Free Questions for HPE7-A07

Shared by Yates on 14-03-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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

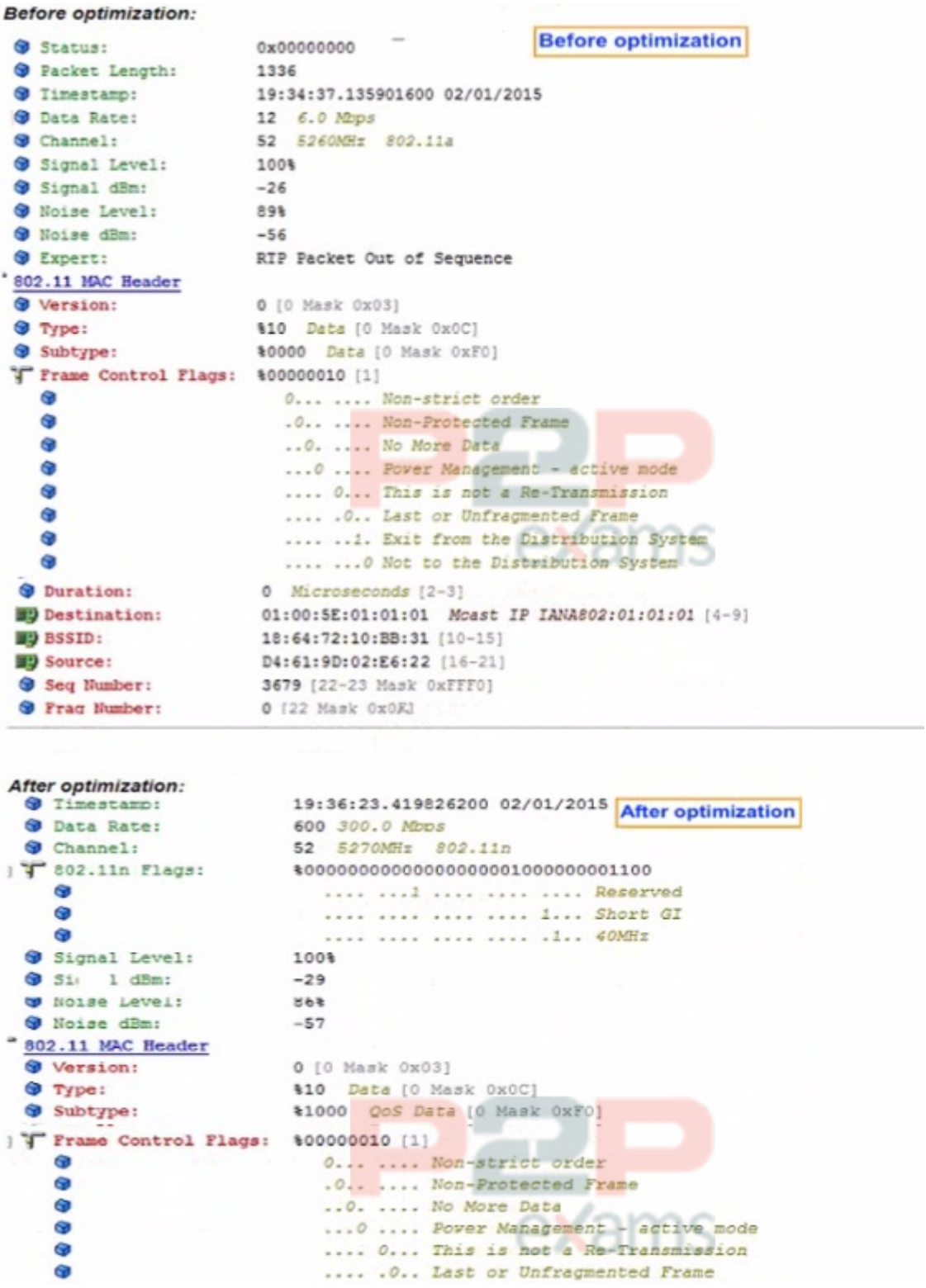
Explanation:

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.

Question 2

Question Type: MultipleChoice

Exhibit.



A network administrator attempts to improve multicast traffic flow and performs some packet captures for validation What can the network administrator conclude from the results?

Options:

A- The data rate increased from 6 Mops to 300 Mops because Broadcast Multicast optimization (BCMCO) was configured.

B- The capture taken after optimization does not show a packet length because Multicast

Transmission Optimization was configured.
C- The type flew remains consistent because Dynamic Multicast Optimization (DMO) was configured.
D- The data rate increased from 6 Mbps to 300 Mops because Dynamic Multicast Optimization (DMO) was configured.

Answer:

D

Explanation:

Dynamic Multicast Optimization (DMO) is a feature that enhances the delivery of multicast traffic by optimizing the data rate. The before and after optimization images show a significant increase in the data rate, which is a typical result of DMO being configured, as it allows multicast traffic to be transmitted at higher data rates by converting multicast streams into unicast streams for the clients that need them.

Question 3

Question Type: MultipleChoice

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?

Options:

A- There are no active fabric clients on the CX switch with RD 172.16.10.1
B- 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.
C- A wired client with IP address 10 203 1 100 has a host route that is not being properly advertised
D- The overlay loopbacK addresses are advertised in the faerie with 2d-bit subnet masks

Answer:

B

Explanation:

The CLI output provided shows routing information from a CX 6300 switch. The output under 'VRF: default' 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.

Question 4

Question Type: MultipleChoice

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)

```
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
```

Options:

A- Option A
B- Option B
C- Option C
D- Option D

Answer:

A

Explanation:

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.

Question 5

Question Type: MultipleChoice

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?

Options:

A- device profiting on the switch
B- from the AP MAC address table
C- from the switch LLDP neighbors table
D- from the switch MAC address table

Answer:

D

Explanation:

HPE Aruba Networking Central can identify which switch port a rogue AP is connected to by using the switch'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'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.

Question 6

Question Type: MultipleChoice

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?

Options:

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

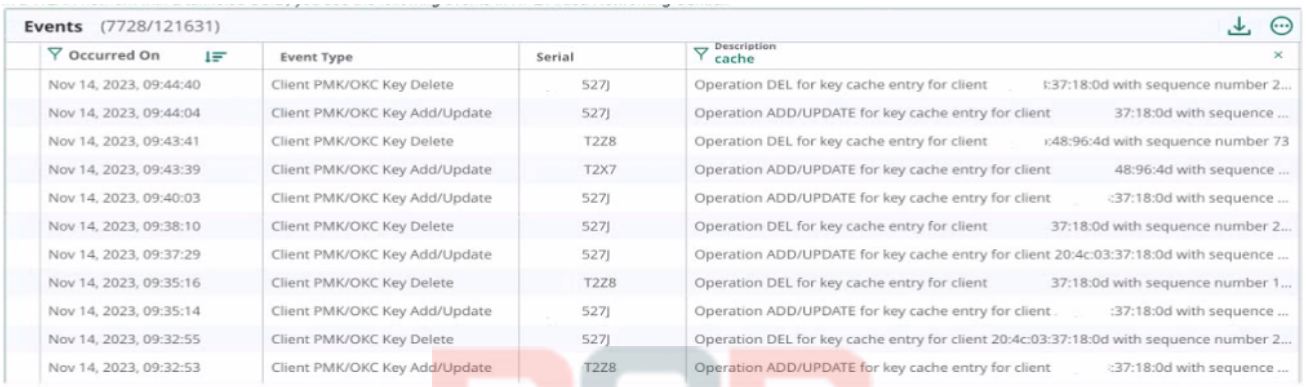
Explanation:

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.

Question 7

Question Type: MultipleChoice

in a WLAN network with a tunneled SSID. you see the following events in HPE Aruba Networking Central:



Events (7728/121631)

Occurred On	Event Type	Serial	Description cache
Nov 14, 2023, 09:44:40	Client PMK/OKC Key Delete	527J	Operation DEL for key cache entry for client :37:18:0d with sequence number 2...
Nov 14, 2023, 09:44:04	Client PMK/OKC Key Add/Update	527J	Operation ADD/UPDATE for key cache entry for client 37:18:0d with sequence ...
Nov 14, 2023, 09:43:41	Client PMK/OKC Key Delete	T2Z8	Operation DEL for key cache entry for client :48:96:4d with sequence number 73
Nov 14, 2023, 09:43:39	Client PMK/OKC Key Add/Update	T2X7	Operation ADD/UPDATE for key cache entry for client 48:96:4d with sequence ...
Nov 14, 2023, 09:40:03	Client PMK/OKC Key Add/Update	527J	Operation ADD/UPDATE for key cache entry for client :37:18:0d with sequence ...
Nov 14, 2023, 09:38:10	Client PMK/OKC Key Delete	527J	Operation DEL for key cache entry for client 37:18:0d with sequence number 2...
Nov 14, 2023, 09:37:29	Client PMK/OKC Key Add/Update	527J	Operation ADD/UPDATE for key cache entry for client 20:4c:03:37:18:0d with sequence ...
Nov 14, 2023, 09:35:16	Client PMK/OKC Key Delete	T2Z8	Operation DEL for key cache entry for client 37:18:0d with sequence number 1...
Nov 14, 2023, 09:35:14	Client PMK/OKC Key Add/Update	527J	Operation ADD/UPDATE for key cache entry for client :37:18:0d with sequence ...
Nov 14, 2023, 09:32:55	Client PMK/OKC Key Delete	527J	Operation DEL for key cache entry for client 20:4c:03:37:18:0d with sequence number 2...
Nov 14, 2023, 09:32:53	Client PMK/OKC Key Add/Update	T2Z8	Operation ADD/UPDATE for key cache entry for client :37:18:0d with sequence ...

The customer asks you to investigate log messages What should you tell them?

Options:

A- This indicates a security issue. The client with a MAC address ending with 37 18;0d Is performing a Denial-of-Service attack on your network. You should track down the client and remove it from the network.

B- This is normal, expected behavior. No further actions are needed.

C. This indicates a client WLAN driver issue for the client with a MAC address ending with 37:18 :Od. You should upgrade the client WLAN driver.

D- There is a roaming issue Enable Fast Roaming 802.11r and OKC to resolve the issue.

Answer:

B

Explanation:

The event log showing PMK (Pairwise Master Key) and OKC (Opportunistic Key Caching) key add/update and delete operations is indicative of normal client behavior in a WLAN environment. These events are part of the standard process for maintaining client session security and do not necessarily indicate any issue.

Question 8

Question Type: MultipleChoice

A customer is running out of IP addresses in a network segment. What will happen If they add an

additional IPsubnet to the same VLAN?

Options:

A- Broadcasts for me two subnets win arrive on all ports in the same VLAN
B- IGMP will not work in both of the subnets in the same VLAN
C- This would result in a single SVI using two subinterfaces.
D- Users can reach each other and establish PTP traffic without passing an L3 point in the same VLAN

Answer:

D

Explanation:

Adding an additional IP subnet to the same VLAN means that devices configured with either subnet can communicate at Layer 2 without the need for routing. This is because they are on the same VLAN and thus in the same broadcast domain. However, to communicate between subnets, an L3 device or inter-VLAN routing would be required.

Question 9

Question Type: MultipleChoice

A customer has deployed an AOS 10 mobility gateway cluster consisting of three controllers at a single site The WLAN is configured to tunnel wireless device traffic to the AOS 10 mobility cluster The clients are authenticated by ClearPass using WPA3-Enterprise (opmode wpa3-aes-ccm-128). The security team has requested the ability to force a wireless device to reauthenticate using ClearPass.

Which steps are required to ensure ClearPass can consistently initiate a change of authorization against an AOS 10 mobility cluster, including during gateway failover scenarios? (Select two)

Options:

A- set cluster mode to Auto Site under High Availability - Cluster configuration
B- modify WLAN - SSID - VLAN - Mode Configuration
C- enable manual cluster configuration under High Availability - Cluster Configuration
D- enable Dynamic Authorization CoA under High Availability - Cluster Configuration

E- modify NAS IPv4 address under Security - Advanced - RADIUS Client

Answer:

D, E

Explanation:

To ensure that ClearPass can initiate a Change of Authorization (CoA) consistently, it's important to enable dynamic authorization to allow RADIUS CoA messages to be processed. This setting typically falls under the high-availability cluster configuration to ensure that it persists across gateway failovers. Additionally, the NAS IP address must be configured under RADIUS client settings to ensure that the correct IP address is used for RADIUS communications, which is necessary for CoA to function correctly.