HPE6-A79 Q&As

Aruba Certified Mobility Expert Written Exam

Pass HP HPE6-A79 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/hpe6-a79.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Users run Skype for Business on wireless clients with no WMM support over an Aruba Mobility Master (MM) - Mobility Controller (MC) based network. When traffic arrives at the wired network, it does not include either L2 or L3 markings.

Which configuration steps should the network administrator take to classify and mark voice and video traffic with UCC heuristics mode?

A. Enable WMM in a VAP profile, and explicitly permit voice and video UDP ports in a firewall policy.

B. Confirm OpenFlow is enabled in the user role and VAP profile. Then enable WMM in a SSID profile, and explicitly permit voice and video UDP ports in a firewall policy.

C. Confirm the MC is the Openflow controller of the MMs and Openflow is enabled in VAP and firewall roles. Enable Skype4Business ALG in UCC profiles.

D. Confirm MM is the Openflow controller of MCs and Openflow is enabled in VAP and firewall roles. Enable Skype4Business ALG in UCC profiles.

Correct Answer: A

QUESTION 2

An organization wants to deploy a WLAN infrastructure that provides connectivity to these client categories:

Employees Contractors Guest users Corporate IoT legacy devices that support no authentication or encryption Employees and contractors must authenticate with company credentials and get network access based on AD group membership. Guest users are required to authenticate with captive portal using predefined credentials. Only employees will run L2 encryption.

Which implementation plan fulfills the requirements while maximizing the channel usage?

A. Create VAP1 to run WPA2-AES and 802.1x authentication, VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal and L2 fail through.

B. Create a single VAP to run WPA2-AES and 802.1x authentication, MAC authentication L2 fail through, captive portal, and VIA support.

C. Create VAP1 to run WPA2-AES and 802.1x authentication, VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal.

D. Create VAP1 to run WPA2-AES and 802.1x authentication, and VAP2 to run opensystem encryption with MAC authentication and captive portal.

Correct Answer: D

QUESTION 3

A network administrator has racked up a 7210 Mobility Controller (MC) that will be terminating 200+ Aps on a medium-

size branch office. Next, the technician cabled the appliance with 4SPF+ Direct Attached Cables (DACs) distributed between two-member switching stack and powered it up.

What must the administrator do next in the MCs to assure maximum wired bandwidth utilization?

A. Map the four physical ports to port channel 0.

B. Disable spanning tree and allocate unique VLANs to each port.

C. Manually set 10Gbps speeds on all ports.

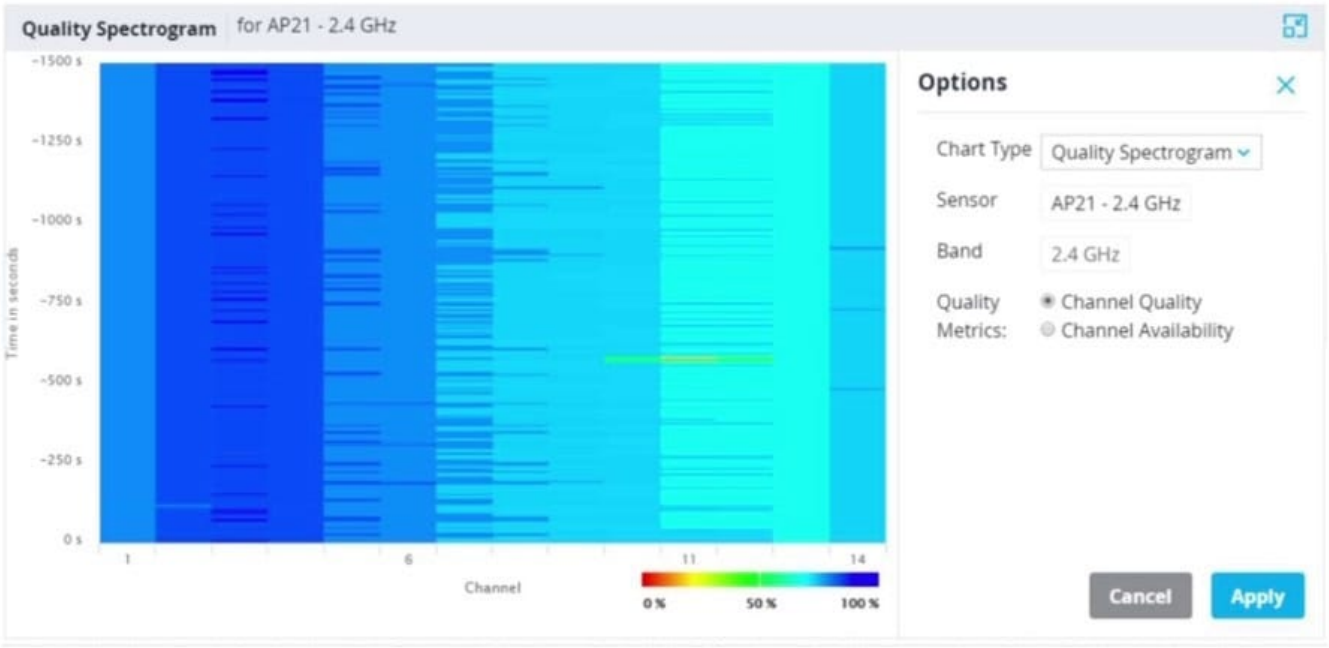
D. Configure the same MSTP region that the switches have.

E. Make all ports trunk interfaces and permit data VLANs.

Correct Answer: C

QUESTION 4

Refer to the exhibit.



Based on the output shown in the exhibit, which channel offers the highest quality?

A. Channel 1

B. Channel 6

C. Channel 11

D. Channel 14

Correct Answer: B

QUESTION 5

Refer to the exhibit.

```
(MC2) #show auth-tracebuf mac xx:xx:xx:xx:xx:xx 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            *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -       -    wpa2 aes
Jun 29 20:56:51  eap-id-req           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1       5
Jun 29 20:56:51  eap-start             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -       -
Jun 29 20:56:51  eap-id-req           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1       5
Jun 29 20:56:51  eap-id-resp            ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1       7    it
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          42      174  10.1.140.101
Jun 29 20:56:51  eap-id-resp            ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1       7    it
Jun 29 20:56:51  rad-resp              <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  42      88
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          2       6
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          2       214
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  43      423  10.1.140.101
Jun 29 20:56:51  rad-resp              <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  43      228
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          3       146
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          3       61
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  44      270  10.1.140.101
Jun 29 20:56:51  rad-resp              <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  44      128
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          4       46
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          4       46
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  45      255  10.1.140.101
Jun 29 20:56:51  rad-accept            <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  45      231
Jun 29 20:56:51  eap-success           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          4       4
Jun 29 20:56:51  user repkey change     *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          65535   -    204c0306e790000000170008
Jun 29 20:56:51  macuser repkey change   *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          65535   -    xx:xx:xx:xx:xx:xx
Jun 29 20:56:51  wpa2-key1             <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -       117
Jun 29 20:56:51  wpa2-key2             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -       117
Jun 29 20:56:51  wpa2-key3             <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -       151
Jun 29 20:56:51  wpa2-key4             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -       95
```

Based on the output shown in the exhibit, which wireless connection phase has just completed?

A. L3 authentication and encryption

B. MAC Authentication and 4-way handshake

C. 802.11 enhanced open association

D. L2 authentication and encryption

Correct Answer: A

QUESTION 6

A network administrator is in charge of a Mobility Master (MM) ?Mobility Controller (MC) based WLAN. The administrator has deployed an Airwave Management Platform (AMP) server in order to improve the monitoring capabilities and

generate reports and alerts.

The administrator has configured SNMPv3 and Admin credentials on both the MMs and MCs and has created Groups and Folders in the AMP server.

What two additional steps must the administrator do in order to let Airwave monitor the network devices? (Choose two.)

A. Manually add the Active MM and wait for automatic Discovery.

B. Map the AMP\\'s IP address with a mgmt-config profile in the MM.

C. Set the AMP\\'s IP address and Org string as DHCP option 43.

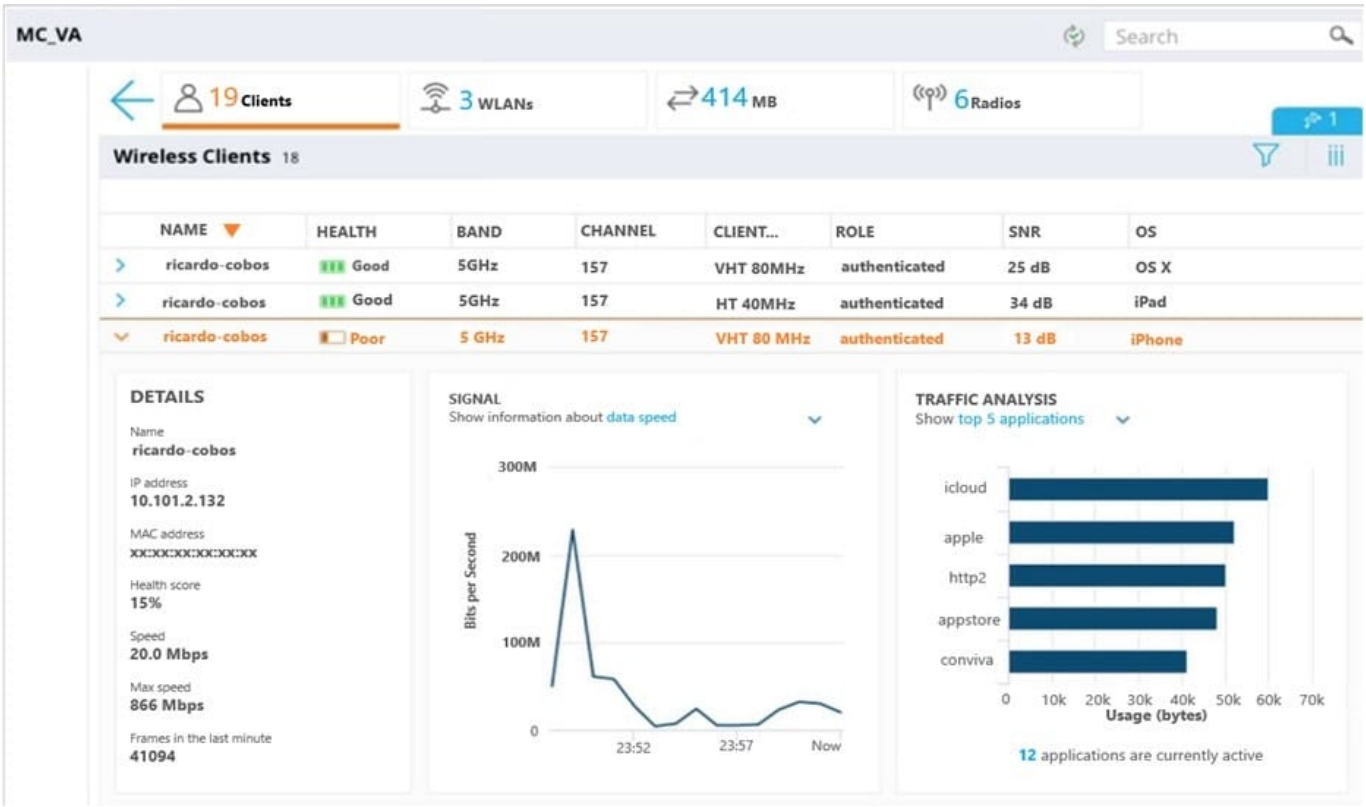
D. Manually add each MM, MC and Access Point in the AMP server.

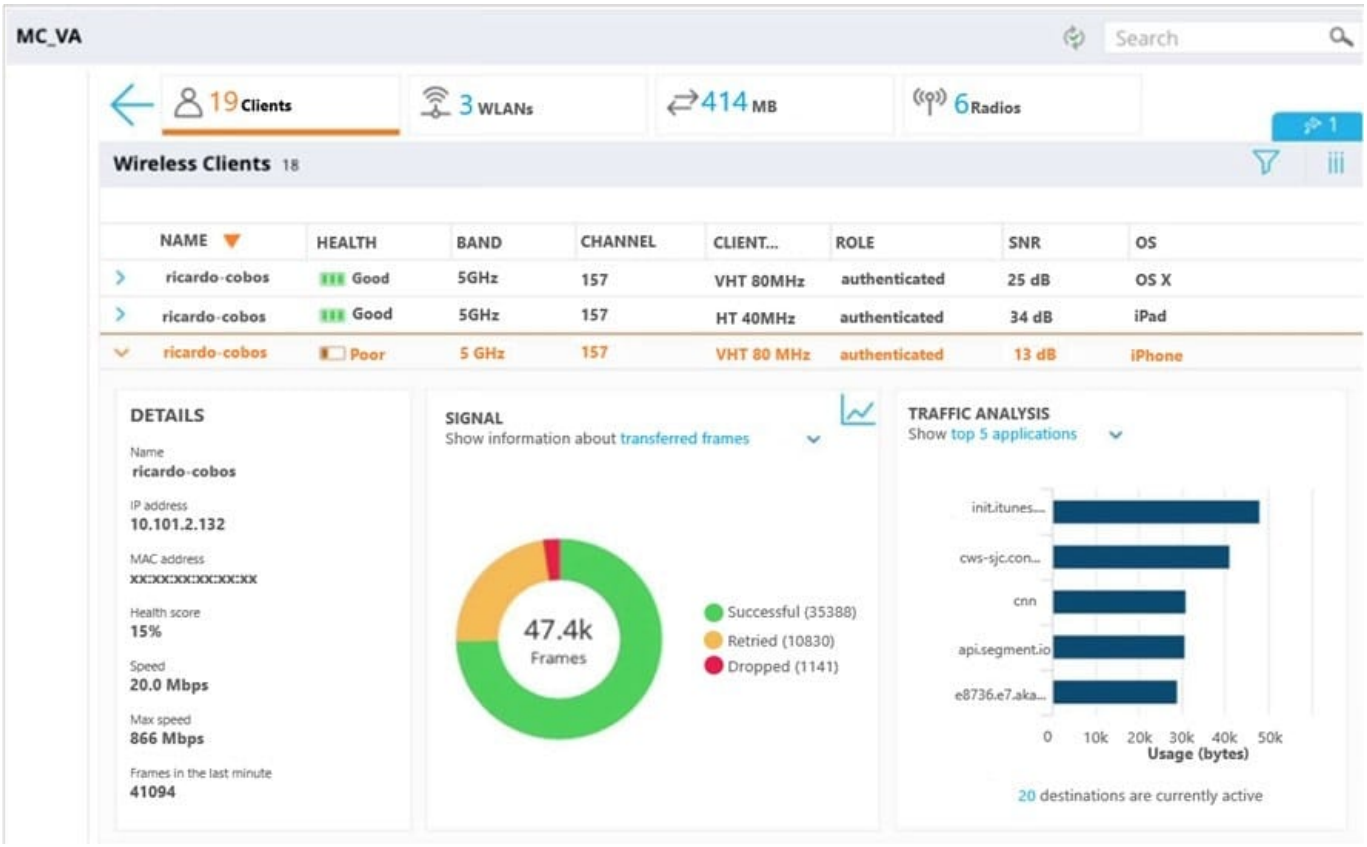
E. Move "New" devices into a group and folder in Airwave.

Correct Answer: AB

QUESTION 7

Refer to the exhibits.





A user reports slow response time to a network administrator and suggests that there might be a problem with the WLAN. The user\\'s phone supports 802.11ac in the 5 GHz band. The network administrator finds the user in the Mobility Master (MM) and reviews the output shown in the exhibit.

What can the network administrator conclude after analyzing the data?

A. The low SNR forces the client to back off to low MCs, therefore speed is low and retransmits are high.

B. Client health is poor, but SNR is fair. TX power must be increased in both the client and the AP.

C. Since SNR is good, then the high retransmit rate must be due a hidden node scenario or high interference.

D. High Successful frame count and high Max Speed is an indication of a healthy client. Connection will improve at any time.

Correct Answer: D

QUESTION 8

Refer to the exhibit.

```
(MC2) #show auth-tracebuf mac xx:xx:xx:xx:xx:xx count 27

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

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

A. EAP authentication

B. 802.1X machine authentication

C. MAC authentication

D. 802.1X user authentication

Correct Answer: D

QUESTION 9

Refer to the exhibit.

```
(MC2) #show datapath session table 10.1.141.150


Datapath Session Table Entries
------------------------------

Flags: F - fast age, S - src NAT, N - dest NAT
       D - deny, R - redirect, Y - no syn
       H - high prio, P - set prio, T - set ToS
       C - client, M - mirror, V - VOIP
       Q - Real-Time Quality analysis
       u - Upstream Real-Time Quality analysis
       I - Deep inspect, U - Locally destined
       E - Media Deep Inspect, G - media signal
       r - Route Nexthop, h - High Value
       A   Application Firewall Inspect
       B - Permanent, O - Openflow
       L - Log

Source IP         Destination IP   Port   SPort   DPort  Cntr      Prio  ToS  Age  Destination  TAge  Packets   Bytes     Flags
---------------- ---------------- ----  -----  -----  --------- ----  ---  ---  ------------ ----  --------  --------- -------------
10.254.1.21       10.1.141.150     17    53      64519  0/0       0     0    1    tunnel 29    12    2         318       FIA
10.254.1.24       10.1.141.150     6     5061    62781  0/0       6     0    0    tunnel 29    5f5   110       79604     I
10.1.141.150      13.107.21.200    6     62852   443    0/0       0     6    1    tunnel 29    25    29        8501      C
10.1.141.150      10.254.1.21      17    64519   53     0/0       0     0    1    tunnel 29    12    2         154       FCIA
10.254.1.24       10.1.141.150     17    51248   5968   0/0       5     34   0    0/0/0        22    1294      270387    FHPTCV

10.1.141.150      10.254.1.24      6     62781   5061   0/0       6     6    0    tunnel 29    5f7   100       32340     CI
10.254.1.24       10.1.141.150     17    51249   5969   0/0       5     34   0    0/0/0        24    208       134541    FHPTCV
23.218.154.187    10.1.141.150     6     443     62849  0/0       0     0    4    tunnel 29    3a    16        15430
10.1.141.150      13.107.21.200    6     62853   443    0/0       0     6    2    tunnel 29    27    11        1137      C
10.1.141.150      10.254.1.24      17    5969    51249  0/0       0     0    0    0/0/0        24    207       131034    FHPTV

13.107.21.200     10.1.141.150     6     443     62853  0/0       0     0    3    tunnel 29    27    14        8962
10.1.141.150      23.218.145.187   6     62849   443    0/0       0     6    4    tunnel 29    3a    10        1198      C
13.107.21.200     10.1.141.150     6     443     62852  0/0       0     0    2    tunnel 29    27    32        10610
10.1.141.150      10.254.1.24      17    5968    51248  0/0       0     0    1    0/0/0        24    19        2304      FHPTV
```

A network administrator deploys DSCP based prioritization in the entire wired network to improve voice quality for a SIP-based IP telephony system used by the company. However, users report that calls they make from WLAN have poor audio quality, while desktop phones do not experience the same problem. The network administrator makes a test call and looks in the datapath session table.

Based on the output shown in the exhibit, what is one area that the network administrator should focus on?

A. UCC based DSCP correction

B. WMM support on the WLAN

C. Dynamic Multicast Rate Optimization

D. wired network congestion

Correct Answer: D

QUESTION 10

Refer to the exhibit.

```
xx:xx:xx:xx:xx:xx# sh dhcp subnets

DHCP Subnet Table
-----------------
VLAN  Type  Subnet        Mask             Gateway       Mode                  Rolemap
----  ----  ------        ----             -------       ----                  -------
124   l3    10.21.124.32  255.255.255.224  10.21.124.33  local, split-tunnel
81    l2    0.0.0.0       255.255.255.255  0.0.0.0       remote, full-tunnel
```

A network engineer deploys two different DHCP pools in an Instant AP (IAP) cluster for WLANs that will have

connectivity to a remote site using Aruba IPSec. Based on the output shown in the exhibit, which IAP-VPN DHCP modes are being used?

A. distributed L3 and centralized L2

B. local L3 and centralized L2

C. local L3 and distributed L2

D. centralized L3 and distributed L2

Correct Answer: D