSK AES with HPE Aruba Networking Central Cloud Authentication
C. MPSK Local
D. MPSK AES with MAC Auth
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract of HPE Aruba Networking Switching:
The requirement in this question is to allow IT staff to provision unique pre-shared keys (PSKs) for each IoT device on a single SSID, ensuring that one device's PSK cannot be used by another. This is the definition of Multi-Pre-Shared Key (MPSK) functionality.
HPE Aruba Networking supports three main MPSK deployment methods:
* MPSK Local - Keys are defined locally on the AP or gateway; no external integration.
* MPSK with ClearPass - Keys are managed and validated via ClearPass Policy Manager.
* MPSK with Cloud Authentication - Keys are generated, stored, and managed natively through Aruba Central Cloud Authentication.
In this scenario, the IT Helpdesk wants a simplified, cloud-based method to generate and manage per-device unique PSKs without needing a ClearPass deployment. This aligns directly with MPSK AES with HPE Aruba Networking Central Cloud Authentication.

Exact Extract from HPE Aruba Networking Switching and Central Documentation:
"MPSK with Cloud Authentication allows administrators to configure a single SSID where each device is assigned a unique PSK. The PSKs are securely stored and validated using Aruba Central's cloud-based authentication service."
"Each PSK is tied to a specific client identity. If another device attempts to connect using the same PSK, the authentication will fail."
"This method simplifies onboarding of IoT and headless devices while maintaining security equivalent to 802.1X."
Thus, the correct recommendation is MPSK AES with Aruba Central Cloud Authentication, which fully supports per-device key uniqueness, centralized management, and cloud-based authentication-ideal for IoT device onboarding.
Why the Other Options Are Incorrect:
* A. MPSK AES with ClearPass:Valid and secure, but requires an on-prem ClearPass Policy Manager deployment. The question specifies a simpler method for IT Helpdesk to manage keys directly, which Cloud Authentication provides natively.
"ClearPass MPSK requires policy manager integration; Aruba Central Cloud Authentication provides a simpler cloud-native alternative."
* C. MPSK Local:Suitable for small static environments, but not scalable and requires manual key creation on the AP or gateway. Does not allow IT staff to easily generate new keys per device via Central.
"MPSK Local does not support centralized lifecycle management or key revocation."
* D. MPSK AES with MAC Auth:MPSK already handles per-device authentication via unique keys; MAC authentication is unnecessary and less secure.
"MAC authentication is an alternate method for non-802.1X devices but is not required with MPSK." References of HPE Aruba Networking Switching Documents or Study Guide:
* Aruba Central Cloud Authentication and MPSK Deployment Guide - "Configuring MPSK AES with Cloud Authentication."
* Aruba Wi-Fi 6 and IoT Integration Best Practices Guide - "Securing IoT with Cloud-Managed MPSK."
* ArubaOS 10 WLAN Configuration Guide - "MPSK Modes (Local, ClearPass, Cloud Authentication) and Use Cases."

NEW QUESTION: 40
A customer's infrastructure is set up to use both primary and secondary gateway clusters on the SSID profile cased on best practices. Why do they have an equal split of their 120 APs across the primary and secondary gateway clusters?
A. The primary gateway cluster is a heterogeneous cluster with six nodes.
B. The primary and secondary gateway clusters are up. and the cluster preemption is enabled
C. The secondary gateway cluster is a homogeneous cluster with six nodes.
D. The primary and secondary gateway clusters are up. but the cluster preemption Is not enabled
Answer: D (LEAVE A REPLY)
When cluster preemption is not enabled, access points (APs) will not automatically fail back to the primary gateway cluster once it is up again after having failed over to the secondary. This would result in an equal split of APs across primary and secondary clusters if both clusters are operational. Without preemption, there's no automatic rebalancing of APs back to the primary cluster, leading to the current distribution.

NEW QUESTION: 41
A customer has interfering devices that are seen over the air. They contact you and ask you to configure RAPIDS to help identify interfering and rogue APs.
HPE Aruba Networking Central identifies a rogue AP and displays the connected switch port.
How can HPE Aruba Networking Central identify which switch port the AP is connected to?
A. Device profiling on the switch
B. From the switch MAC address table
C. From the switch LLDP neighbors table

D. From the AP MAC address table

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (Verified Extract from HPE Aruba Networking Central and ClearPass Documentation) RAPIDS (Rogue AP Detection System) in Aruba Central or AirWave works by correlating information between wireless and wired infrastructure to detect rogue devices and identify their wired connectivity location.

When Aruba Central detects a rogue AP or interfering device, it uses wired-side discovery mechanisms such as LLDP (Link Layer Discovery Protocol) to trace the device's physical connection.

If the managed switch supports LLDP, it advertises and records neighbor information, including device type, MAC address, and connected port. Aruba Central queries this LLDP neighbor table from managed switches to determine the exact switch port where the rogue AP is physically connected.

Aruba Central and RAPIDS Documentation Extract:

"Aruba Central correlates rogue or interfering AP MAC addresses with wired-side discovery data. Using LLDP neighbor table information from managed switches, Central identifies the physical switch port where the rogue device is connected." Other options such as the MAC address table can show where a MAC is learned, but LLDP provides the direct, authenticated neighbor relationship that allows Aruba Central to accurately identify the rogue AP connection point and display it in the dashboard.

Option Analysis:

* A. Incorrect - Device profiling identifies endpoint types, not wired connection ports for rogue AP detection.
* B. Incorrect - MAC tables alone don't provide direct port-device mapping context for rogue detection in Central.
* C. # Correct - Aruba Central uses LLDP neighbor data from managed switches to map rogue or interfering APs to specific switch ports.
* D. Incorrect - AP MAC address tables exist in controllers or APs, not in Central's rogue-tracking mechanism.

Final Verified answer: C

Reference Sources (HPE Aruba Official Materials):

* Aruba Central Administration and RAPIDS Configuration Guide
* ArubaOS-Switch and CX Network Management Fundamentals - LLDP Discovery Integration
* Aruba Certified Network Security Professional (ACNSP) Study Guide - Rogue AP Detection and Wired Correlation

NEW QUESTION: 42

A BGP routing table contains multiple routes to the same destination prefix.

Referring to the table below, which route would be marked with a ">" symbol?

Route	Distance	Metric	Origin Code	Local Preference
A		200	i	0
B		0	?	100
C		20	?	0
D	200	0	i	100
E	20	0	i	100

A. A

B. B

C. C

D. D

E. E

Answer: E (LEAVE A REPLY)

The Aruba AOS-CX BGP Best Path Selection Process determines which route becomes the active (>) route in the BGP routing table.

This process is consistent with RFC 4271 but detailed in HPE's Aruba AOS-CX Routing Guide and ACSP Study Guide - BGP and Dynamic Routing.
Extract 1 - BGP Path Selection Hierarchy (Aruba AOS-CX Routing Guide)
"When multiple BGP routes exist to the same destination, the router uses the following decision sequence to select the best path:
* Highest LOCAL_PREFERENCE
* Lowest AS_PATH length
* Lowest ORIGIN type (IGP 'i' preferred over EGP 'e', preferred over Incomplete '?')
* Lowest MULTI_EXIT_DISC (MED) if received from the same AS
* Lowest IGP cost to the next hop (closest exit)
* Lowest BGP router ID as tie-breaker."
Extract 2 - Aruba Certified Switching Professional (ACSP) Study Guide - BGP Path Decision
"Local Preference is the first and most significant criterion within a single AS.
A higher Local Preference value indicates a preferred exit.
If multiple routes have equal Local Preference, the router compares their Origin Codes.
An Origin Code of 'i' (IGP) is preferred over '?' (Incomplete).
If still tied, the route with the lowest IGP cost to the next-hop is chosen as best." Step-by-Step Application to the Table Step 1 - Local Preference
* Routes B, D, and E have Local Preference = 100
* Routes A and C have Local Preference = 0
# Routes A and C are eliminated.
Remaining candidates: B, D, E
Step 2 - Origin Code
* D and E: Origin Code = i (IGP) # Preferred
* B: Origin Code = ? (Incomplete) # Less preferred
# Eliminate B
Remaining candidates: D, E
Step 3 - MED / Metric
Both D and E have Metric = 0 # Still tied
Step 4 - IGP Cost / Administrative Distance
* D: Distance = 200
* E: Distance = 20
According to ArubaOS-CX:
"When all BGP attributes are equal, the route with the lowest internal cost (shortest IGP distance) to the next-hop is selected."
E wins because it has a lower distance (20 < 200)
Extract 3 - ArubaOS-CX Routing Reference
"The route that wins the selection process is marked with a '>' symbol in the routing table.
This route is installed in the forwarding table and used for traffic forwarding." Final Explanation
* Route E has:
* Highest Local Preference (100)
* Best Origin (IGP 'i')
* Lowest IGP distance (20)
Hence, Route E is selected as the best path, and the ">" symbol is placed beside it in the BGP routing table.
Final Verified answer: E

Official Aruba Documentation References:
* Aruba AOS-CX Routing Guide - Section: BGP Best Path Selection Criteria
* Aruba Certified Switching Professional (ACSP) Study Guide - Module: BGP and Path Selection Logic
* Aruba AOS-CX Configuration and Management Guide - Command: show ip bgp summary / route selection

NEW QUESTION: 43
Which command would allow you to verify receipt of a CoA (Change of Authorization) message on an AOS-10 Gateway?
A. packet-capture interprocess udp 3799
B. packet-capture controlpath udp 3799
C. diag utilities tcpdump host-port 3576
D. tcpdump host-port 3576
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation (Verified Extract from HPE Aruba Networking AOS-10 Gateway Documentation) The Change of Authorization (CoA) message is a RADIUS-based control packet typically sent by ClearPass Policy Manager or another RADIUS server to modify client authorization dynamically after authentication.
In ArubaOS 10, CoA and Disconnect-Request (DM) messages use UDP port 3799 and are received on the control path of the gateway, not the datapath.
HPE Aruba AOS-10 documentation specifies:
"Use the command packet-capture controlpath udp 3799 on the gateway to verify that CoA packets are being received and processed on the control plane."
"The controlpath capture displays inbound CoA or DM messages received from RADIUS servers such as ClearPass." Command breakdown:
packet-capture controlpath udp 3799
* controlpath # Captures control-plane traffic (used for management protocols like RADIUS, CoA, CAPWAP, etc.)
* udp 3799 # Filters only CoA/DM packets
Why Others Are Incorrect:
* A. interprocess captures internal gateway processes, not RADIUS packets.
* C. diag utilities tcpdump is used in AOS 8.x, not AOS 10.
* D. tcpdump host-port 3576 uses the wrong port; CoA uses UDP 3799, not 3576 (which is for standard RADIUS authentication).
# Final Verified answer: B. packet-capture controlpath udp 3799
# Reference Sources (HPE Aruba Official Materials):
* Aruba AOS-10 Gateway Troubleshooting Guide - Control Path Packet Capture Commands
* Aruba ClearPass and AOS Integration Guide - RADIUS CoA Port (UDP 3799)
* Aruba Certified Mobility Professional (ACMP) Study Guide - CoA and Disconnect Message Verification

NEW QUESTION: 44
The ACME company has an AOS-CX 6200 switch stack with an uplink oversubscription ratio of 9.6:1. They are considering adding two more nodes to the stack without adding any additional uplinks due to cabling constraints One oftheir architects has expressed concerns that their critical UDP traffic from both wired and bridged AP clients will encounter packet drops.They have already applied the following configuration:

```
vsf1(config)# qos threshold-profile acmethreshold
vsf1(config-threshold)# queue 0 action wred-resp yellow min-threshold 40 percent max-threshold 80 percent
vsf1(config)# int lag 1
vsf1(config-if)# description uplink-to-collapsed-core
vsf1(config-if)# apply qos threshold-profile acmethreshold
```

DSCP	code_point	local_priority	cos	color	name
000000	0	1		green	CS0
000001	1	1		green	
000010	2	1		green	
000011	3	1		green	
000100	4	1		green	
000101	5	1		green	
000110	6	1		green	
000111	7	1		green	
001000	8	0		green	CS1
001001	9	0		green	
001010	10	0		green	AF11
001011	11	0		green	
001100	12	0		yellow	AF12
001101	13	0		green	
001110	14	0		yellow	AF13
001111	15	0		green	
010000	16	2		green	CS2
010001	17	2		green	
010010	18	2		green	AF21
010011	19	2		green	
010100	20	2		yellow	AF22
010101	21	2		green	
010110	22	2		yellow	AF23
010111	23	2		green	
011000	24	3		green	CS3
011001	25	3		green	
011010	26	3		green	AF31
011011	27	3		green	
011100	28	3		yellow	AF32
011101	29	3		green	
011110	30	3		yellow	AF33
[illegible]	31	4		green	
100010	34	4		green	AF41
100011	35	4		green	
100100	36	4		yellow	AF42
100101	37	4		green	
100110	38	4		yellow	AF43
100111	39	4		green	
101000	40	5		green	CS5
101001	41	5		green	
101010	42	5		green	
101011	43	5		green	
101100	44	5		green	
101101	45	5		green	
101110	46	5		green	EF
101111	47	5		green	
110000	48	6		green	CS6
110001	49	6		green	
110010	50	6		green	
110011	51	6		green	
110100	52	6		green	
110101	53	6		green	
110110	54	6		green	
110111	55	6		green	
111000	56	7		green	CS7
111001	57	7		green	
111010	58	7		green	
111011	59	7		green	
111100	60	7		green	
111101	61	7		green	
111110	62	7		green	

Which strategy will complement this solution to achieve their objective?

A. edge mark lower priority TCP traffic with AF12

B. edge mark critical UDP Traffic with CSS

C. edge mark lower priority TCP traffic with AF11

D. edge mark critical UDP traffic with AF42

Answer: D (LEAVE A REPLY)

Given that the ACME company's concern is about UDP traffic potentially encountering packet drops due to uplink oversubscription, they need a strategy that prioritizes critical UDP traffic to minimize loss.

Option D,edge mark critical UDP traffic with AF42, is the correct answer. Assured Forwarding (AF) classes provide a way to assign different levels of delivery assurance for IP packets. AF42 is typically used for traffic that requires low latency and low loss, such as voice and video, which often use UDP. Marking critical UDP traffic with AF42 will help ensure that this traffic is treated with higher priority over the network.
Option A (edge mark lower priority TCP traffic with AF12) and Option C (edge mark lower priority TCP traffic with AF11) suggest marking lower priority TCP traffic, which does not directly address the concern for critical UDP traffic.
Option B (edge mark critical UDP Traffic with CS5) suggests using Class Selector 5 for critical UDP traffic, which is also a valid approach but does not match the existing configuration that is focused on Assured Forwarding (AF) classes.

NEW QUESTION: 45
You configured a tunneled SSID with captive portal and a ClearPass Guest Self Registration workflow when testing and launching the self-registration workflow, after successful registration, the login action shows the following error:

What is the best solution to resolve this error?
A. You need to include the root and intermediate certificates in the captive portal certificate for your access points
B. You need to De connected to the guest SSiD while testing.
C. You need to change the Login Address in ClearPass to securelogin arubanetworKs.com
D. You need to include the root and intermediate certificates in the captive portal certificate for your gateway
Answer: (SHOW ANSWER)
Including the root and intermediate certificates in the captive portal certificate for the gateway will resolve the error seen during the login action after successful registration. This is necessary to ensure the SSL/TLS handshake can be completed successfully, as the client browser needs to validate the entire certificate chain.

NEW QUESTION: 46
A customer is planning to add IoT devices that connect wirelessly to the existing 802.1X SSID. The customer will use ClearPass to authenticate the IoT devices by MAC address but other devices will still need to authenticate by only 802 1X Exhibit.

The customer provided the current configuration and reported their non-IoT 802. IX devices are no longer able to connect. Which configuration change can be made to fix the issue?

A. Modify opmode wpa3-aes-gcm-256 to opmode wpa2-aes

B. Add i2-autn-fairtnrougn to the WLAN configuration

C. Remove mac-authentication from the WLAN configuration

D. Modify max-authentication failures to 0.

Answer: C (LEAVE A REPLY)

The existing configuration for the WLAN ssid-profile has enabled MAC authentication which, while suitable for IoT devices that may not support 802.1X, can interfere with the normal 802.1X authentication process for other devices. By removing themac-authenticationdirective from the WLAN configuration, the non-IoT 802.1X devices should be able to connect without issues as the authentication process will not be disrupted by MAC authentication checks. This adjustment ensures that the WLAN ssid-profile is correctly aligned with the authentication requirements for both IoT and non-IoT devices within the network environment, conforming to the best practices for mixed-device WLAN configurations.

NEW QUESTION: 47

Which data transmission method provides the most efficient use of airtime for VoIP traffic?

A. FDMA

B. OFDM

C. MU-MIMO

D. TWT

Answer: C (LEAVE A REPLY)

MU-MIMO (Multi-User, Multiple Input, Multiple Output) provides the most efficient use of airtime for VoIP traffic among the options listed. MU-MIMO allows multiple users to receive multiple data streams simultaneously, improving the overall efficiency of the network, especially in dense environments where VoIP applications need consistent and reliable connectivity.

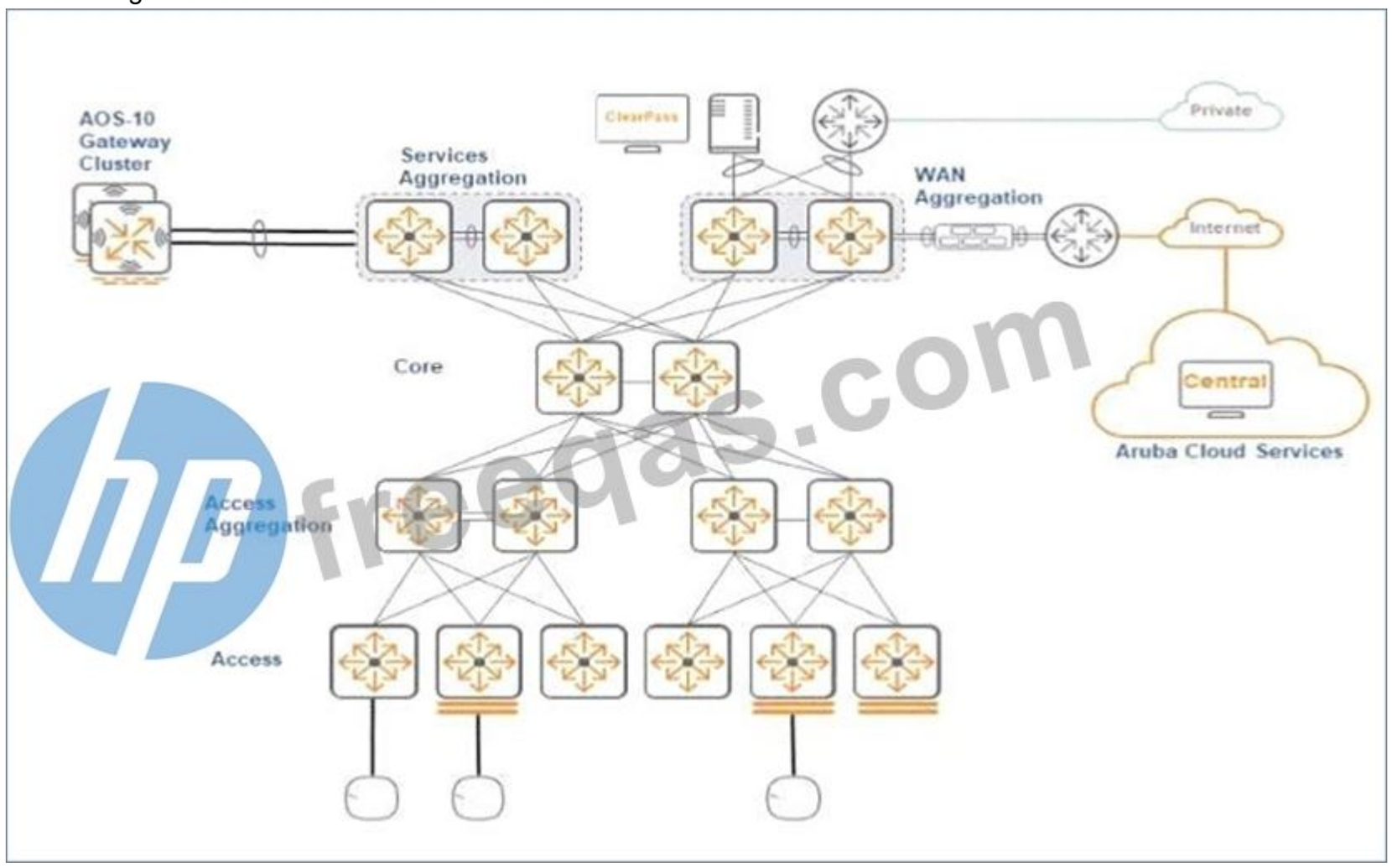
NEW QUESTION: 48

What directly affects the MCS used by wireless stations? (Select two.)

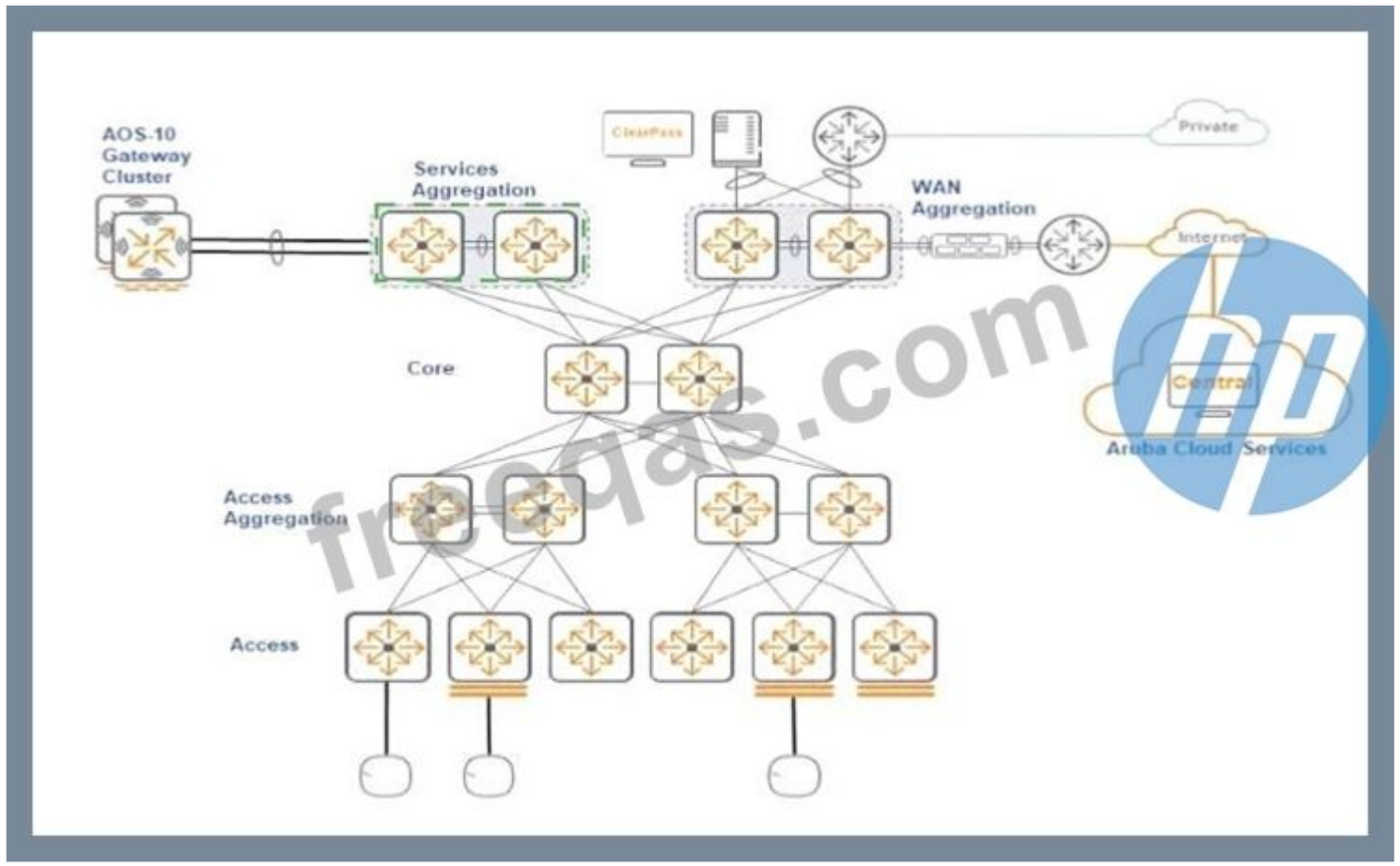
A. SNR

B. retry rate
C. channel utilization
D. number of connected clients
E. frequency band
Answer: A,E (LEAVE A REPLY)
The Modulation and Coding Scheme (MCS) used by wireless stations is directly affected by the signal-to-noise ratio (SNR) and the frequency band. Higher SNR can lead to higher MCS values, which means better data rates. The frequency band can affect MCS due to different channel characteristics, such as the presence of interference and propagation properties, which are factors in determining data rates.

NEW QUESTION: 49
An administrator is creating a fabric withNetConductor in HPE Aruba Networking Central Considering an EVPN VXLAN fabric, click on the most appropriate layer to be configured as a Rome-Reflector Persona.



Answer:



Explanation:
In the context of an EVPN VXLAN fabric, the Route-Reflector Persona is most appropriately configured at theServices Aggregationlayer. This layer is responsible for interconnecting different network services and typically includes more robust, higher-capacity devices capable of handling the route-reflection functions for EVPN VXLAN.
In an Aruba Networks fabric, route reflectors are used to optimize the distribution of BGP routes. The Services Aggregation layer, which is centrally located in the network topology, is best suited for this role due to its high availability and ability to efficiently manage routes between the core and access layers.
Therefore, if you were to click on the image provided, you would select the Services Aggregation layer to configure the Route-Reflector Persona.

NEW QUESTION: 50
A customer would like to allow their IT Helpdesk to configure IoT devices to connect lo a single SSID using a unique PSK that other devices cannot use. Which solution would you recommend?
A. MPSK AES with MAC Auth
B. MPSK Local
C. MPSK AES with Cloud Auth
D. MPSK AES with ClearPass
Answer: D (LEAVE A REPLY)
Multi-Pre-Shared Key (MPSK) with ClearPass is the recommended solution for a scenario where the IT Helpdesk needs to configure IoT devices to connect to a single SSID using unique PSKs. MPSK allows for the use of different PSKs on the same SSID, and ClearPass enables the management of these unique keys efficiently.

NEW QUESTION: 51
You want to configure an MTU of 9198 for a routedlag interface on a CX 6300 switch.Which configuration achieves this?

A.
```
interface lag 11 multi-chassis
    no shutdown
    ip mtu 9198
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
```

B.
```
interface lag 11
    no shutdown
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

C.
```
interface lag 11 multi-chassis
    lacp mode act
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
```

D.
```
interface lag 11
    no shutdown
    ip mtu 9198
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

Answer: A (LEAVE A REPLY)

In the context of ArubaOS-CX, particularly with the 6300 series switches, setting the MTU on a routed Link Aggregation Group (LAG) interface requires theinterface lag idcommand in the configuration, specifying the LAG interface you're configuring. Theip mtucommand is then used to set the desired MTU size for that LAG.

Option A correctly shows this configuration process, where the MTU is set to 9198 for the LAG interface, in line with the requirements for routing larger frames, which could be necessary for certain applications or data flows that require jumbo frames.

The information related to the configuration of Aruba switches is consistent with the principles and guidelines found in the technical documentation for the ArubaOS-CX 6300 series switches, which emphasizes the importance of correct MTU settings for network performance and stability.

NEW QUESTION: 52

An OSPF router has learned a pain 10 an external network by Doth an E1 and an E2 advertisement Both routes have the same path cost Which path will the router prefer?

A. The router will prefer the E1 path.

B. The router will use Doth paths equally utilizing ECMP.

C. The router will prefer the E2 path.

D. Both routes will be suppressed until the path conflict has been resolved.

Answer: A (LEAVE A REPLY)

In OSPF, when a router learns about an external network through both E1 and E2 advertisements, and if both have the same path cost, the router will prefer the E1 path. This is because E1 routes consider both the external cost to reach the external network and the internal cost to reach the ASBR, providing a more comprehensive metric. E2 routes only consider the external cost and ignore the internal cost to the ASBR, which could potentially lead to suboptimal routing. Therefore, the router will choose the E1 path due to its more accurate representation of the total path cost.

NEW QUESTION: 53
Your customer recently decided to build a new wireless network based on AOS-10. The following legacy settings still exist:
* The DHCP server still sends option 60 "ArubaInstantAP" and option 43 including the IP address of the AirWave server in the ZTP VLAN.
* The DNS server has an entry for "aruba-airwave" pointing to the AirWave server.
The customer purchased new AP-655 access points and HPE Aruba Networking Central subscriptions.
Each AP is assigned to the "ACX-Group" in the Device Pre-provisioning section of Central, and the external firewall allows HTTPS traffic between APs and the Internet.
What will happen when the new factory default APs are connected to the customer's network for the first time?
A. The new APs will contact the IP address of AirWave learned from the DNS entry "aruba-airwave"
B. The new APs will contact the cloud and get the "ACX-Group" configuration in HPE Aruba Networking Central
C. The new APs will contact the IP address of AirWave from DHCP option 43
D. The new APs will contact the cloud and will be pointed to the IP address of AirWave
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Exhibit.

```
AP#show network IoT
Name :IoT
ESSID :IoT
Status :Enabled
Mode :wpa-psk-tkip,wpa2-psk-aes
Band :2.4
Type :employee
Zone :
Termination :Disabled
Passphrase :7e2fdbe07d533847ee5d2fdf7bfdb3d08ef1ac4efc644ea2
Passphrase Size :8
WEP Key :
WEP Key Index :1
Coding :UTF-8
dot11r :Enabled
dot11k :Disabled
dot11v :Enabled
MPSK :Disabled
MPSK-local :Disabled
High Throughput :Enabled
Very High Throughput :Enabled
High Efficiency :Enabled
HE TXBF :Enabled
HE MU-OFDMA :Enabled
HE MU-MIMO :Enabled
HE UL MU-MIMO :Disabled
HE Guard Interval :800ns,1600ns,3200ns
A-beacon-rate :Default
G-beacon-rate :Default
Enable Agile Multiband (MBO) :Disabled
Advertise Cellular Data Capability attribute of MBO :Disabled
Fine Timing Measurement (802.11mc) Responder Mode :Disabled
Dot11k Profile :default
```


Which statement is true?
A. The SSID supports RC4 encryption.
B. The SSID supports 802.11nac clients.
C. The SSID supports implicit beamforming.
D. The SSID supports sending neighbor reports.
Answer: (SHOW ANSWER)

The SSID supports 802.11ac clients, which is indicated by the "High Throughput" and "Very High Throughput" options being enabled. These are terms associated with the 802.11ac wireless standard, indicating that the SSID can serve clients that support this technology.

NEW QUESTION: 55
A network administrator wants to configure an 802 1X supplicant for a wireless network that includes the following:
1. AES encryption
2. EAP-MSCHAPv2-based user and machine authentication
3. validation of server certificate in Microsoft Windows 10
The network administrator creates a WLAN profile and selects the change connection settings option Then the network administrator changes the security type to Microsoft Protected EAP (PEAP) and enables user and machine authentication under Additional Settings.
What must the network administrator do next to accomplish the task?
A. Enable user authentication
B. Change the security type to Microsoft: Smart Card or other certificate.
C. Change default RC4 encryption for AES
D. Enable server certificate validation
Answer: (SHOW ANSWER)
When configuring an 802.1X supplicant for wireless network access with Microsoft Windows 10, enabling server certificate validation is a critical step to ensure the security of the authentication process. Server certificate validation helps prevent man-in-the-middle attacks by ensuring the RADIUS server presenting the certificate is the correct server that the client expects to communicate with.

NEW QUESTION: 56
A customer has deployed anAOS 10 mobilitygateway cluster consisting of three controllers at a single site The WLAN is configured to tunnel wireless device traffic to the AOS 10 mobilitycluster.The clients areauthorized to use WPA2-Personal.An end-userhas opened a ticket with the helpdesk stating they cannot connect their client device to the network.There are other devices currently associated with the SSID with no issues.

```
Nov 15 00:47:48.923  station-up *                 c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  -    wpa2 psk aes
Nov 15 00:47:48.923  wpa2-key1    <-             c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  117
Nov 15 00:47:48.939  wpa2-key2    ->             c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  123  mic failure
Nov 15 00:47:49.700  rad-acct-start   ->         c8:34:8e:20:50:4b  cc:88:c7:43:23:b1/__gw_172.20.10.102  -  -
Nov 15 00:47:50.421  wpa2-key1    <-             c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  117
Nov 15 00:47:50.428  wpa2-key2    ->             c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  123  mic failure
Nov 15 00:47:51.924  wpa2-key1    <-             c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  117
Nov 15 00:47:51.937  wpa2-key2    ->             c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  123  mic failure
AP-635#
```

Reviewing the output, what Is the issue?
A. The RADIUS response from the authentication server is
B. The client device has an invalid certificate
C. The client device has an invalid pre-shared key.
D. transition mode is not enabled
Answer: C (LEAVE A REPLY)
The issue indicated by the output is an invalid pre-shared key (PSK). The logs show multiple failures during the WPA2 key exchange process, which points to a mismatch between the PSK configured on the client device and the PSK expected by the AOS 10 mobility gateway.

NEW QUESTION: 57
Your customer asked for help to apply an ACL for wireless guest users with the following criteria:
* Wi-Fi guests are on VLAN 555

* allow internet access
* only allow access to public DNS servers
* deny access to all internal networks except for any DHCP server

These session ACLs are already present in the CLI of the mobility gateway group:

You have access to the CLI. Which user role meets all the criteria?

A.
```
user-role "WiFi-guest"
    access-list session dhcp-acl
    access-list session internal-networks
    access-list session dns-acl
    vlan 555
```

B.
```
user-role "WiFi-guest"
    access-list session dhcp-acl
    access-list session dns-acl
    access-list session internal-networks
    access-list session allowall
    vlan 555
```

C.
```
user-role "WiFi-guest"
    access-list session dhcp-acl
    access-list session dns-acl
    access-list session internal-networks
    access-list session allowall
    vlan 555
```

D.
```
user-role "WiFi-guest"
    access-list session dns-acl
    access-list session internal-networks
    access-list session dhcp-acl
    access-list session allowall
    vlan 555
```

Answer: (SHOW ANSWER)

Based on the criteria provided for wireless guest users, the correct user role configuration must allow internet access, only allow access to public DNS servers, deny access to all internal networks except for any DHCP server, and place the Wi-Fi guests on VLAN 555. The ACLs must permit services necessary for basic internet access (such as DNS and DHCP) and block access to internal networks.

Option A satisfies these criteria with the following configurations:

* user-role "WiFi-guest": This defines the role for Wi-Fi guests.
* access-list session dhcp-acl: This applies the access list that likely permits DHCP, which is necessary for guests to obtain an IP address.
* access-list session dns-acl: This applies the DNS access list, which likely restricts guests to using public DNS servers.
* access-list session internal-networks: This applies the internal networks access list, which denies access to internal networks.
* vlan 555: This sets the VLAN for Wi-Fi guests to 555.

Options B, C, and D are incorrect because they include access-list session allowall which would permit all traffic, contradicting the requirement to deny access to all internal networks.

NEW QUESTION: 58

After onboarding three new AOS-10 gateways using the full-setup method into the same HPE Aruba Networking Central group, a customer cannot log in to one of the gateways using the HPE Aruba Networking Central remote console due to an incorrect password.

What is causing this issue?

A. The admin password created during the full-setup process is not configured to allow the remote console access

B. The admin password created at the HPE Aruba Networking Central group level has expired
C. The admin password created using full-setup does not match the global HPE Aruba Networking Central admin password
D. The admin password created during the full-setup process does not match the HPE Aruba Networking Central group admin password
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract of HPE Aruba Networking Switching:
When an AOS-10 gateway is onboarded into Aruba Central using the Full-Setup method, a local admin password is defined during the setup wizard on the gateway itself. Later, when the gateway joins an existing Aruba Central group, the group-level configuration (which includes the admin password defined for that group) is automatically pushed down to all devices in that group for configuration consistency.
However, if the password defined during full-setup is different from the admin password defined in the Aruba Central group, the synchronization process can cause a mismatch between the local device password and the one expected by Central. This mismatch prevents remote console login from working properly because Aruba Central attempts to authenticate to the gateway using the group-level admin credentials, not the local credentials from full-setup.
Exact Extract from HPE Aruba Networking Switching and Aruba Central Configuration Documents:
"During onboarding, the admin password configured at the group level in Aruba Central is applied to all devices in the group. If a device is added using full-setup with a different password, it may fail Central- initiated authentication functions such as remote console."
"When gateways are provisioned using the full-setup workflow, the local administrator password must match the group-level administrator credentials in Aruba Central to allow remote console and CLI access through Central." Therefore, the issue arises because the full-setup password for the gateway does not match the group admin password defined in Aruba Central, resulting in the 'incorrect password' error when attempting to access the gateway remotely through Central.
Why the Other Options Are Incorrect:
* A. The full-setup admin password is valid for remote access; there is no separate configuration option that "allows" or "disallows" remote console use.
"Remote console access uses the same admin account configured for device login; there is no additional enablement required."
* B. Aruba Central admin passwords do not expire by default. Group-level admin credentials are persistent configuration items, not time-based credentials.
"Local and group administrator passwords are static until manually changed."
* C. There is no "global Aruba Central admin password" used to authenticate to devices; authentication is performed using per-group or per-device credentials configured in Central.
"Each Aruba Central group maintains its own admin credentials that are propagated to member devices; there is no single global password for all groups."
References of HPE Aruba Networking Switching Documents or Study Guide:
* ArubaOS 10.5.0 Gateway Deployment and Configuration Guide - "Onboarding using Full Setup" and "Group-Level Configuration Synchronization."
* Aruba Central Device Management Guide - "Group Admin Credentials and Remote Console Access."
* Aruba AOS 10 Campus Gateway Installation and Setup Guide - "Matching Group Admin Passwords for Central-Managed Devices."