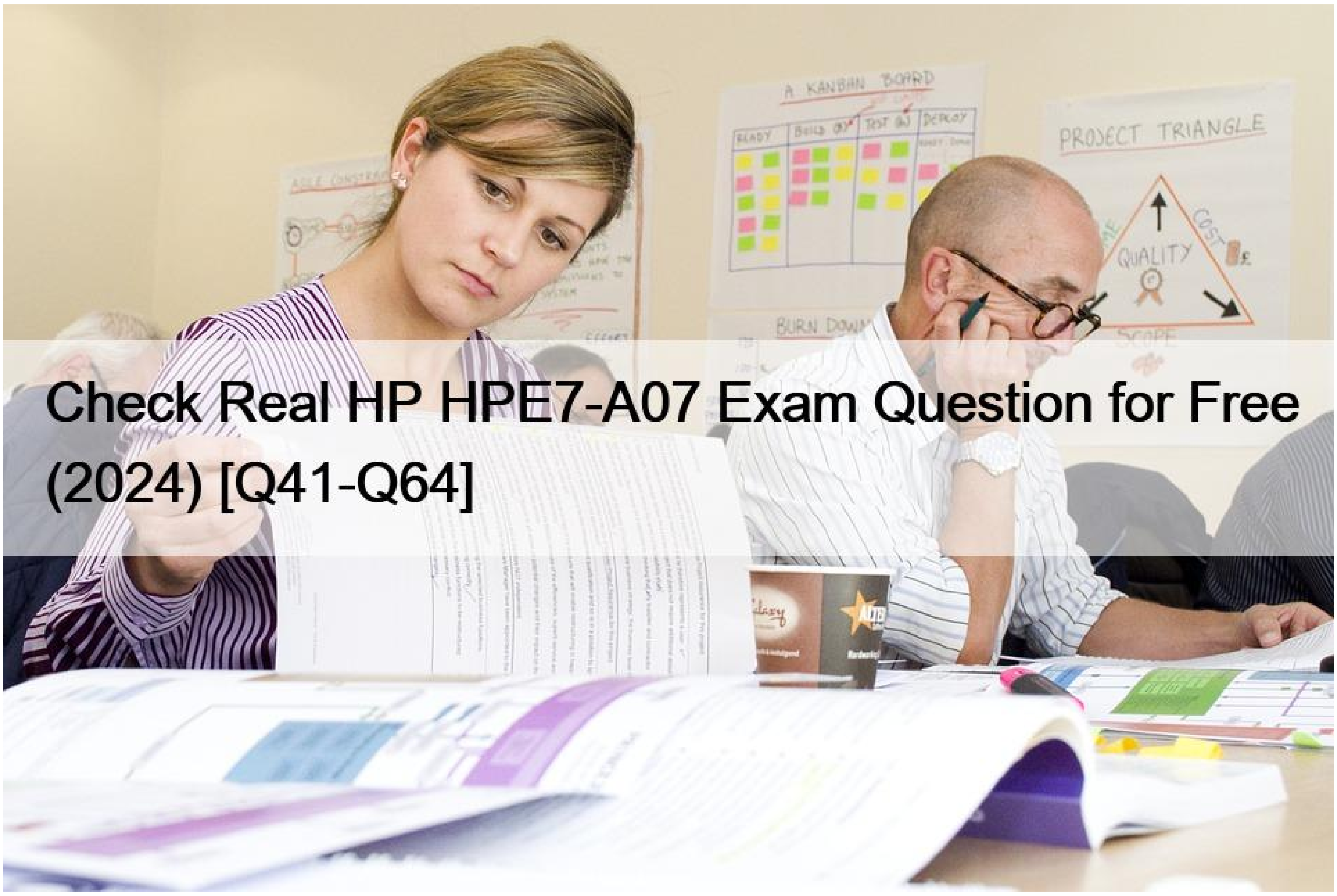
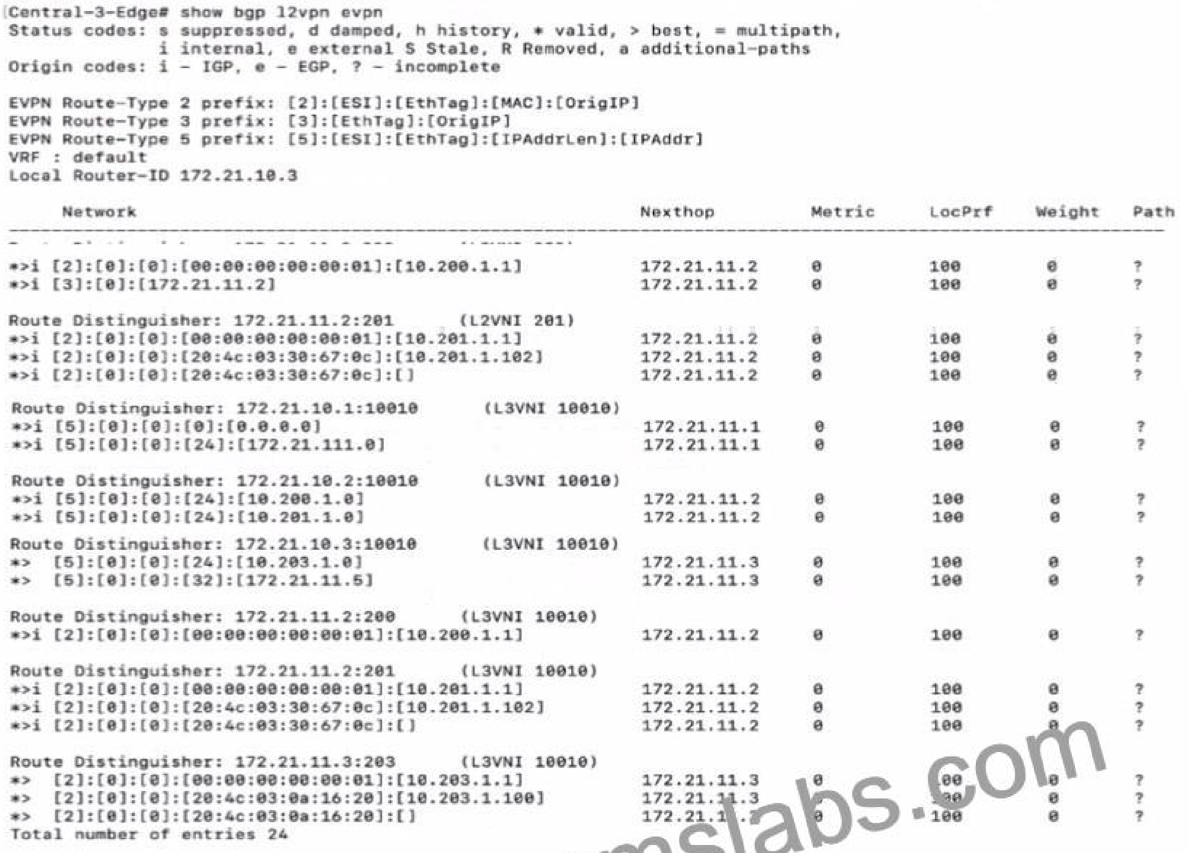
Check Real HP HPE7-A07 Exam Question for Free (2024) [Q41-Q64

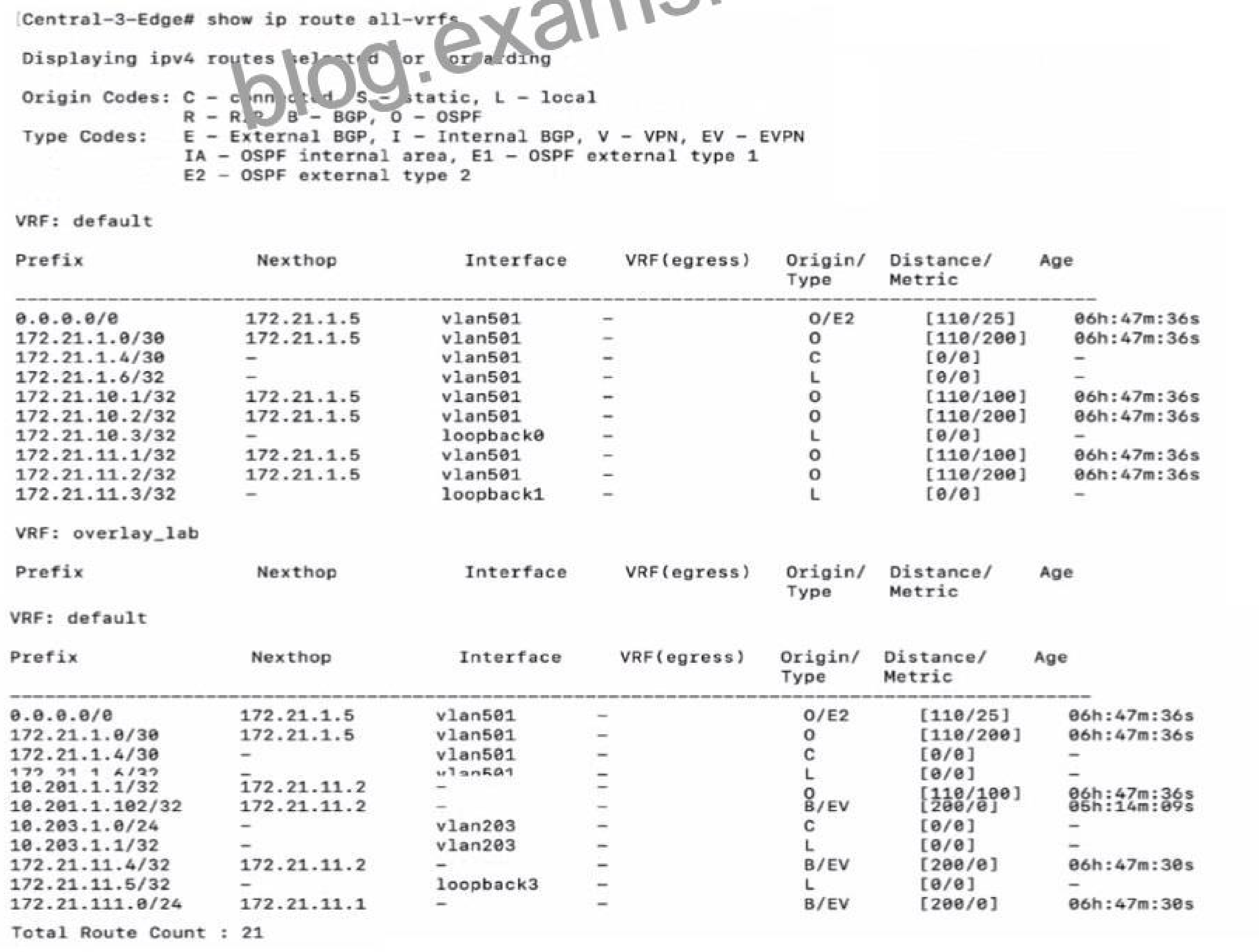


Check Real HP HPE7-A07 Exam Question for Free (2024) Get Ready to Boost your Prepare for your HPE7-A07 Exam with 70 Questions NEW QUESTION 41

Exhibit.



```
Central-3-Edge# show bgp l2vpn 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    Path
-----------------------------------------------------------------------------------------------------------

*>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: 172.21.11.2:201      (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]:[20:4c:03:30:67:0c]:[10.201.1.102]      172.21.11.2     0          100        0         ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[]                  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]:[10.203.1.0]                       172.21.11.3     0          100        0         ?
*>  [5]:[0]:[0]:[32]:[172.21.11.5]                      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         ?

Route Distinguisher: 172.21.11.2:201      (L3VNI 10010)
*>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]:[20:4c:03:30:67:0c]:[10.201.1.102]      172.21.11.2     0          100        0         ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[]                  172.21.11.2     0          100        0         ?

Route Distinguisher: 172.21.11.3:203      (L3VNI 10010)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.203.1.1]        172.21.11.3     0          100        0         ?
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[10.203.1.100]      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 24
```



```
Central-3-Edge# show ip route all-vrfs

 Displaying ipv4 routes selected for forwarding

 Origin Codes: C - connected, S - static, L - local
               R - RIP, B - BGP, O - OSPF
 Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
               IA - OSPF internal area, E1 - OSPF external type 1
               E2 - OSPF external type 2

VRF: default

Prefix            Nexthop          Interface     VRF(egress)     Origin/   Distance/     Age
                                                                 Type      Metric
-----------------------------------------------------------------------------------------------
0.0.0.0/0         172.21.1.5       vlan501     -                  O/E2       [110/25]     06h:47m:36s
172.21.1.0/30     172.21.1.5       vlan501     -                  O          [110/200]    06h:47m:36s
172.21.1.4/30     -                vlan501     -                  C          [0/0]        -
172.21.1.6/32     -                vlan501     -                  L          [0/0]        -
172.21.10.1/32    172.21.1.5       vlan501     -                  O          [110/100]    06h:47m:36s
172.21.10.2/32    172.21.1.5       vlan501     -                  O          [110/200]    06h:47m:36s
172.21.10.3/32    -                loopback0   -                  L          [0/0]        -
172.21.11.1/32    172.21.1.5       vlan501     -                  O          [110/100]    06h:47m:36s
172.21.11.2/32    172.21.1.5       vlan501     -                  O          [110/200]    06h:47m:36s
172.21.11.3/32    -                loopback1   -                  L          [0/0]        -

VRF: overlay_lab

Prefix            Nexthop          Interface     VRF(egress)     Origin/   Distance/     Age
                                                                 Type      Metric
VRF: default

Prefix            Nexthop          Interface     VRF(egress)     Origin/   Distance/     Age
                                                                 Type      Metric
-----------------------------------------------------------------------------------------------
0.0.0.0/0         172.21.1.5       vlan501     -                  O/E2       [110/25]     06h:47m:36s
172.21.1.0/30     172.21.1.5       vlan501     -                  O          [110/200]    06h:47m:36s
172.21.1.4/30     -                vlan501     -                  C          [0/0]        -
172.21.1.6/32     -                vlan501     -                  L          [0/0]        -
10.201.1.1/32     172.21.11.2      -           -                  O          [110/100]    06h:47m:36s
10.201.1.102/32   172.21.11.2      -           -                  B/EV       [200/0]      05h:14m:09s
10.203.1.0/24     -                vlan203     -                  C          [0/0]        -
10.203.1.1/32     -                vlan203     -                  L          [0/0]        -
172.21.11.4/32    172.21.11.2      -           -                  B/EV       [200/0]      06h:47m:30s
172.21.11.5/32    -                loopback3   -                  L          [0/0]        -
172.21.111.0/24   172.21.11.1      -           -                  B/EV       [200/0]      06h:47m:30s
Total Route Count : 21
```

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

* There are no active fabric clients on the CX switch with RD 172.16.10.1

* A wired client with IP address 10.203 1.100 is on a remote CX 6300 in the fabric with loopback IP address 172.21.11.2.

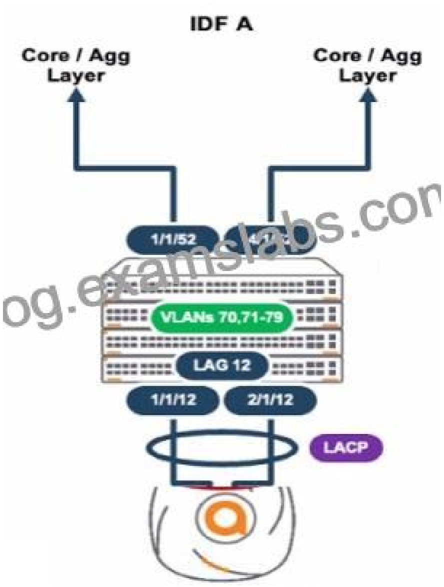
* A wired client with IP address 10 203 1 100 has a host route that is not being properly advertised

* The overlay loopbacK addresses are advertised in the faerie with 2d-bit subnet masks

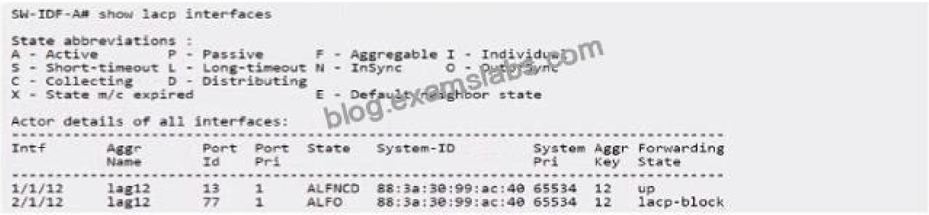
The CLI output provided shows routing information from a CX 6300 switch. The output under &#8220;VRF: default&#8221; shows various IP routes, including a route for 10.203.1.100/32 with a next hop of 172.21.11.2. This indicates that the route to the client with IP address 10.203.1.100 is known in the network and is reachable via another device in the fabric, which has the loopback IP address 172.21.11.2. Since the route is present in the routing table, it means that the client is known and active within the fabric network.

NEW QUESTION 42

A deployment using AP-635S is connectedto a stack of CX 6300s as shown.



The output of the snow LACPinterfaces 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?

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

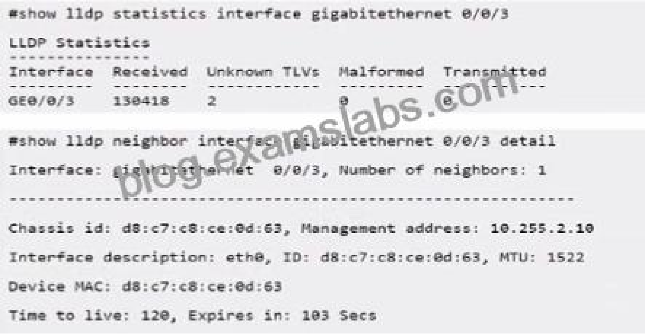
* Spanning tree and loop protect are enabled on both AP uplink ports.

* Each AP interface is connected to a routed-only interlace on different networks
* The AP is configured with LACP active
In an Aruba deployment, if an AP&#8217;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&#8217;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 43

A customer wan a gateway connected to a device on gigabitethernet0/0/3 configures an Asset ID TLVon the device for inventory management.

Exhibit.



```
#show lldp statistics interface gigabitethernet 0/0/3

LLDP Statistics
---------------
Interface  Received  Unknown TLVs  Malformed  Transmitted
---------  --------  ------------  ---------  -----------
GE0/0/3    130418    2             0          0

#show lldp neighbor interface gigabitethernet 0/0/3 detail

Interface: gigabitethernet  0/0/3, Number of neighbors: 1

------------------------------------------------------------

Chassis id: d8:c7:c8:ce:0d:63, Management address: 10.255.2.10

Interface description: eth0, ID: d8:c7:c8:ce:0d:63, MTU: 1522

Device MAC: d8:c7:c8:ce:0d:63

Time to live: 120, Expires in: 103 Secs
```

The customer mentions me Asset ID is not shown What is causing the issue?
* LLDP TX is not enabled.
* LLPD-MED needs to be enabled.
* MTU size is too small.
* Unknown TLVs cannot be displayed.
The issue is that unknown TLVs (Type Length Values) cannot be displayed. LLDP (Link Layer Discovery Protocol) is used to share device information with network neighbors, but if a TLV is not recognized by the LLDP implementation on the gateway, it won&#8217;t be displayed or processed. Hence, the Asset ID TLV set on the device for inventory management is not showing up because it is unrecognized or unsupported by the gateway&#8217;s LLDP.

NEW QUESTION 44

A customer is deploying a new warehouse with AP-634 APs inthe unitedStates with mobile devices that can operate in the 6GHz spectrum All testing and RF analyses were performed during the POC using AP-635 APs In a different location During the deployment, they noticed fewer 6GHz channels were broadcasting in the air.

Why would the AP-634 deployment have a lesser amount of broadcasting channels?
* The AP-634 APs do not have an advanced subscription.
* The AP-634 APs cannot broadcast an 6Gnz channels due to regulatory restrictions.
* The AP-635 APs received different allowable 6GHz channels from the AFC service versus the AP-634 APs due to the POC running in a different location.
* The AP-634 AP&#8217;s persona was configured in the Central group as Standard Power.
In the United States, the operation in the 6GHz band for Wi-Fi devices such as the AP-634 and AP-635 is regulated by the Automated Frequency Coordination (AFC) system, which determines the channels that can be used based on the location. Since the Proof of Concept (POC) was conducted in a different location using AP-635 APs, the allowable channels identified by the AFC

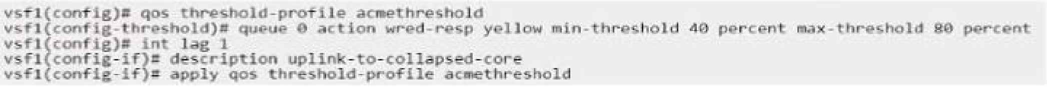
service for that location would be different than the channels allowed for the actual deployment location of the AP-634 APs. This would result in a different set of broadcasting channels being available for use in the new warehouse deployment.

NEW QUESTION 45

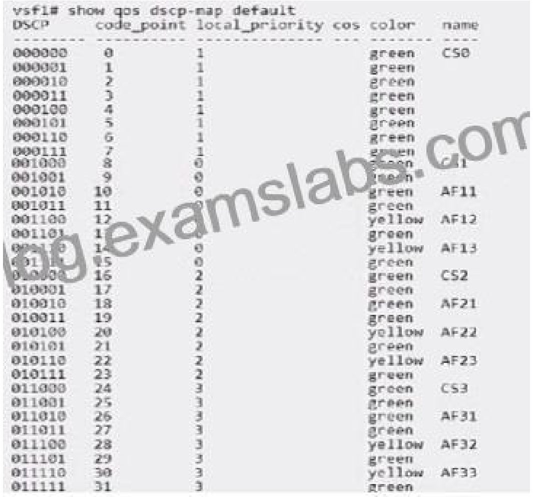
You are testing the use of the automated port-access role configuration process using RadSec authentication over VXLAN. During your testing you observed that the RadSec connection will fan during the digital certificate exchange What would be the cause of this Issue?
* The RadSec server was defined on the switch using an IPv6 address that was unreachable
* Tracking mode was set to &#8220;dead-only&#8221;, and the RadSec server was marked as unreachable.
* The switch is configured to establish a TLS connection with a proxy server, not the radius server.
* The RADIUS TCP packets are Being dropped and the TLS tunnel is not established.
During the testing of RadSec authentication over VXLAN, if the RadSec connection fails during the digital certificate exchange, it typically indicates an issue with the establishment of the TLS tunnel, which is required for RadSec&#8217;s secure communication. The failure of TLS tunnel establishment can occur due to RADIUS TCP packets being dropped, preventing the secure exchange of digital certificates necessary for RadSec authentication. The other options, such as IPv6 address reachability, tracking mode settings, and proxy server misconfiguration, are not directly related to the failure of the TLS tunnel establishment during the certificate exchange process

NEW QUESTION 46

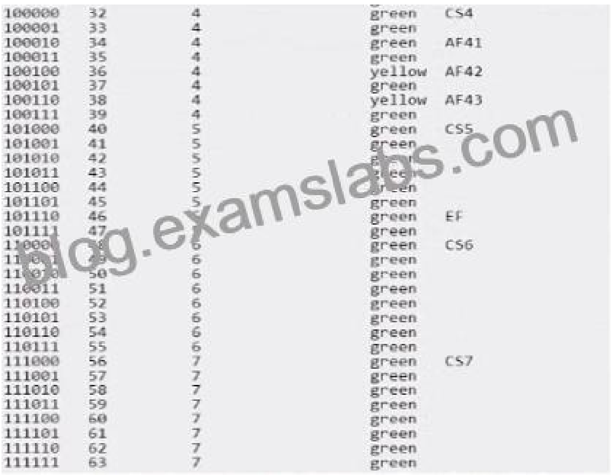
The ACME company has an AOS-CX 6200 switch stack with an uplink oversubscription ratio of 9.6:1. They are considering adding two more nodes to the stack without adding any additional uplinks due to cabling constraints One oftheir architects has expressed concerns that their critical UDP traffic from 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
```



```
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?
* edge mark lower priority TCP traffic with AF12
* edge mark critical UDP Traffic with CSS
* edge mark lower priority TCP traffic with AF11
* edge mark critical UDP traffic with AF42
Given that the ACME company&#8217;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.

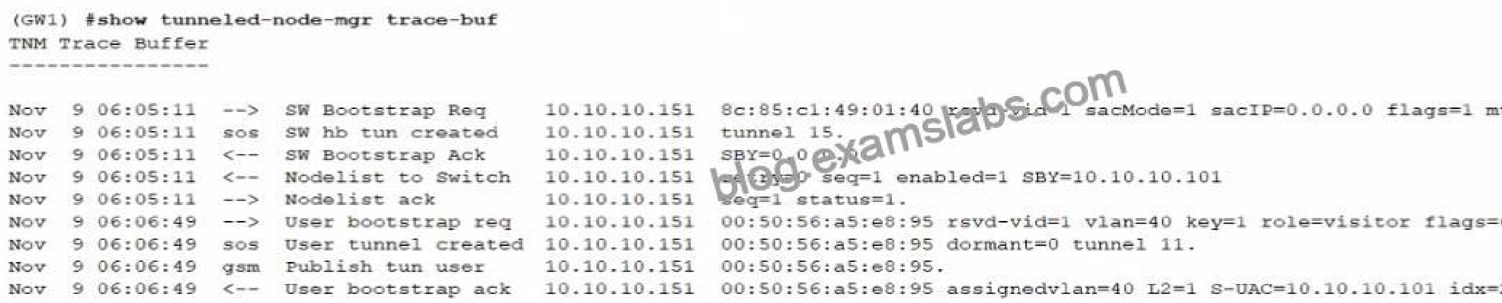
Option D,edge mark critical UDP traffic with AF42, is the correct answer. Assured Forwarding (AF) classes provide a way to assign different levels of delivery assurance for IP packets. AF42 is typically used for traffic that requires low latency and low loss, such as voice and video, which often use 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 47

Refer to the CLI output below:



```
(GW1) #show tunneled-node-mgr trace-buf
TNM Trace Buffer
----------------

Nov  9 06:05:11  -->  SW Bootstrap Req     10.10.10.151  8c:85:c1:49:01:40 rsvd-vid=1 sacMode=1 sacIP=0.0.0.0 flags=1 m
Nov  9 06:05:11  sos  SW hb tun created    10.10.10.151  tunnel 15.
Nov  9 06:05:11  <--  SW Bootstrap Ack     10.10.10.151  SBY=0.0.0.0
Nov  9 06:05:11  <--  Nodelist to Switch   10.10.10.151  active=0 seq=1 enabled=1 SBY=10.10.10.101
Nov  9 06:05:11  -->  Nodelist ack         10.10.10.151  seq=1 status=1.
Nov  9 06:06:49  -->  User bootstrap req   10.10.10.151  00:50:56:a5:e8:95 rsvd-vid=1 vlan=40 key=1 role=visitor flags=
Nov  9 06:06:49  sos  User tunnel created  10.10.10.151  00:50:56:a5:e8:95 dormant=0 tunnel 11.
Nov  9 06:06:49  gsm  Publish tun user     10.10.10.151  00:50:56:a5:e8:95.
Nov  9 06:06:49  <--  User bootstrap ack   10.10.10.151  00:50:56:a5:e8:95 assignedvlan=40 L2=1 S-UAC=10.10.10.101 idx=
```

What statement about the output above is correct?

- The port-access role was configured with gateway-role visitor
- The secondary tunnel endpoint IP is 10.10-10.151.
- The client authenticated using dot1x.
- The UBT zone was configured to use a user-defined VRF

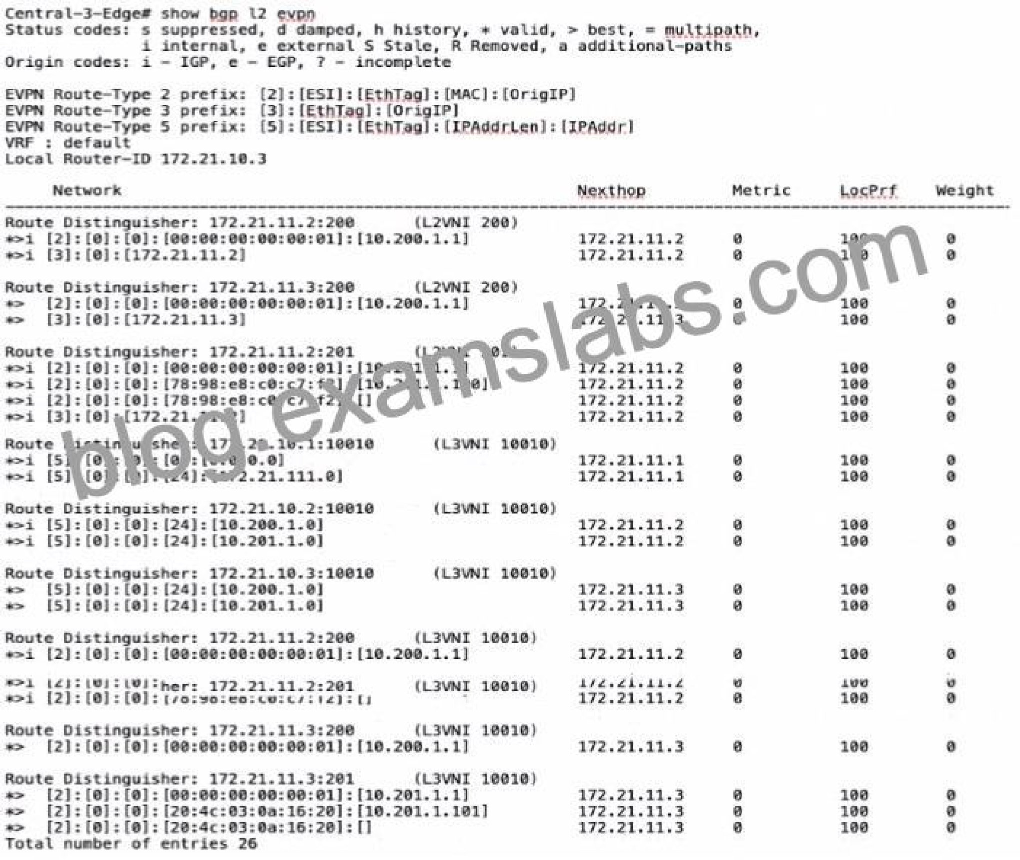
The CLI output indicates a tunnel creation process, where &#8220;SW hw tun created&#8221; refers to the switch hardware tunnel being created. The line mentioning &#8220;BYP-10.10.10.101 -> SW hw tun created to 10.10.10.151 tunnel

15.&#8221; implies that a tunnel was established to the secondary tunnel endpoint with the IP address 10.10.10.151.

This is a common configuration for User-Based Tunneling (UBT) setups where traffic is tunneled to a specific endpoint.

NEW QUESTION 48

Which statement is true given the following CLIoutput 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
```

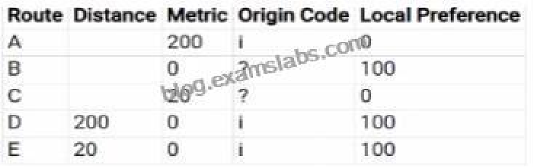
- The underlay loopback addresses are in the 172 21 11 x range.
- There are two anycast addresses m me overlay fabric.
- Duplicate MAC addresses were detected in the overlay fabric
- There are three active client overlay VLANs in the overlay fabric

The CLI output displays EVPN routes and their corresponding next hops. The &#8220;Route Distinguisher&#8221; 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 49

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

Referring to the table below whichroutewould be marked with a &#8220;>&#8221; 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

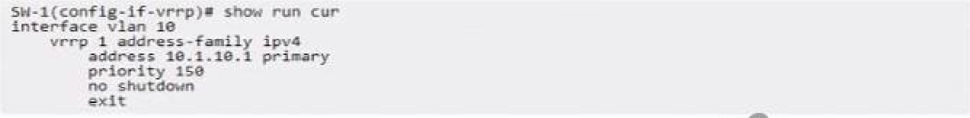
* Option A
* Option B
* Option C
* Option D
* Option E
In BGP, the route marked with a &#8220;>&#8221; symbol is the best route that is chosen based on BGP attributes in the following order: highest weight (Cisco-specific), highest local preference, originated by BGP running on the local router, shortest 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 &#8220;>&#8221; symbol as it has the highest local preference of 100 which is a decisive factor in the BGP best path selection process.

NEW QUESTION 50

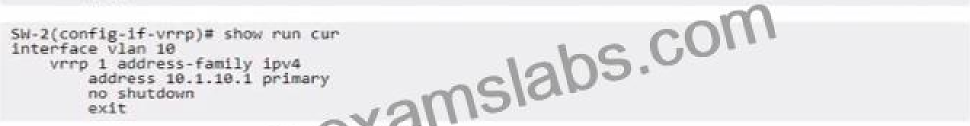
A customer&#8217;s infrastructure is set up to use both primary and secondary gateway clusters on the SSID profile based on best practices What is a valid cause tor having an equal spirt in APs connected to the primary and secondary gateway clusters?
* The secondary gateway cluster is heterogeneous
* The secondary gateway cluster is homogeneous
* 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
* The primary gateway cluster is up. out some APs cannot reach the secondary gateway cluster. These APs would connect to the secondary gateway cluster
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 51

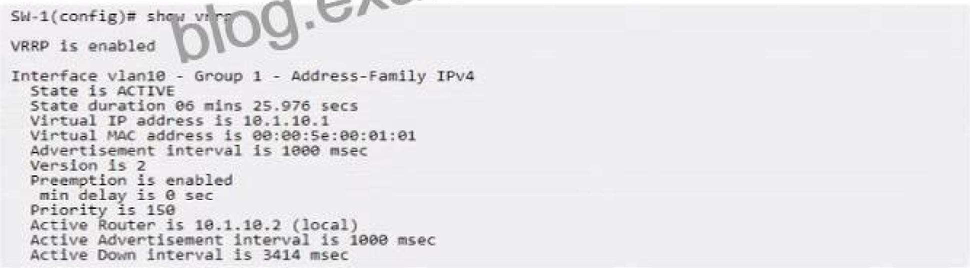
Exhibit.



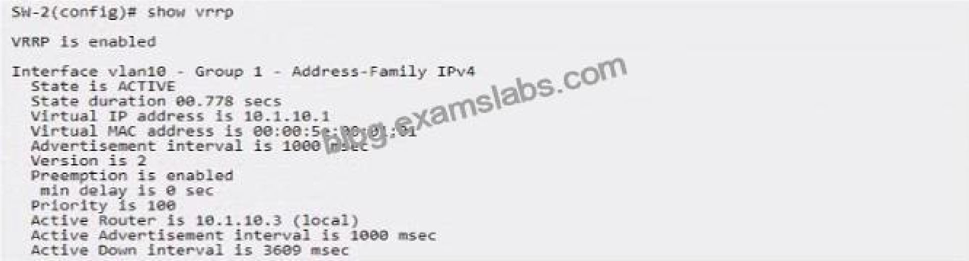
```
SW-1(config-if-vrrp)# show run cur
interface vlan 10
    vrrp 1 address-family ipv4
        address 10.1.10.1 primary
        priority 150
        no shutdown
        exit
```



```
SW-2(config-if-vrrp)# show run cur
interface vlan 10
    vrrp 1 address-family ipv4
        address 10.1.10.1 primary
        no shutdown
        exit
```



```
SW-1(config)# show vrrp

VRRP is enabled

Interface vlan10 - Group 1 - Address-Family IPv4
  State is ACTIVE
  State duration 06 mins 25.976 secs
  Virtual IP address is 10.1.10.1
  Virtual MAC address is 00:00:5e:00:01:01
  Advertisement interval is 1000 msec
  Version is 2
  Preemption is enabled
   min delay is 0 sec
  Priority is 150
  Active Router is 10.1.10.2 (local)
  Active Advertisement interval is 1000 msec
  Active Down interval is 3414 msec
```



```
SW-2(config)# show vrrp

VRRP is enabled

Interface vlan10 - Group 1 - Address-Family IPv4
  State is ACTIVE
  State duration 00.778 secs
  Virtual IP address is 10.1.10.1
  Virtual MAC address is 00:00:5e:00:01:01
  Advertisement interval is 1000 msec
  Version is 2
  Preemption is enabled
   min delay is 0 sec
  Priority is 100
  Active Router is 10.1.10.3 (local)
  Active Advertisement interval is 1000 msec
  Active Down interval is 3609 msec
```

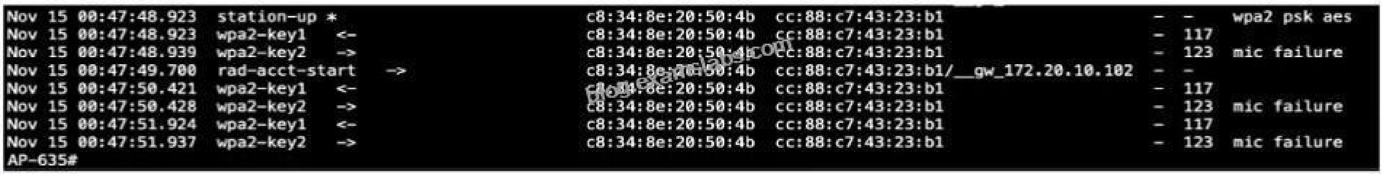
After configuring VRRP between sw-1 and SW-2. you notice that both switches are showing as active. What could be the reason for this issue?

* VRRP preemptive mode is disabled.
* SW-1 cam reach SW-2 on VLAN 10.
* Both switches are configured as VRRP &#8216;primary.&#8217;
* SW-2 has no priority configurations for VRRP 1.

In VRRP (Virtual Router Redundancy Protocol), only one switch should be the primary (master) for a given virtual IP address, with the other switches being backups. If both switches are showing as active, it suggests a misconfiguration where both are set to act as the primary for the same VRRP group. The exhibits provided indicate that both switches believe they are the active or primary for the VRRP group, which is an incorrect configuration.

NEW QUESTION 52

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#
```

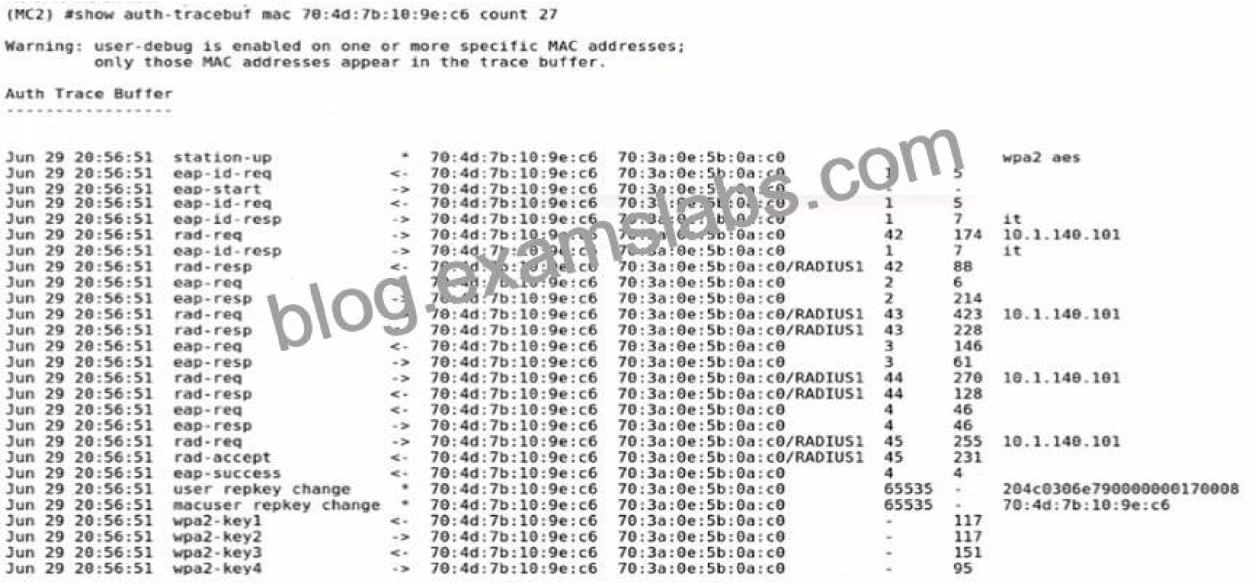
Reviewing the output, what Is the issue?

- The RADIUS response from the authentication server is
- The client device has an invalid certificate
- The client device has an invalid pre-shared key.
- transition mode is not enabled

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 53

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?

- MAC Authentication and 4-way handshake
- L3 authentication and encryption
- 802.11 enhanced open association
- L2 authentication and encryption

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 54

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

- SNR
- retry rate
- channel utilization
- number of connected clients

* frequency band

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 55

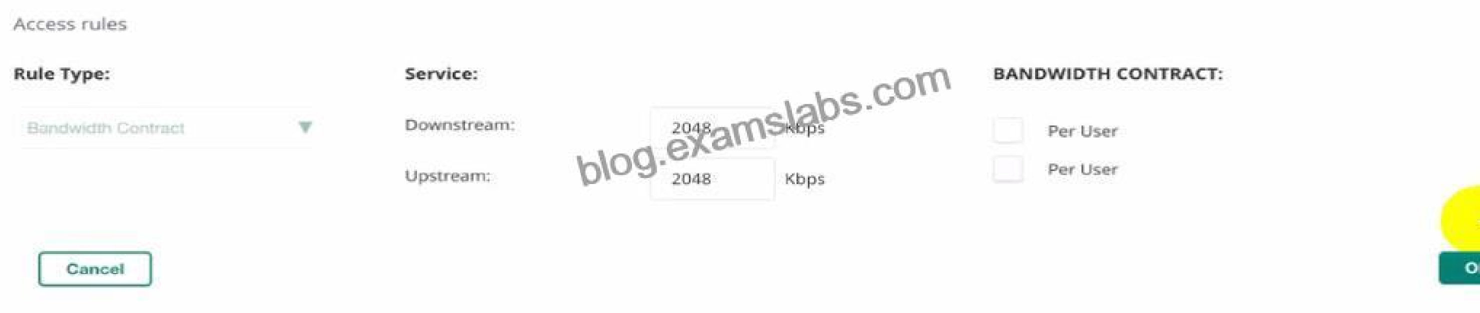
After onboarding three new AOS 10 gateways using the full-setup methodinto the same Central group, a customer cannot log in to one of the gateways using the HPE Aruba Networking Central remote console due to an incorrect password.

* The admin password created using full-setup does not match the global Central admin password.
* The admin password created during the run-setup process is not configured to allow me remote console access
* The admin password created during the full-setup process does not match the Central group admin password
* The admin password created at the Central group level has expired

When onboarding devices into a centralized management system, each device can have its individual admin password set during the onboarding process. If this password doesn&#8217;t match what is expected at the group level in the central management platform, login issues such as the one described can occur.

NEW QUESTION 56

Which option shows the correct Banawidth Control for 1024 kbpsdown and 2048 Kops up for the SSID?

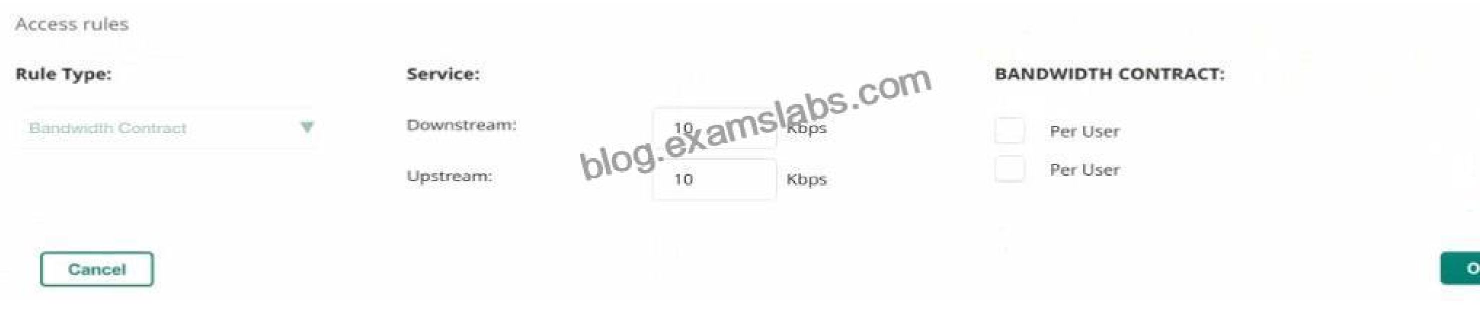
*


Access rules

Rule Type: Bandwidth Contract

Service:
Downstream: 2048 Kbps
Upstream: 2048 Kbps

BANDWIDTH CONTRACT:
□ Per User
□ Per User

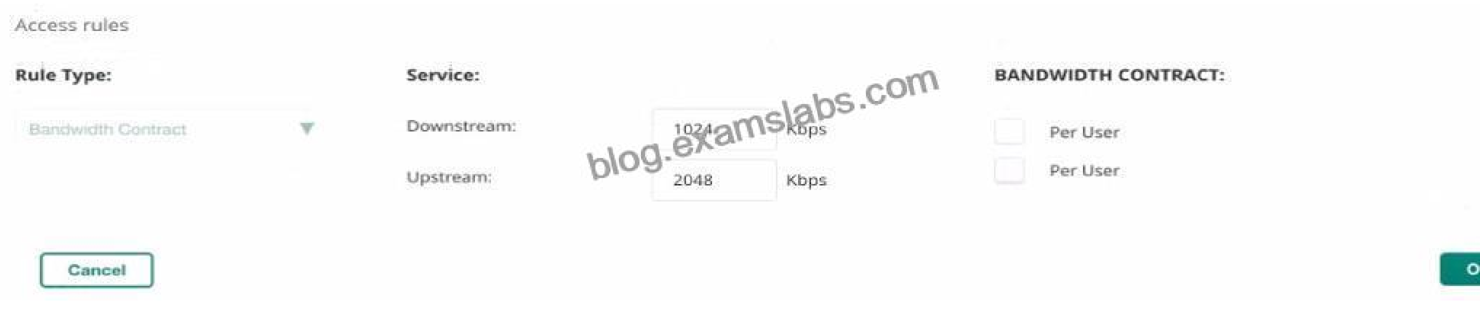
*


Access rules

Rule Type: Bandwidth Contract

Service:
Downstream: 10 Kbps
Upstream: 10 Kbps

BANDWIDTH CONTRACT:
□ Per User
□ Per User

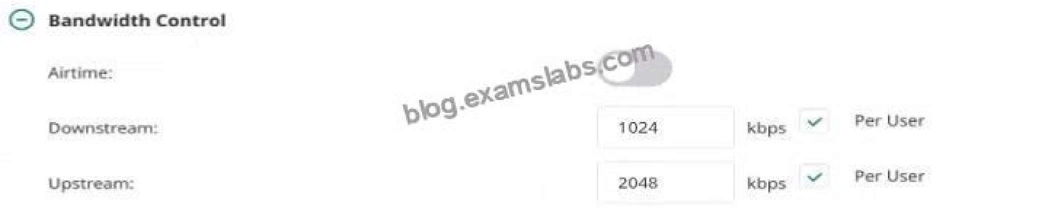
*


Access rules

Rule Type: Bandwidth Contract

Service:
Downstream: 1024 Kbps
Upstream: 2048 Kbps

BANDWIDTH CONTRACT:
□ Per User
□ Per User

* 

Bandwidth Control

Airtime:

Downstream: 1024 kbps ✓ Per User

Upstream: 2048 kbps ✓ Per User

The correct Bandwidth Control settings for 1024 Kbps down and 2048 Kbps up for the SSID are shown in Option D. In Option D, the downstream is set at 1024 Kbps and the upstream at 2048 Kbps, both configured per user, which matches the requested configuration. This setup ensures that each user has a guaranteed bandwidth allocation of the specified rates when connected to the SSID, providing a controlled and predictable user experience.

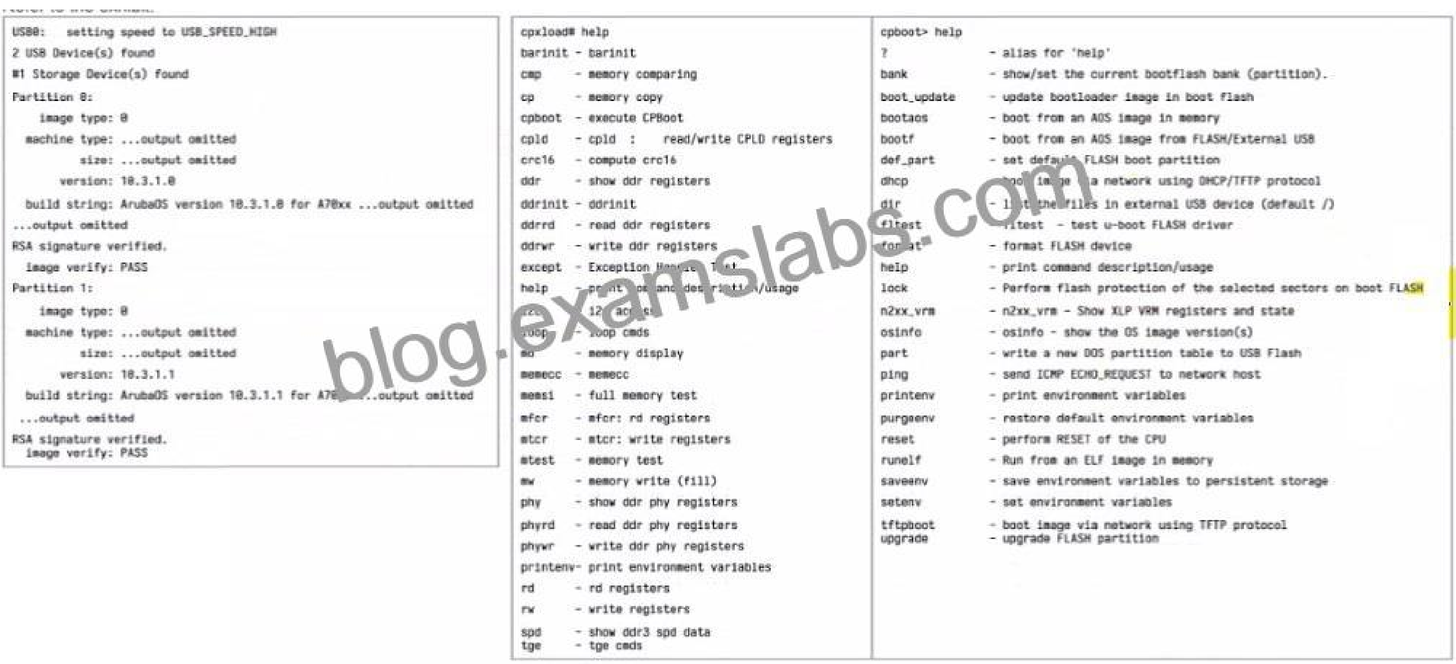
NEW QUESTION 57

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?
* device profiting on the switch
* from the AP MAC address table
* from the switch LLDP neighbors table
* from the switch MAC address table
HPE Aruba Networking Central can identify which switch port a rogue AP is connected to by using the switch&#8217;s MAC address table. The MAC address table contains the associations between MAC addresses and the switch ports to which devices (including APs) are connected. When Aruba Central detects a rogue AP, it can look up the MAC address of the rogue AP in the switch&#8217;s MAC address table to find the specific switch port it is connected to. This enables network administrators to quickly locate and address the rogue AP issue.

NEW QUESTION 58

Exhibit.



```
USB0:   setting speed to USB_SPEED_HIGH
2 USB Device(s) found
#1 Storage Device(s) found
Partition 0:
    image type: 0
  machine type: ...output omitted
          size: ...output omitted
       version: 10.3.1.0
  build string: ArubaOS version 10.3.1.0 for A70xx ...output omitted
...output omitted
RSA signature verified.
  image verify: PASS
Partition 1:
    image type: 0
  machine type: ...output omitted
          size: ...output omitted
       version: 10.3.1.1
  build string: ArubaOS version 10.3.1.1 for A70xx ...output omitted
 ...output omitted
RSA signature verified.
  image verify: PASS
```

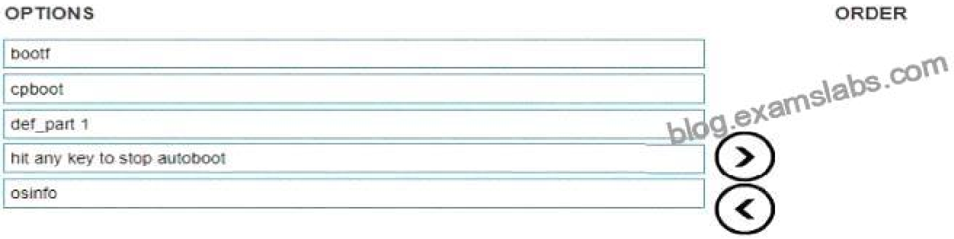
```
cpxload# help
barinit - barinit
cmp     - memory comparing
cp      - memory copy
cpboot  - execute CPBoot
cpld    - cpld  :    read/write CPLD registers
crc16   - compute crc16
ddr     - show ddr registers
ddrinit - ddrinit
ddrrd   - read ddr registers
ddrwr   - write ddr registers
except  - Exception Handler Test
help    - print command description/usage
i2c     - i2c access
loop    - loop cmds
md      - memory display
memecc  - memecc
memsi   - full memory test
mfcr    - mfcr: rd registers
mtcr    - mtcr: write registers
mtest   - memory test
mw      - memory write (fill)
phy     - show ddr phy registers
phyrd   - read ddr phy registers
phywr   - write ddr phy registers
printenv- print environment variables
rd      - rd registers
rw      - write registers
spd     - show ddr3 spd data
tge     - tge cmds
```

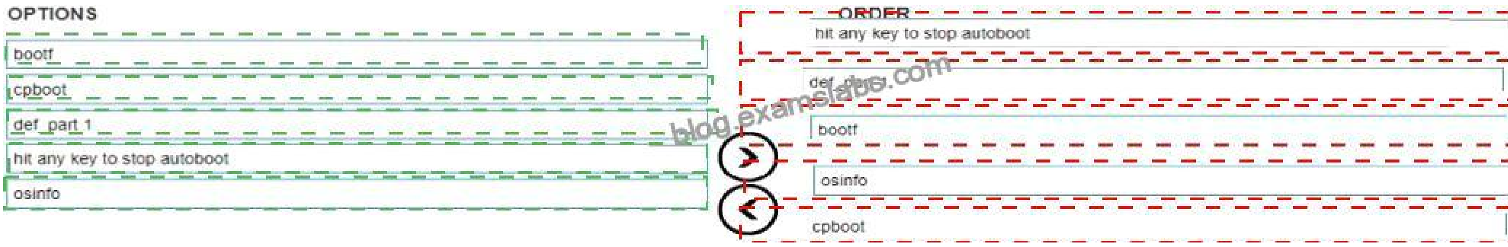
```
cpboot> help
?                - alias for 'help'
bank             - show/set the current bootflash bank (partition).
boot_update      - update bootloader image in boot flash
bootaos          - boot from an AOS image in memory
bootf            - boot from an AOS image from FLASH/External USB
def_part         - set default FLASH boot partition
dhcp             - boot image via network using DHCP/TFTP protocol
dir              - list the files in external USB device (default /)
fltest           - fltest  - test u-boot FLASH driver
format           - format FLASH device
help             - print command description/usage
lock             - Perform flash protection of the selected sectors on boot FLASH
n2xx_vrm         - n2xx_vrm - Show XLP VRM registers and state
osinfo           - osinfo - show the OS image version(s)
part             - write a new DOS partition table to USB Flash
ping             - send ICMP ECHO_REQUEST to network host
printenv         - print environment variables
purgeenv         - restore default environment variables
reset            - perform RESET of the CPU
runelf           - Run from an ELF image in memory
saveenv          - save environment variables to persistent storage
setenv           - set environment variables
tftpboot         - boot image via network using TFTP protocol
upgrade          - upgrade FLASH partition
```

You updated your gateway to me most recent firmware However after the firmware was updated, the gateway could no longer connect to HPE Aruba Networking Central. Your corporate ITIL procedures require you to implement your backout plan. You connected a console cable to your gateway and saw the following prompt.

Cpxload#

in what order, do you need to execute the following commands to return to the previous firmware version?





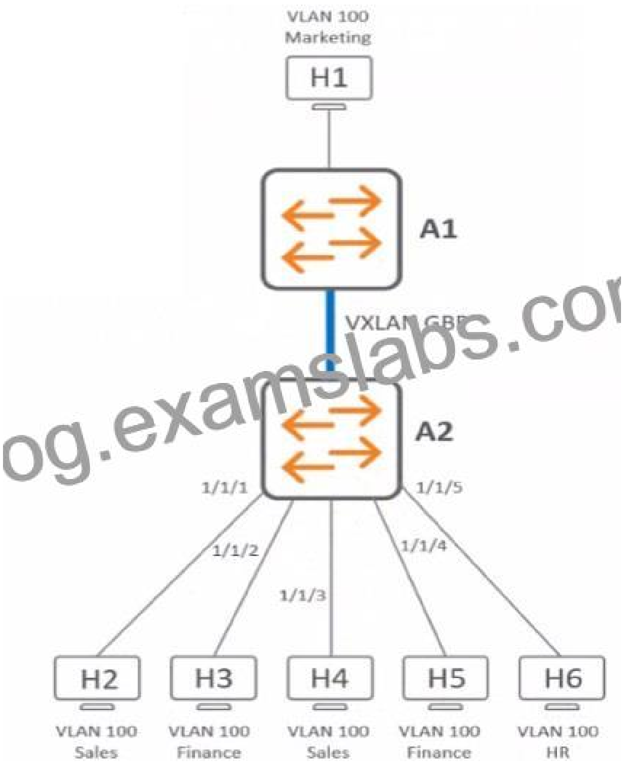
Explanation:

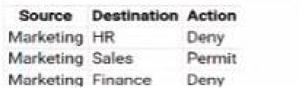
The sequence to return to the previous firmware version after an unsuccessful update would typically be:

hit any key to stop autoboot(This would prevent the system from automatically booting into the current, problematic firmware.) def_part 1(This command sets the default boot partition, which is likely where the previous working firmware is located.) bootf(This command would boot from the specified flash partition, which after the second step, would be the previous firmware.) osinfo(After the system is booted, this command could be used to confirm the firmware version now running on the gateway.)

NEW QUESTION 59

Exhibit.





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

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

- A2 will drop the ARP traffic.
- A2 will send the ARP traffic out of ports 1/1/1-1/1/4.
- A2 willflood the ARP traffic out of all interfaces.
- A2 willsend the ARP traffic out of ports 1/1/1 and 1/1/3.

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 requestreaches its intended destination, which might be on any of the interfaces. It&#8217;s a part of the standard behavior of switches to handle ARP traffic when the destination hardware address is unknown.

NEW QUESTION 60

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

- Use a custom LACP hash algorithm for improved load Balancing.
- Keep the MTU values at the default setting for GRE and VXLAN communications
- Use the command &#8220;vsx-sync mclag-interfaces&#8221; under the VSX context.
- Use the command &#8220;vsx-sync active-gateways&#8221; under the VSX context.

When configuring Virtual Switching Extension (VSX) in a campus topology for link aggregation across two aggregation switches, it is important to synchronize Multi-Chassis Link Aggregation Group (MC-LAG) interfaces. The command &#8220;vsx-sync mclag-interfaces&#8221; ensures that the state and configuration of MC-LAG interfaces are synchronized between the two VSX-linked switches,providing consistent link aggregation and preventing any loops or mismatched configurations that might occur if the interfaces were not in sync.

NEW QUESTION 61

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?
* Replace the Class a PoE switches with Class 6 PoE switches.
* Create two separate service profiles in the loT tab of the Central configuration settings.
* Perform a &#8220;poe disable&#8221; followed by a &#8220;poe enable&#8221; for the switch ports which connect to the APs so that the APs reboot.
* Move the AP-635 access points to a different group in Central to configure the dongles separately from the AP-615.

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 62

You are troubleshooting a WLAN deployment with APs and gateways set up with an 802.1X tunneled SSIO.

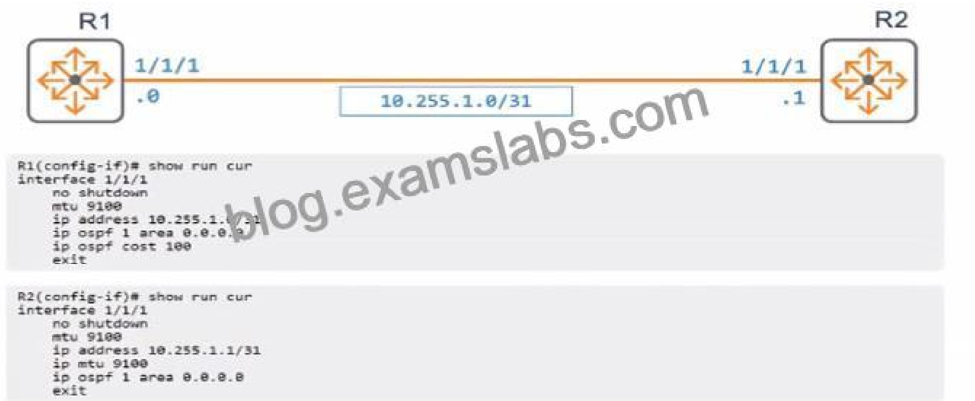
End-users are complaining that they can&#8217;t connect to die enterprise SSID. Which possible AP tunnel states could be the cause of the Issue? (Select two.)
* SM_STATE_RE KEYING
* SM_STATE_SURVIVED
* SM_STATE_CONNECTED
* SM_STATE_SURVIVING
* SM_STATE_CONNECTING

When troubleshooting a WLAN with 802.1X tunneled SSID issues, AP tunnel states indicate the status of the connection between the AP and the gateway/controller. The states &#8216;SM_STATE_REKEYING&#8217; and

&#8216;SM_STATE_CONNECTING&#8217; could indicate transitional states where the connection has not been fully established, hence users might face issues connecting to the SSID. &#8216;SM_STATE_REKEYING&#8217; implies that the AP is in the process of re-establishing encryption keys, while &#8216;SM_STATE_CONNECTING&#8217; indicates that the AP is trying to establish a connection with the controller or gateway. These states could lead to temporary connectivity issues until the state transitions to &#8216;SM_STATE_CONNECTED&#8217;.

NEW QUESTION 63

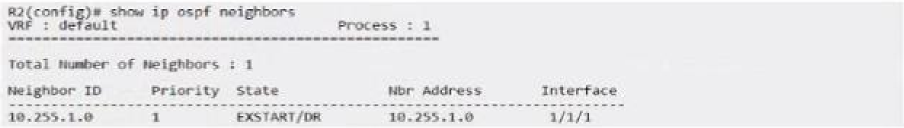
Exhibit.



```
R1(config-if)# show run cur
interface 1/1/1
    no shutdown
    mtu 9100
    ip address 10.255.1.0/31
    ip ospf 1 area 0.0.0.0
    ip ospf cost 100
    exit
```

```
R2(config-if)# show run cur
interface 1/1/1
    no shutdown
    mtu 9100
    ip address 10.255.1.1/31
    ip mtu 9100
    ip ospf 1 area 0.0.0.0
    exit
```

An engineer has applied the above configuration to R1 and R2 However the routers OSPF adjacency never progresses past the &#8220;EXSTART-DR&#8221; 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 &#8220;EXSTART/DR&#8221; state?
* Change R1 and R2 to a network type of point-to-point.
* Remove the layer 3 MTU configuration.
* Ensure the OSPF process is not configured with passive-interface default.
* Change the IP address and mask applied to interface 1/1/1.
In OSPF, the &#8220;EXSTART/DR&#8221; 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 &#8220;EXSTART&#8221; state and form a full adjacency.

NEW QUESTION 64

Your customer&#8217;s employees connected to a wired network are complaining about a poor user experience. The customer has UXI sensors deployed on their premises. These sensors nave been running for multiple months.

They are testing both the wired network (using the wired Interface of each sensor) and the wireless networks.

Your customer used the UXI dashboard to find the reason for the poor userexperience to find more details, the customer asked you to check the packet captures that have been downloaded from the sensors using the UXI dashboard.

From the zip file downloaded from the UXI sensors, you checked the &#8220;datagrams&#8221; .pcap file, but you were not able to find any issues How can you explain this?
* The &#8220;datagrams- pcap file only contains me successful tests Failed tests are contained in the

&#8220;datagrams-failed&#8221; .pcap file
* The UXI sensor could not upload the latest test results to the cloud, so the packet capture is outdated
* The datagrams captured on the physical Ethernet interface are in a different .pcap file.
* The default filers of the packet captures do not allow tailed tests to be captured by the sensor
It is a common practice to separate successful and failed test results into different files for ease of troubleshooting. If the &#8220;datagrams.pcap&#8221; file shows no issues, it&#8217;s likely because it only contains successful test data, and the failed tests that could explain the poor user experience would be in a different file, such as

&#8220;datagrams-failed.pcap.&#8221;

Use Free HPE7-A07 Exam Questions that Stimulates Actual EXAM :
https://www.examslabs.com/HP/Aruba-Certified-Professional/best-HPE7-A07-exam-dumps.html]