Free Questions for HPE6-A79 by vceexamstest

Shared by Maynard on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company with 50 small coffee shops in a single country requires a single mobility solution that solves connectivity needs at both the main office and branch locations. Coffee shops must be provisioned with local WiFi internet access for customers.

The shops must also have a private WLAN that offers communication to resources at the main office to upload sales, request supplies through a computer system, and make phone calls if needed. In order to simplify network operations, network devices at the coffee shops should be cloud managed.

Which technologies best meet the company needs at the lowest cost?

Options:

A- IAPVPN

B- SD-Branch

C- Activate with RAPs

D- BOC with CAPs

Answer:

B

Question 2

Question Type: MultipleChoice

An Aruba Mobility Master (MM) - Mobility Controller (MC) solution is connected to a wired network that is ready to prioritize DSCP marked traffic. A group of WMM-enabled clients sends traffic marked at L2 only.

What must the network administrator do to map those markings to DSCP equivalent values when traffic is received by the APs?

Options:

A- Enable WMM in the SSID profile.

B- Enable WMM in the VAP profile.

C- Enable Skype4Business ALG Support.

D- Enable traffic to be marked with session ACLs.

Answer:

B

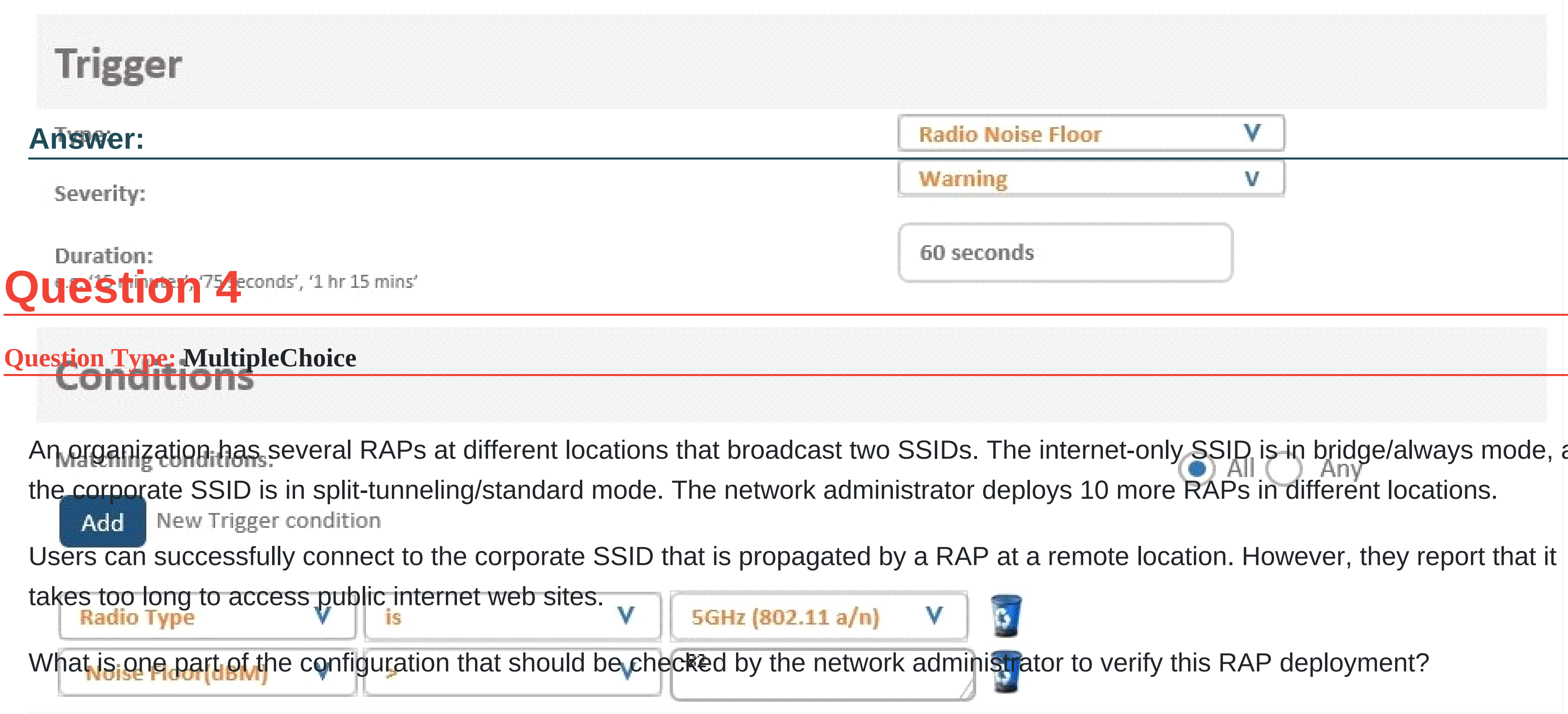
Question 3

Question Type: Hotspot

A network administrator wants to receive a warning level alarm every time the noise floor rises above -82 dBm on any of the AP radios.

Which alarm definition must the network administrator create to accomplish this?

Answer:



Trigger

Type: Radio Noise Floor

Severity: Warning

Duration: 60 seconds
e.g. '15 minutes', '75 seconds', '1 hr 15 mins'

Conditions

Matching conditions: ● All ○ Any

Radio Type	is	5GHz (802.11 a/n)
Noise Floor(dBM)	>	-82

Question 4

Question Type: MultipleChoice

An organization has several RAPs at different locations that broadcast two SSIDs. The internet-only SSID is in bridge/always mode, and the corporate SSID is in split-tunneling/standard mode. The network administrator deploys 10 more RAPs in different locations.

Users can successfully connect to the corporate SSID that is propagated by a RAP at a remote location. However, they report that it takes too long to access public internet web sites.

What is one part of the configuration that should be checked by the network administrator to verify this RAP deployment?

Options:

A- User roles policies

B- IP pool

C- Operating mode

D- Assigned VLAN

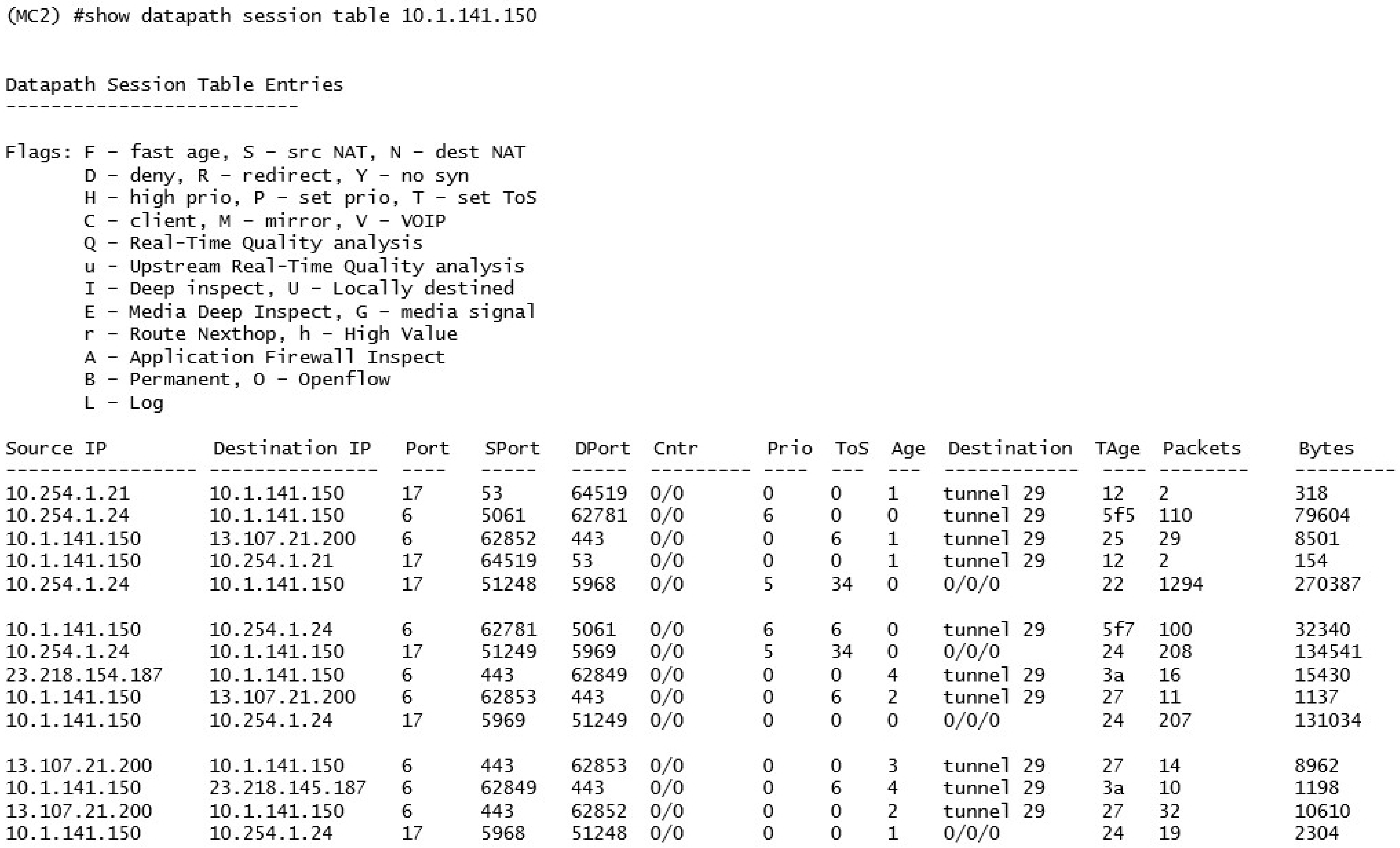
Answer:

A

Question 5

Question Type: **MultipleChoice**

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
----------------- ---------------  ----   -----   -----  --------- ----  ---  ---  -----------  ----  --------    ---------
10.254.1.21       10.1.141.150     17     53      64519  0/0       0     0    1    tunnel 29    12    2           318
10.254.1.24       10.1.141.150     6      5061    62781  0/0       6     0    0    tunnel 29    5f5   110         79604
10.1.141.150      13.107.21.200    6      62852   443    0/0       0     6    1    tunnel 29    25    29          8501
10.1.141.150      10.254.1.21      17     64519   53     0/0       0     0    1    tunnel 29    12    2           154
10.254.1.24       10.1.141.150     17     51248   5968   0/0       5     34   0    0/0/0        22    1294        270387

10.1.141.150      10.254.1.24      6      62781   5061   0/0       6     6    0    tunnel 29    5f7   100         32340
10.254.1.24       10.1.141.150     17     51249   5969   0/0       5     34   0    0/0/0        24    208         134541
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
10.1.141.150      10.254.1.24      17     5969    51249  0/0       0     0    0    0/0/0        24    207         131034

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
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
```

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?

Options:

A- UCC based DSCP correction

B- WMM support on the WLAN

C- Dynamic Multicast Rate Optimization

D- wired network congestion

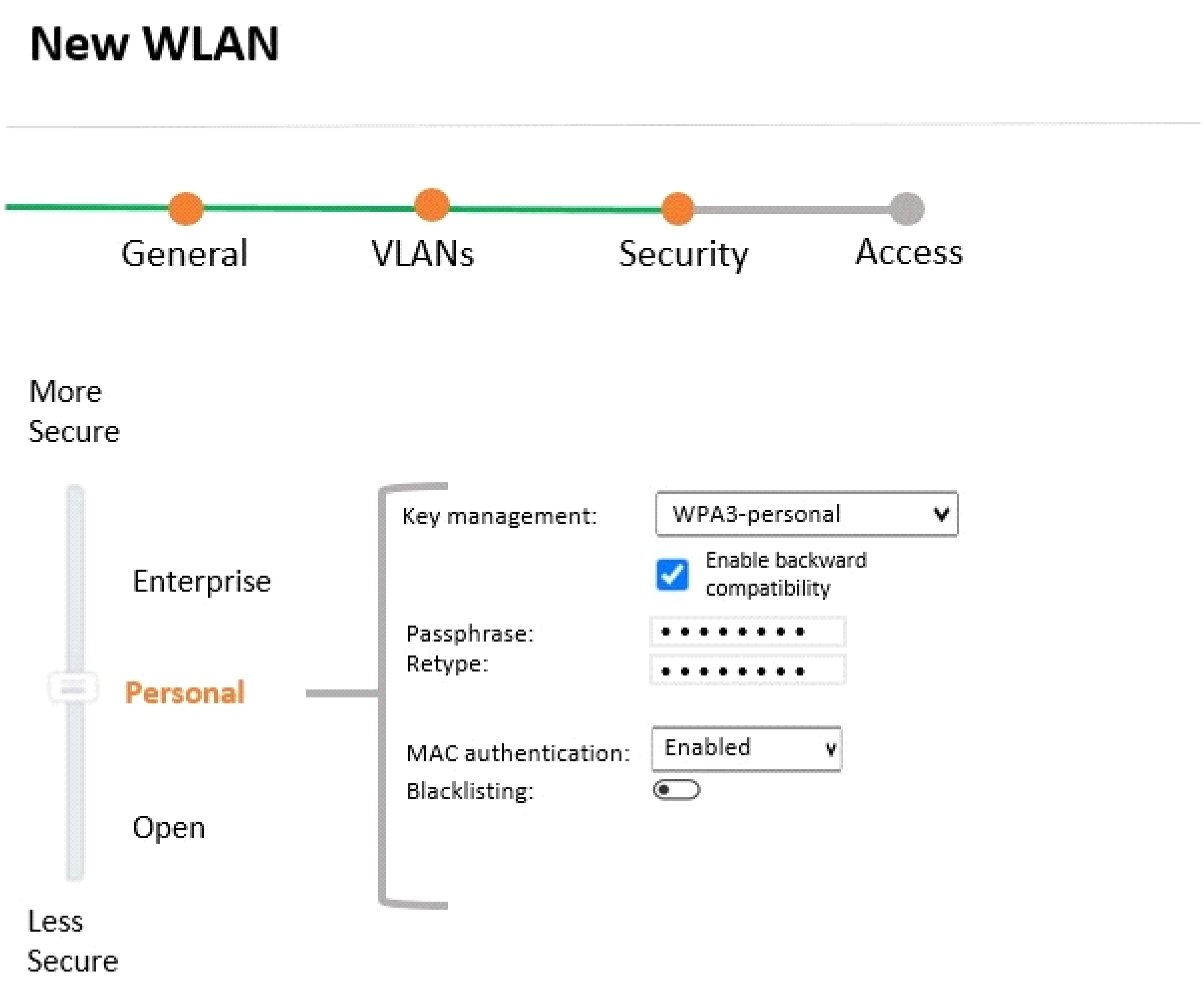
Answer:

D

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit:



New WLAN

Key management: WPA3-personal

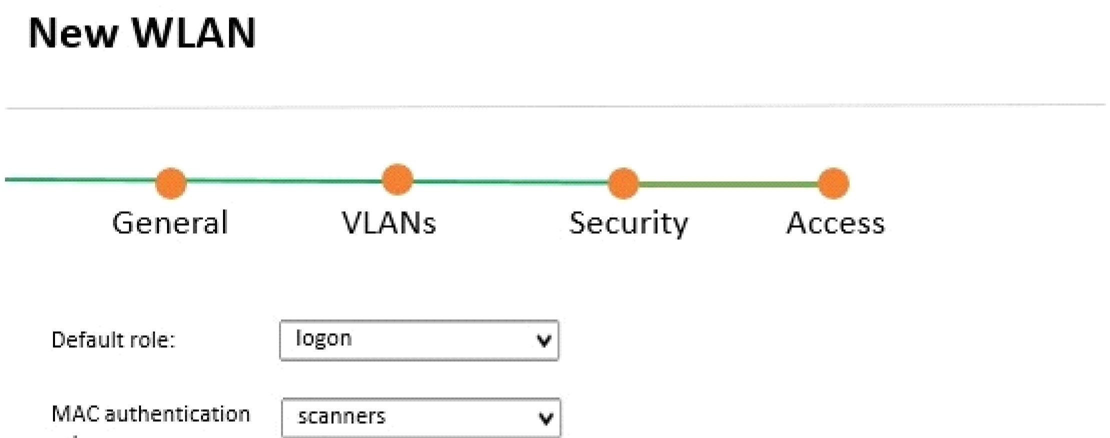
☑ Enable backward compatibility

Passphrase: •••••••••

Retype: •••••••••

MAC authentication: Enabled

Blacklisting: ○



New WLAN

Default role: logon

MAC authentication: scanners

A company acquires ten barcode scanners to run inventory tasks. These WiFi devices support WPA2-PSK security only. The network administrator deploys a WLAN named scanners using the configuration shown in the exhibit.

What must the network administrator do next to ensure that the scanner devices successfully connect to their SSID?

Options:

A- Set internal as the MAC authentication server group.

B- Add scanner MAC addresses in user derivation rules.

C- Enable L2 Authentication Fail Through.

D- Add scanner MAC addresses in the internal database.

Answer:

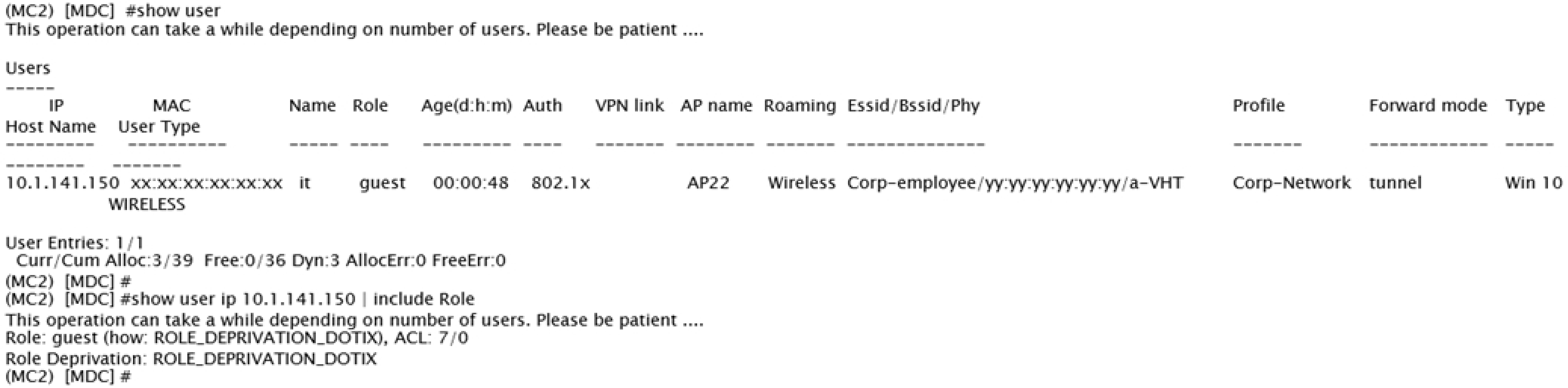
D

Question 7

Question Type: MultipleChoice

Refer to the exhibits.

Exhibit 1

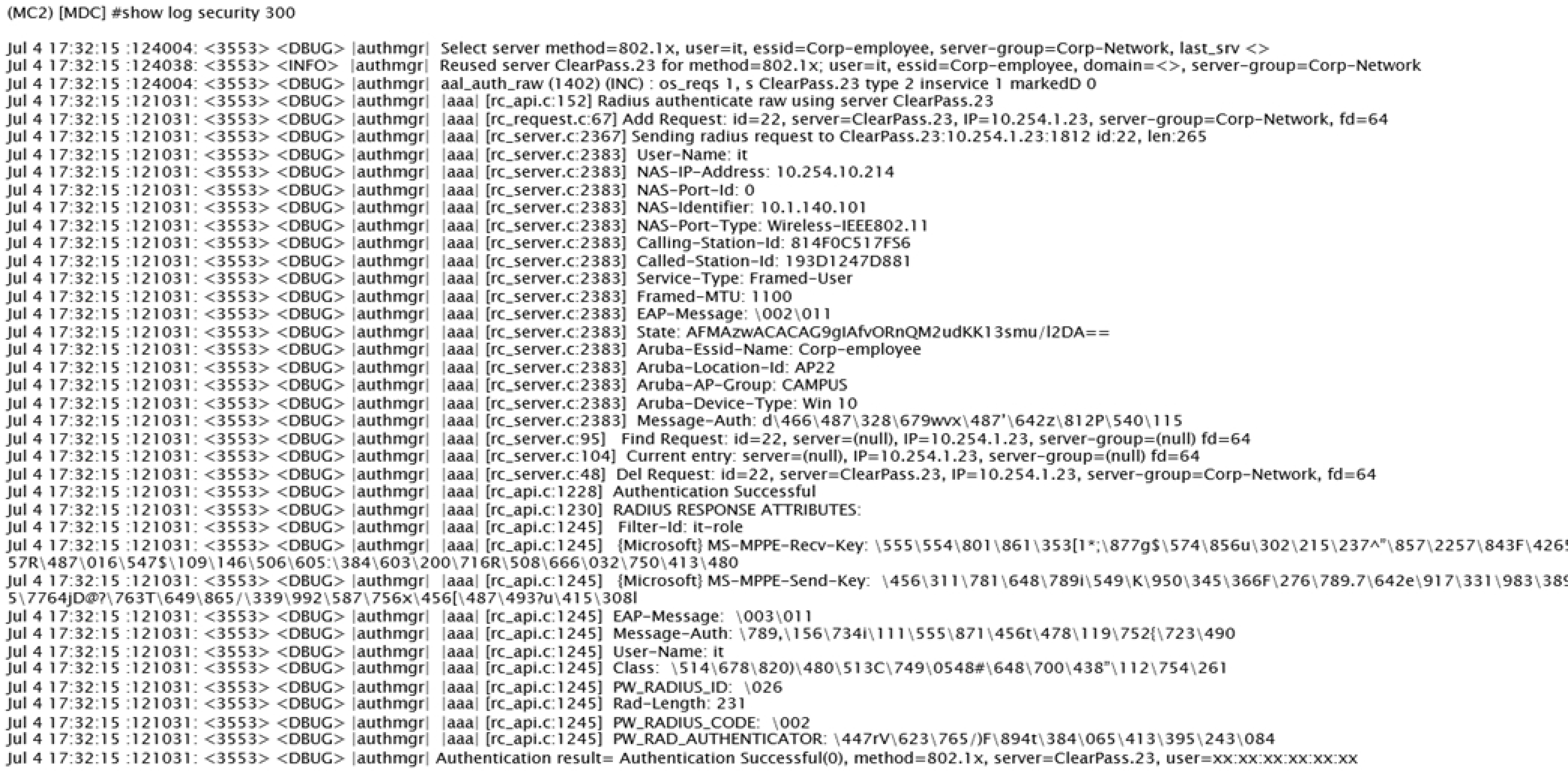


```
(MC2)  [MDC]  #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
      IP            MAC               Name   Role      Age(d:h:m)  Auth      VPN link   AP name  Roaming  Essid/Bssid/Phy                                  Profile           Forward mode   Type
Host Name    User Type
----------     -----------         -----  ----      ----------  ----      --------  --------  --------  ---------------                                  --------          -------------  -----
---------     --------
10.1.141.150  xx:xx:xx:xx:xx:xx   it        guest     00:00:48    802.1x              AP22      Wireless  Corp-employee/yy:yy:yy:yy:yy:yy/a-VHT          Corp-Network   tunnel          Win 10
              WIRELESS

User Entries: 1/1
  Curr/Cum Alloc:3/39  Free:0/36 Dyn:3 AllocErr:0 FreeErr:0
(MC2)  [MDC] #
(MC2)  [MDC] #show user ip 10.1.141.150 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: guest (how: ROLE_DEPRIVATION_DOTIX), ACL: 7/0
Role Deprivation: ROLE_DEPRIVATION_DOTIX
(MC2)  [MDC] #
```

Exhibit 2



```
(MC2) [MDC] #show log security 300

Jul 4 17:32:15 :124004: <3553> <DBUG> |authmgr|  Select server method=802.1x, user=it, essid=Corp-employee, server-group=Corp-Network, last_srv <>
Jul 4 17:32:15 :124038: <3553> <INFO>  |authmgr|  Reused server ClearPass.23 for method=802.1x; user=it, essid=Corp-employee, domain=<>, server-group=Corp-Network
Jul 4 17:32:15 :124004: <3553> <DBUG> |authmgr|  aal_auth_raw (1402) (INC) : os_reqs 1, s ClearPass.23 type 2 inservice 1 markedD 0
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:152] Radius authenticate raw using server ClearPass.23
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_request.c:67] Add Request: id=22, server=ClearPass.23, IP=10.254.1.23, server-group=Corp-Network, fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2367] Sending radius request to ClearPass.23:10.254.1.23:1812 id:22, len:265
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  User-Name: it
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  NAS-IP-Address: 10.254.10.214
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  NAS-Port-Id: 0
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  NAS-Identifier: 10.1.140.101
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  NAS-Port-Type: Wireless-IEEE802.11
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  Calling-Station-Id: 814F0C517FS6
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  Called-Station-Id: 193D1247D881
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  Service-Type: Framed-User
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  Framed-MTU: 1100
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  EAP-Message: \002\011
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  State: AFMAzwACACAG9gIAfvORnQM2udKK13smu/l2DA==
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  Aruba-Essid-Name: Corp-employee
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  Aruba-Location-Id: AP22
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  Aruba-AP-Group: CAMPUS
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  Aruba-Device-Type: Win 10
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:2383]  Message-Auth: d\466\487\328\679wvx\487'\642z\812P\540\115
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:95]   Find Request: id=22, server=(null), IP=10.254.1.23, server-group=(null) fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:104]  Current entry: server=(null), IP=10.254.1.23, server-group=(null) fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_server.c:48]  Del Request: id=22, server=ClearPass.23, IP=10.254.1.23, server-group=Corp-Network, fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1228]  Authentication Successful
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1230]  RADIUS RESPONSE ATTRIBUTES:
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]   Filter-Id: it-role
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]   {Microsoft} MS-MPPE-Recv-Key: \555\554\801\861\353[1*;\877g$\574\856u\302\215\237^"\857\2257\843F\4265
57R\487\016\547$\109\146\506\605:\384\603\200\716R\508\666\032\750\413\480
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]   {Microsoft} MS-MPPE-Send-Key:  \456\311\781\648\789i\549\K\950\345\366F\276\789.7\642e\917\331\983\389
5\7764jD@?\763T\649\865/\339\992\587\756x\456[\487\493?u\415\308l
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]  EAP-Message:  \003\011
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]  Message-Auth: \789,\156\734i\111\555\871\456t\478\119\752{\723\490
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]  User-Name: it
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]  Class:  \514\678\820)\480\513C\749\0548#\648\700\438"\112\754\261
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]  PW_RADIUS_ID:  \026
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]  Rad-Length: 231
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]  PW_RADIUS_CODE:  \002
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr|  |aaa| [rc_api.c:1245]  PW_RAD_AUTHENTICATOR: \447rV\623\765/)F\894t\384\065\413\395\243\084
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| Authentication result= Authentication Successful(0), method=802.1x, server=ClearPass.23, user=xx:xx:xx:xx:xx:xx
```

A network administrator integrates a current Mobility Master (MM) - Mobility Controller (MC) deployment with a RADIUS server to authenticate a wireless user, the network administrator realizes that the client machine is not failing into the it_department role, as shown the exhibits.

Which configuration is required to map the users into the proper role, based on standard attributes returned by the RADIUS server in the Access Accept message?

Options:

A- aaa server-group Corp-Network
set role condition Filter-Id equals it-role set-value it_department

B- aaa server-group Corp-employee
set role condition Filter-Id value-of

C- aaa server-group Corp-employee
set role condition Filter-Id equals it-role set-value it_department

D- aaa server-group ClearPass
set role condition Filter-Id equals it_department set-value it-role

E- aaa server-group Corp-Network
set role condition Filter-Id equals it_department set-value it-role

Answer:

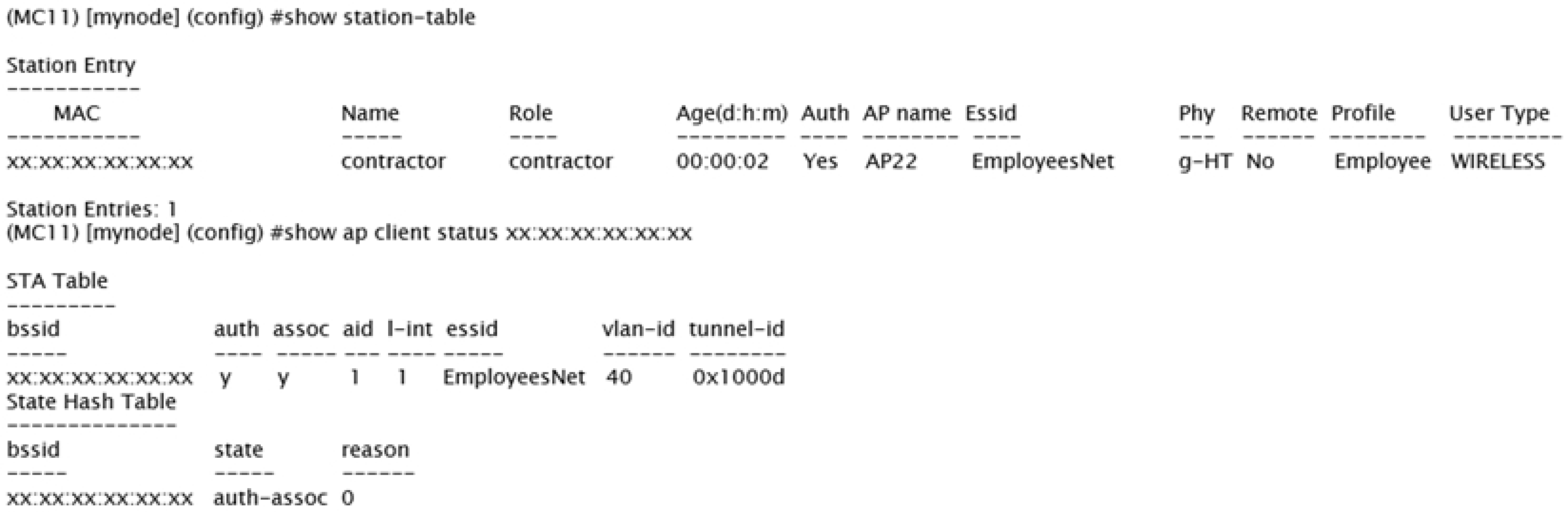
C

Question 8

Question Type: MultipleChoice

Refer to the exhibits.

Exhibit 1



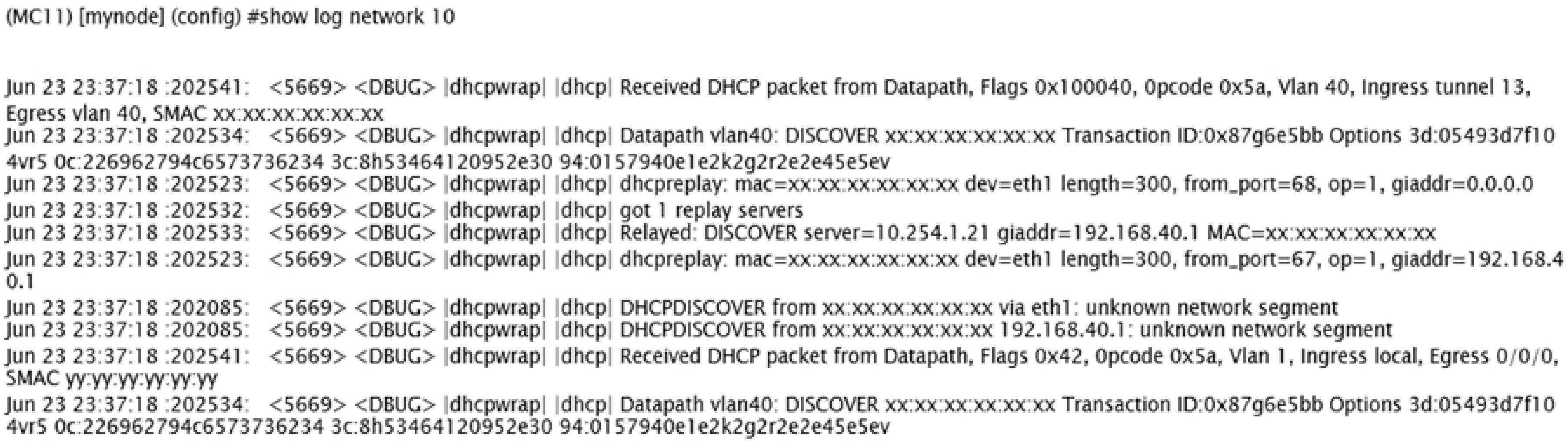
```
(MC11) [mynode] (config) #show station-table

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
```

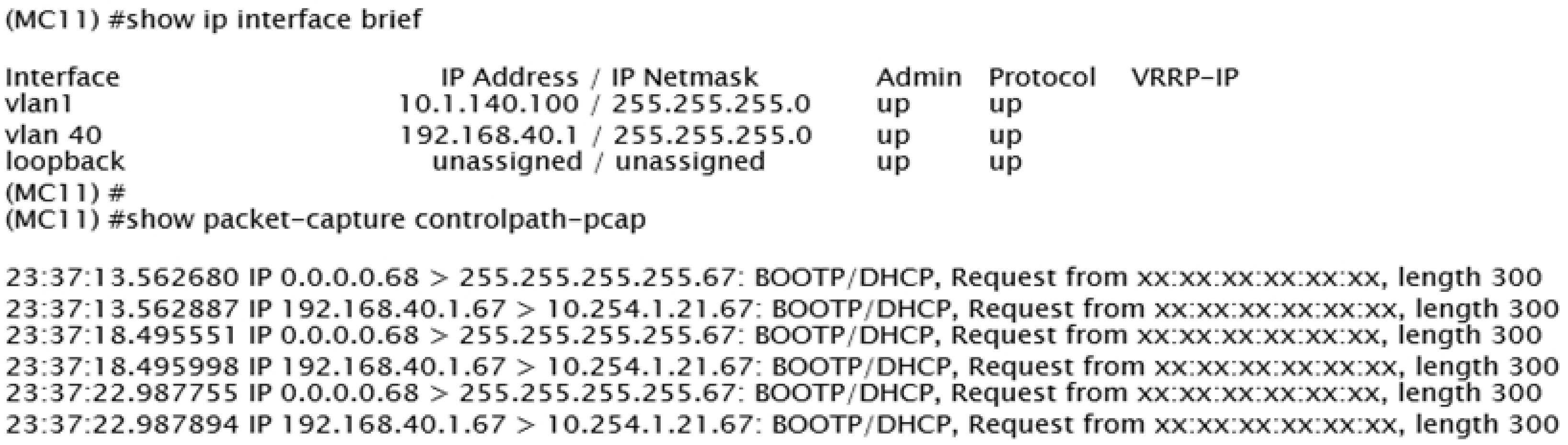
Exhibit 2



```
(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?

Options:

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.

Answer:

A

Question 9

Question Type: **MultipleChoice**

A company plans to build a resort that includes a hotel with 1610 rooms, a casino, and a convention center. The company is interested in a mobility solution that provides scalability and a service-based approach, where they can rent the WLAN infrastructure at the convention center to any customer (tenant) that hosts events at the resort.

The solution should provide:

* Seamless roaming when users move from the hotel to the casino or the convention center

* Simultaneous propagation of the resort and customer-owned SSIDs at the convention center

* Null management access upon resort network infrastructure to the customers (tenants)

* Configuration and monitor rights of rented SSIDs to the customers (tenants)

Which deployment meets the requirements?

Options:

A- Deploy an MM-MC infrastructure with multizone AP's, with one zone for tenant SSIDs.

B- Deploy IAPs along with AirWave. and deploy role-based management access control.

C- Deploy IAPs with zone based SSIDs and manage them with different central accounts.

D- Deploy an MM-MC infrastructure, and create different hierarchy groups for MCs and APs

E- Deploy IAPs. and manage them with different central accounts.

Answer:

E

20%
DISCOUNT