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.lead4pass.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

A network administrator has updated the ArubaOS code of a standalone Mobility Controller (MC) that is used for User-Based Tunneling (UBT) to a newer early release. Ever since the MC seems to reject PAPI sessions from the switch with the 10.1.10.10 IP address. Also the controller\\'s prompt is now followed by a star mark: "(MC_VA) [mynode] *#"

When opening a support ticket, an Aruba TAC engineer asks the administrator to gather the crash logs and if possible replicate UBT connection attempts from the switch while running packet captures of PAPI traffic on the controller and obtain the PCAP files. The administrator has a PC with Wireshark and TFTP server using the 10.0.20.20 IP address.

What commands must the administrator issue to accomplish these requests? (Choose two.)

A.
```
packet-capture destination ip-address 10.0.20.20
packet-capture datapath ipsec 10.1.10.10
```

B.
```
show tech-support logs.tar
copy flash: logs.tar tffp: 10.0.20.20 logs.tar
copy flash: logs.tar_md5sum.txt tffp: 10.0.20.20 logs.tar_md5sum.txt
```

C.
```
tar logs
copy flash: logs.tar tffp: 10.0.20.20 logs.tar
copy flash: logs.tar_md5sum.txt tffp: 10.0.20.20 logs.tar_md5sum.txt
```

D.
```
tar crash
copy flash: logs.tar tffp: 10.0.20.20 crash.tar
copy flash: logstarmd5sum.txt tffp: 10.0.20.20 crash.tarmd5sum.txt
```

E.
```
packet-capture destination ip-address 10.0.20.20
packet-capture controlpath udp all
```


A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Correct Answer: BE

QUESTION 2

Refer to the exhibit

```
(MC11) [mynode] #show ap database | exclude =

AP Database
-----------
Name  Group    AP Type  IP Address    Status   Flags  Switch IP     Standby IP
----  -----    -------  ----------    ------   -----  ----------   ----------
AP21  CAMPUS   355      10.1.145.150  Down            10.254.13.14  0.0.0.0
AP22  CAMPUS   355      10.1.146.150  Up 7m:4s IL     10.254.13.14  0.0.0.0


Total Aps:2
(MC11) [mynode] #show version | include Aruba

Aruba Operating System Software.
ArubaOS (MODEL: ArubaMC-VA-US), Version 8/2/1/0
(MC11) [mynode] #
(MC11) [mynode] #show log system 5| include "license"
Jun 21 12:20:25 :399814: <5481> <DBUG> |cfgn| Config Manager is not ready to send the new license config to the applications yet
Jun 21 12:29:34 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP xx:xx:xx:xx:xx:xx
Jun 21 12:29:38 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP xx:xx:xx:xx:xx:xx
Jun 21 12:34:42 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP AP22
Jun 21 12:34:46 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP AP22
(MC11) [mynode] #
(MC11) [mynode] #show license aggregate

Aggregate License Table for pool /
----------------------------------
Hostname     IP Address   Mac addr          AP   REF  RF Protect  ACR  WebCC  MM  MC-VA-RW  MC-VA-EG  MC-VA-IL  MC-VA-JP  MC-VA-US  VIA
 Last update (secs. ago)
--------     ----------   --------          ---- ---- ----------  ---- -----  --- --------- --------  --------  --------  --------  ---
 ------------------------
From Server  10.254.13.14 yy:yy:yy:yy:yy:yy 16   0    0           0    0      0   0         0         0         0         0         0


Total no. of clients: 0
```

A network administrator deploys a standalone Mobility Controller (MC) and configures some VAPs within the CAMPUS AP group. The network administrator realizes that none of the VAPs are being broadcasted.

Based on the output shown in the exhibit, what should the network administrator do to solve this problem?

A. Install MC-VA licenses, then install PEF licenses and enabled the PEF feature.

B. Install MC-VA licenses, then reprovision the APs.

C. Install MM licenses, then install PEF licenses and enable the PEF feature.

D. Install MM licenses and install MC-VA licenses, then install RFP licenses.

Correct Answer: D

QUESTION 3

A joint venture between two companies results in a fully functional WLAN Aruba solution. The network administrator uses the following script to integrate the WLAN solution with two radius servers, radius1 and radius2.

```
aaa authentication-server radius radius1
   host 10.254.1.1
   key key111
!
aaa authentication-server radius radius2
   host 10.20.2.2
   key key222
!
aaa server-group group-corp
auth-server radius1

aaa profile aaa-corp
authentication-dot1x authenticated
dot1x-server-group group-corp
!
wlan ssid-profile ssid-corp
essid corp
opmode wpa2-aes
!
wlan virtual-ap vap-corp
aaa-profile aaa-corp
ssid-profile ssid-corp
!
ap-group building1
virtual-ap vap-corp
```


While all users authenticate with username@domainname.com type of credentials, radius1 has user accounts with the domain name portion. Which additional configuration is required to authenticate corp1.com users with radius1 and corp2 users with radius2?

A.
```
aaa authentication-server radius radius1
trim-fqdn
!
aaa server-group-corp
 auth-server radius1 match-domain corp1.com
 auth-server radius1 match-domain corp2.com
```

B.
```
aaa authentication-server radius radius1
 trim-fqdn
!
aaa server-group-corp
 auth-server radius1 match-authstring corp1.com
 auth-server radius1 match-authstring corp2.com
```

C.
```
aaa authentication-server radius radius1
!
aaa server-group-corp
 auth-server radius1 match-string corp1.com trim-fqdn
 auth-server radius1 match-string corp2.com
```

D.
```
aaa server-group-corp
 auth-server radius1 match-fqdn corp1.com
 auth-server radius1 trim-fqdn
 auth-server radius2 match-fqdn corp2.com
```


A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 4

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 5

Refer to the exhibit.

```
(MC1) [MDC] #show aaa profile corp_aaa_prof

AAA Profile "corp_aaa_prof"
-----------------------
Parameter                                      Value
---------                                      -----
Initial role                                   logon
MAC Authentication Profile                     N/A
MAC Authentication Default Role                guest
MAC Authentication Server Group                default
802.1X Authentication Profile                  corp-employee_dot1_aut
802.1X Authentication Default Role             guest
802.1X Authentication Server Group             Radius
Download Role from CPPM                        Disabled
Set username from dhcp option 12               Disabled
L2 Authentication Fail Through                 Disabled
Multiple Server Accounting                     Disabled
User idle timeout                              N/A
Max IPv4 for wireless user                     2
RADIUS Accounting Server Group                 N/A
RADIUS Roaming Accounting                      Disabled
RADIUS Interim Accounting                      Disabled
RADIUS Acct-Session-Id In Access-Request       Disabled
XML API server                                 N/A
RFC 3576 server                                N/A
User derivation rules                          N/A
Wired to Wireless Roaming                      Enabled
Reauthenticate wired user on VLAN change       Disabled
Device Type Classification                     Enabled
Enforce DHCP                                   Disabled
PAN Firewall Integration                       Disabled
Open SSID radius accounting                    Disabled
Apply ageout mechanism on bridge mode wireless clients  Disabled
(MC1) [MDC] #
```

A network administrator has created AAA profile for the corporate VAP. In addition to the regular Radius based authentication, the administrator needs to be able to disconnect the users from either of the two servers that are part of the "Radius" server group.

What must the administrator do next in order to achieve this goal?

A. Use the "Radius" server group as the RADIUS Accounting Server Group in the AAA profile.

B. Create two new RFC 3576 servers and assign them as the RFC 3576 servers in the AAA profile.

C. Use the "Radius" server group as both the Accounting Server Group and the RFC 3576 server in the AAA profile.

D. Use the "Radius" server group as the RFC 3576 server in the AAA profile.

Correct Answer: C

Reference: https://www.arubanetworks.com/techdocs/ArubaOS_61/ArubaOS_61_UG/AP_Config.php

QUESTION 6

Refer to the exhibit.

```
(MC2)  [MDC] #show user mac xx:xx:xx:xx:xx:xx
This operation can take a while depending on number of users. Please be patient ....


Name: contractor14, IP:10.1.141.150, MAC: xx:xx:xx:xx:xx:xx, Age: 00:00:00
Role: contractor (how: ROLE_DERIVATION_DOT1X_VSA), ACL: 128/0
Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-PEAP, server: ClearPass.23
Authentication Servers: dot1x authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: ROLE_DERIVATION_DOT1X_VSA
```

A network administrator is evaluating a deployment to validate that a user is assigned the proper role and reviews the output in the exhibit. How is the role assigned to user?

A. The MC assigned the role based on Aruba VSAs.

B. The MC assigned the machine authentication default user role.

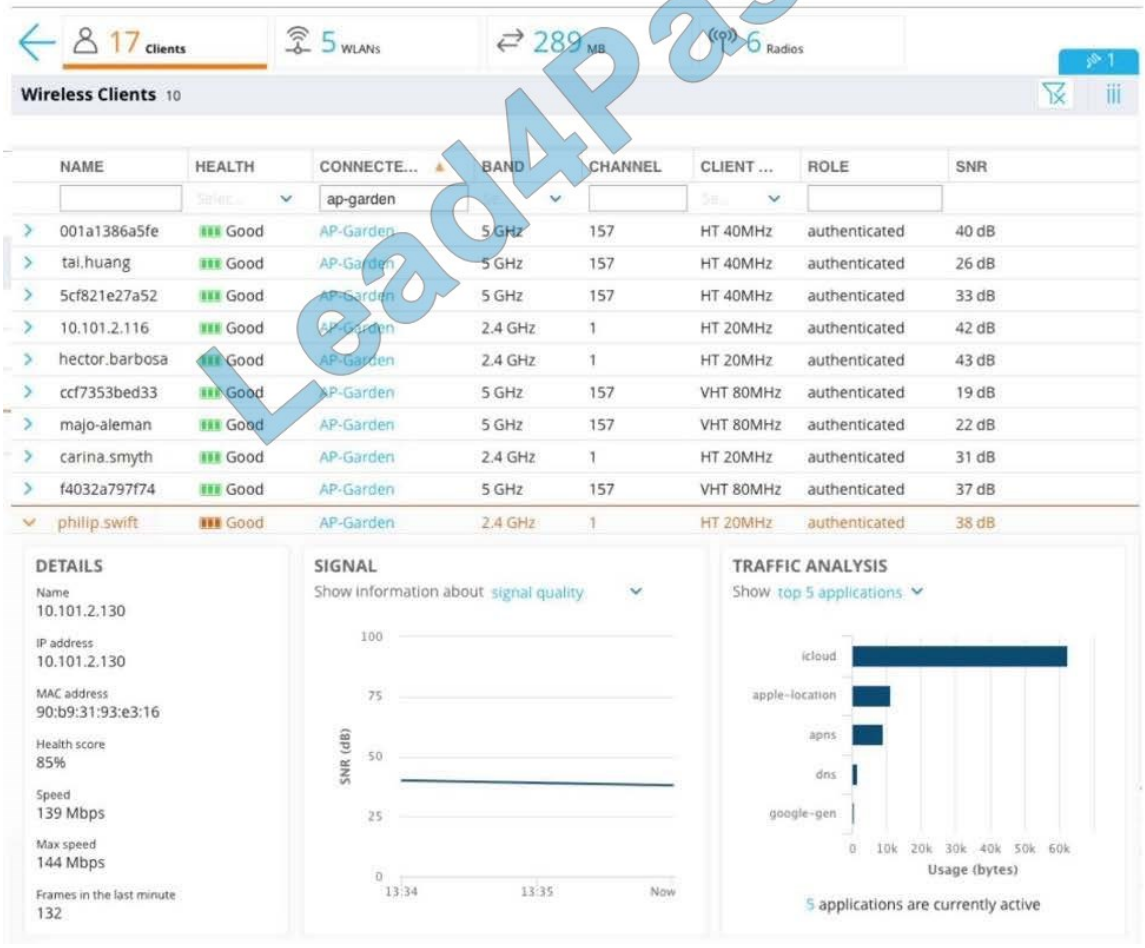
C. The MC assigned the default role based on the authentication method.

D. The MC assigned the role based on server derivation rules.

Correct Answer: C

QUESTION 7

Refer to the exhibits.



A user reports slow connectivity to a network administrator when connecting to AP-Garden and suggests that there might be a problem with the WLAN. The user\\'s device supports 802.11n in the 2.4 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. 2.4Ghz band is currently congested, therefore a NIC upgrade to 802.11ac or higher is recommended so the user can move to 5Ghz.

B. Channel usage is high and though this device has high speed the overall client rate is low on AP-Garden, there could be a few clients monopolizing the airtime on both bands at low speeds.

C. User\\'s SNR value over time is lower than recommended, therefore he should either get closer to the Access Point or increase the transmit power.

D. 365s are low cost outdoor APs recommended for coverage design only. AP-Garden currently has more clients than recommended and is getting congested.

Correct Answer: D

QUESTION 8

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 9

Refer to the exhibit.

```
(MC1) [mynode] #show ap database

AP Database
-----------
Name  Group              AP Type  IP Address    Status           Flags  Switch IP     Standby IP
----  -----              -------  ------------  ------           -----  ------------  ----------
AP1   Main-Campus-SC-B1  355      10.1.145.150  Up 1d:7h:21m:41s 2      10.1.140.100  0.0.0.0
AP2   Main-Campus-SC-B1  355      10.1.146.150  Up 1d:7h:21m:46s 2      10.1.140.100  0.0.0.0

Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- = 802.1x use factory cert; 2 = Using IKE version 2
       B = Built-in AP; C = Cellular RAP; D = Dirty or no config
       E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
       G = no such group; I = Inactive; J = USB cert at AP; L = Unlicensed
       M = Mesh node
       N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth;
       S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
       Y = Mesh Recovery
       c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
       i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z = Datazone AP

Total APs:2
(MC1) [MDC] #
(MC1) [MDC] #show lc-cluster group-membership

Cluster Enabled, Profile Name = "Cluster1"
Redundancy Mode On
Active Client Rebalance Threshold = 50%
Standby Client Rebalance Threshold = 75%
Unbalance Threshold = 5%
AP Load Balancing: Disabled
Cluster Info Table
------------------
Type IPv4 Address     Priority  Connection-Type  STATUS
---- ---------------  --------  ---------------  ------
self    10.1.140.100        10              N/A  ISOLATED (Leader)
peer    10.1.140.101       101              N/A  INCOMPATIBLE (CLUSTER_NAME_MISMATCH)
```

After deploying several cluster pairs, the network administrator notices that all APs assigned to Cluster1 communicate with MC1 instead of being distributed between members of the cluster. Also, no IP addresses are shown under the Standby IP column.

What should the network administrator do to fix this situation?

A. Apply the same cluster profile to both members.

B. Enable Cluster AP load balancing.

C. Rename the cluster profile as "CLUSTER1".

D. Place MCs at the same hierarchical group level.

Correct Answer: C

QUESTION 10

Refer to the exhibits. Exhibit 1

```
(MC11) [mynode] (config) #show station-table

Station Entry
-------------
    MAC                 Name          Role          Age(d:h:m)  Auth  AP name  Essid          Phy  Remote  Profile   User Type
    ---                 ----          ----          ----------  ----  -------  -----          ---  ------  -------   ---------
xx:xx:xx:xx:xx:xx       contractor    contractor    00:00:02    Yes   AP22     EmployeesNet   g-HT No      Employee  WIRELESS

Station Entries: 1
(MC11) [mynode] (config) #show ap client status xx:xx:xx:xx:xx:xx

STA Table
---------
bssid             auth  assoc  aid  l-int  essid          vlan-id  tunnel-id
-----             ----  -----  ---  -----  -----          -------  ---------
xx:xx:xx:xx:xx:xx  y     y      1    1      EmployeesNet   40       0x1000d
State Hash Table
----------------
bssid             state       reason
-----             -----       ------
xx:xx:xx:xx:xx:xx  auth-assoc  0
```

Exhibit 2

```
(MC11) [mynode] (config) #show log network 10

Jun 23 23:37:18 :202541:  <5669> <DBUG> |dhcpwrap| |dhcp| Received DHCP packet from Datapath, Flags 0x100040, 0pcode 0x5a, Vlan 40, Ingress tunnel 13,
Egress vlan 40, SMAC xx:xx:xx:xx:xx:xx
Jun 23 23:37:18 :202534:  <5669> <DBUG> |dhcpwrap| |dhcp| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d:05493d7f10
4vr5 0c:226962794c6573736234 3c:8h53464120952e30 94:0157940e1e2k2g2r2e2e45e5ev
Jun 23 23:37:18 :202523:  <5669> <DBUG> |dhcpwrap| |dhcp| dhcpreplay: mac=xx:xx:xx:xx:xx:xx dev=eth1 length=300, from_port=68, op=1, giaddr=0.0.0.0
Jun 23 23:37:18 :202532:  <5669> <DBUG> |dhcpwrap| |dhcp| got 1 replay servers
Jun 23 23:37:18 :202533:  <5669> <DBUG> |dhcpwrap| |dhcp| Relayed: DISCOVER server=10.254.1.21 giaddr=192.168.40.1 MAC=xx:xx:xx:xx:xx:xx
Jun 23 23:37:18 :202523:  <5669> <DBUG> |dhcpwrap| |dhcp| dhcpreplay: mac=xx:xx:xx:xx:xx:xx dev=eth1 length=300, from_port=67, op=1, giaddr=192.168.4
0.1
Jun 23 23:37:18 :202085:  <5669> <DBUG> |dhcpwrap| |dhcp| DHCPDISCOVER from xx:xx:xx:xx:xx:xx via eth1: unknown network segment
Jun 23 23:37:18 :202085:  <5669> <DBUG> |dhcpwrap| |dhcp| DHCPDISCOVER from xx:xx:xx:xx:xx:xx 192.168.40.1: unknown network segment
Jun 23 23:37:18 :202541:  <5669> <DBUG> |dhcpwrap| |dhcp| Received DHCP packet from Datapath, Flags 0x42, 0pcode 0x5a, Vlan 1, Ingress local, Egress 0/0/0,
SMAC yy:yy:yy:yy:yy:yy
Jun 23 23:37:18 :202534:  <5669> <DBUG> |dhcpwrap| |dhcp| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d:05493d7f10
4vr5 0c:226962794c6573736234 3c:8h53464120952e30 94:0157940e1e2k2g2r2e2e45e5ev
```

Exhibit 3

```
(MC11) #show ip interface brief

Interface                IP Address / IP Netmask     Admin  Protocol  VRRP-IP
vlan1                    10.1.140.100 / 255.255.255.0  up     up
vlan 40                  192.168.40.1 / 255.255.255.0  up     up
loopback                 unassigned / unassigned       up     up
(MC11) #
(MC11) #show packet-capture controlpath-pcap

23:37:13.562680 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:13.562887 IP 192.168.40.1.67 > 10.254.1.21.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:18.495551 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:18.495998 IP 192.168.40.1.67 > 10.254.1.21.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:22.987755 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:22.987894 IP 192.168.40.1.67 > 10.254.1.21.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
```

A network administrator wants to allow contractors to access the corporate WLAN named EmployeesNet with the contractor role in VLAN 40. When users connect, they do not seem to get an IP address. After some verification checks, the network administrator confirms the DHCP server (10.254.1.21) is reachable from the Mobility Controller (MC) and obtains the outputs shown in the exhibits.

What should the network administrator do next to troubleshoot this problem?

A. Permit UDP67 to the contractor role.

B. Remove the IP address in VLAN 40.

C. Configure the DHCP helper address.

D. Confirm there is an IP pool for VLAN 40.

Correct Answer: A

QUESTION 11

Refer to the exhibit.

```
(MC14-1) #show aaa authentication dot1x Corp-Network

802.1X Authentication Profile "Corp-Network"
-------------------------------------------
Parameter                                          Value
---------                                          -----
Max authentication failures                        0
Enforce Machine Authentication                     Enabled
Machine Authentication: Default Machine Role       guest
Machine Authentication Cache Timeout               24 hr(s)
Blacklist on Machine Authentication Failure        Disabled
Machine Authentication: Default User Role          guest
Interval between Identity Requests                 5 sec
Quiet Period after Failed Authentication           30 sec
Reauthentication Interval                          86400 sec
Use Server provided Reauthentication Interval      Disabled
Use the termination-action attribute from the Server  Disabled
Multicast Key Rotation Time Interval               1800 sec
Unicast Key Rotation Time Interval                 900 sec
Authentication Server Retry Interval               5 sec
Authentication Server Retry Count                  3
Framed MTU                                         1100 bytes
Max number of requests sent during an Auth attempt 5
Max Number of Reauthentication Attempts            3
Maximum number of times Held State can be bypassed 0
Dynamic WEP Key Message Retry Count                1
Dynamic WEP Key Size                               128 bits
Interval between WPA/WPA2 Key Messages             1000 msec
Delay between EAP-Success and WPA2 Unicast Key Exchange  0 msec
Delay between WPA/WPA2 Unicast Key and Group Key Exchange 0 msec
Time interval after which the PMKSA will be deleted  8 hr(s)
Delete Keycache upon user deletion                 Disabled
WPA/WPA2 Key Messages Retry Count                  3
Multicast Key Rotation                             Disabled
Unicast Key Rotation                               Disabled
Reauthentication                                   Disabled
Opportunistic Key Caching                          Enabled
```

The network administrator must ensure that the configuration will force users to authenticate periodically every eight hours. Which configuration is required to effect this change?

A. Set the reauth-period to 28800 enable reauthentication in the dot1x profile.

B. Set the reauth-period to 28800 enable reauthentication in the AAA profile.

C. Set the reauth-period to 28800 enable reauthentication in both dot1x and AAA profile.

D. Set the reauth-period to 28800 in the dot1x profile and enable reauthentication in the AAA profile.

Correct Answer: A

QUESTION 12

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 13

A customer wants a WLAN solution that permits Aps to terminate WPA-2 encrypted traffic from different SSIDs to different geographic locations where non-related IT departments will take care of enforcing security policies. A key requirement is to minimize network congestion, overhead, and delay while providing data privacy from the client to the security policy enforcement point. Therefore, the solution must use the shortest path from source to destination.

Which Aruba feature best accommodates this scenario?

A. Inter MC S2S IPsec tunnels

B. RAPs

C. Multizone Aps

D. VIA

E. Inter MC GRE tunnels

Correct Answer: B