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:

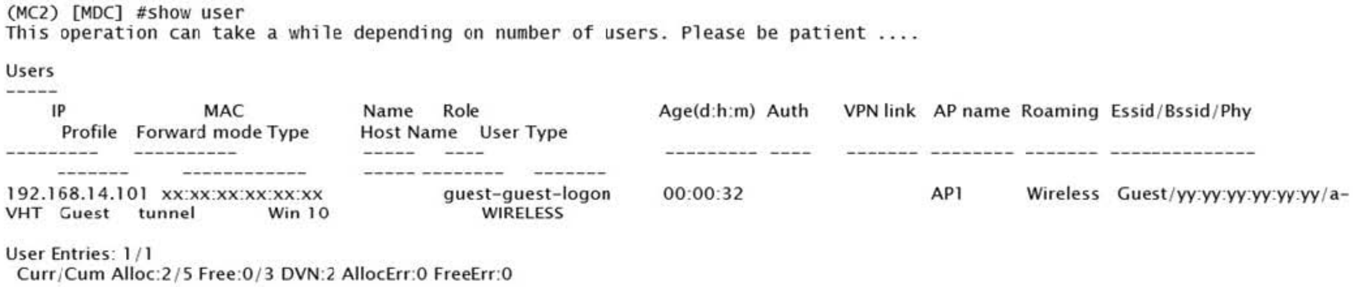
https://www.passapply.com/hpe6-a79.html

100% Passing Guarantee
100% Money Back Assurance

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

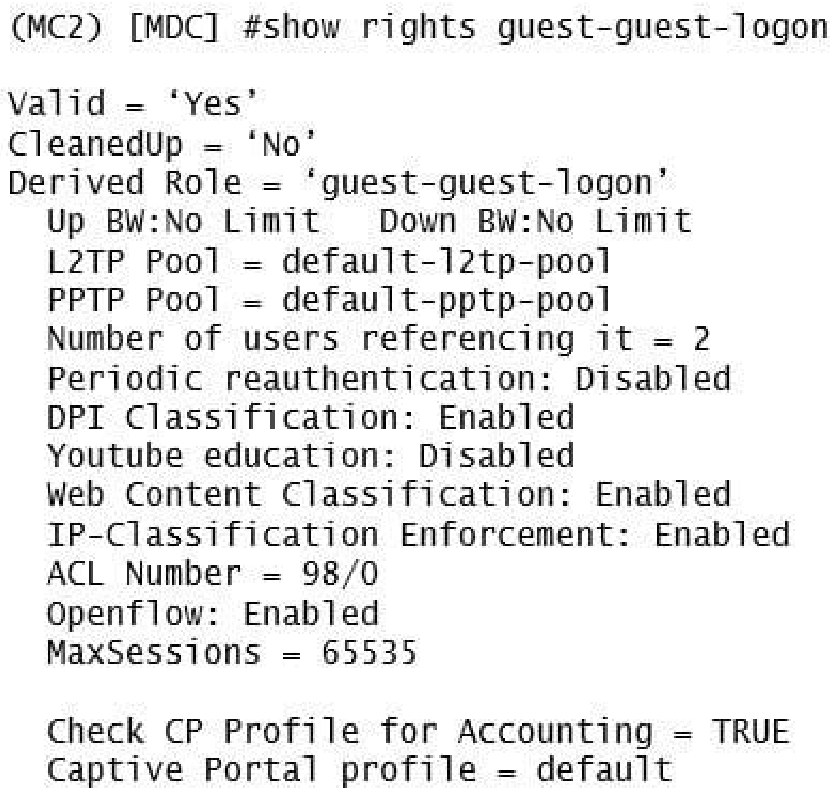
QUESTION 1

Refer to the exhibits. Exhibit 1

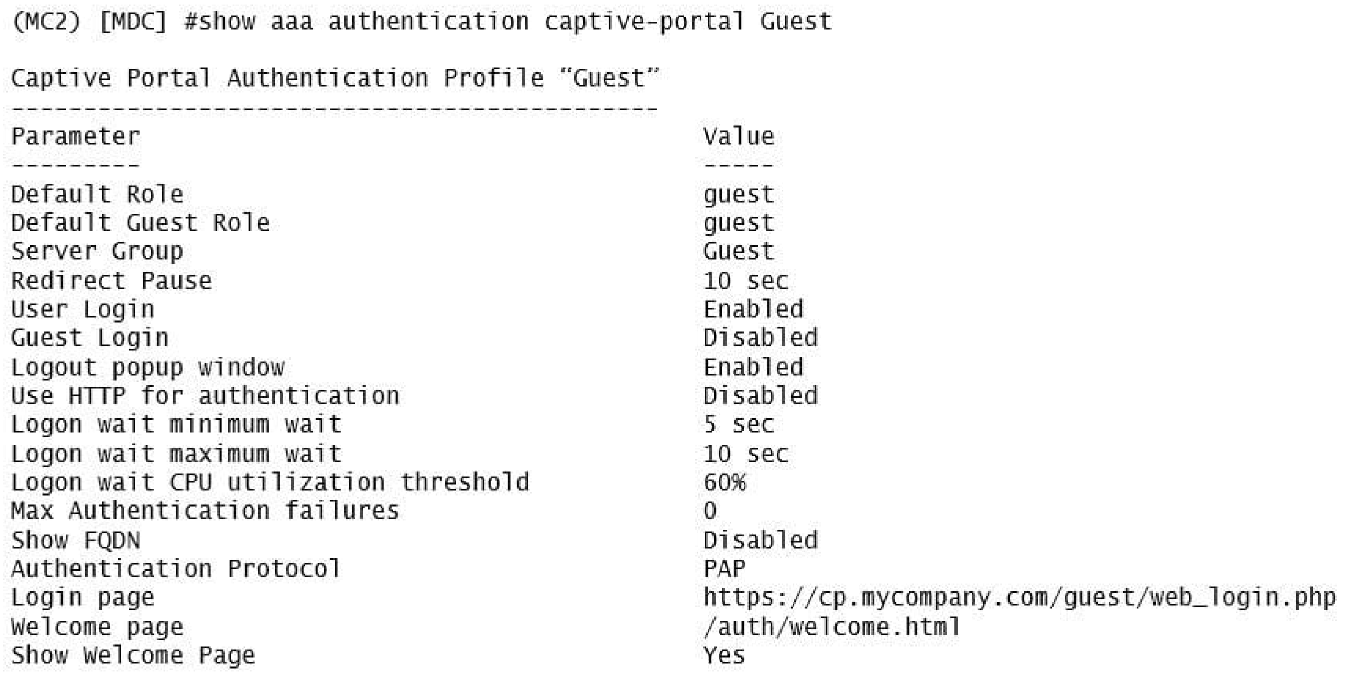


```
(MC2) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

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
---------     ----------              -----     ----                  ---------  ----     -------  --------  -------  -------------
      -------       ------------      ----- --------    --------
192.168.14.101  xx:xx:xx:xx:xx:xx              guest-guest-logon      00:00:32                      AP1       Wireless  Guest/yy:yy:yy:yy:yy:yy/a-
VHT   Guest     tunnel         Win 10              WIRELESS

User Entries: 1/1
  Curr/Cum Alloc:2/5 Free:0/3 DVN:2 AllocErr:0 FreeErr:0
```

Exhibit 2 Exhibit 3

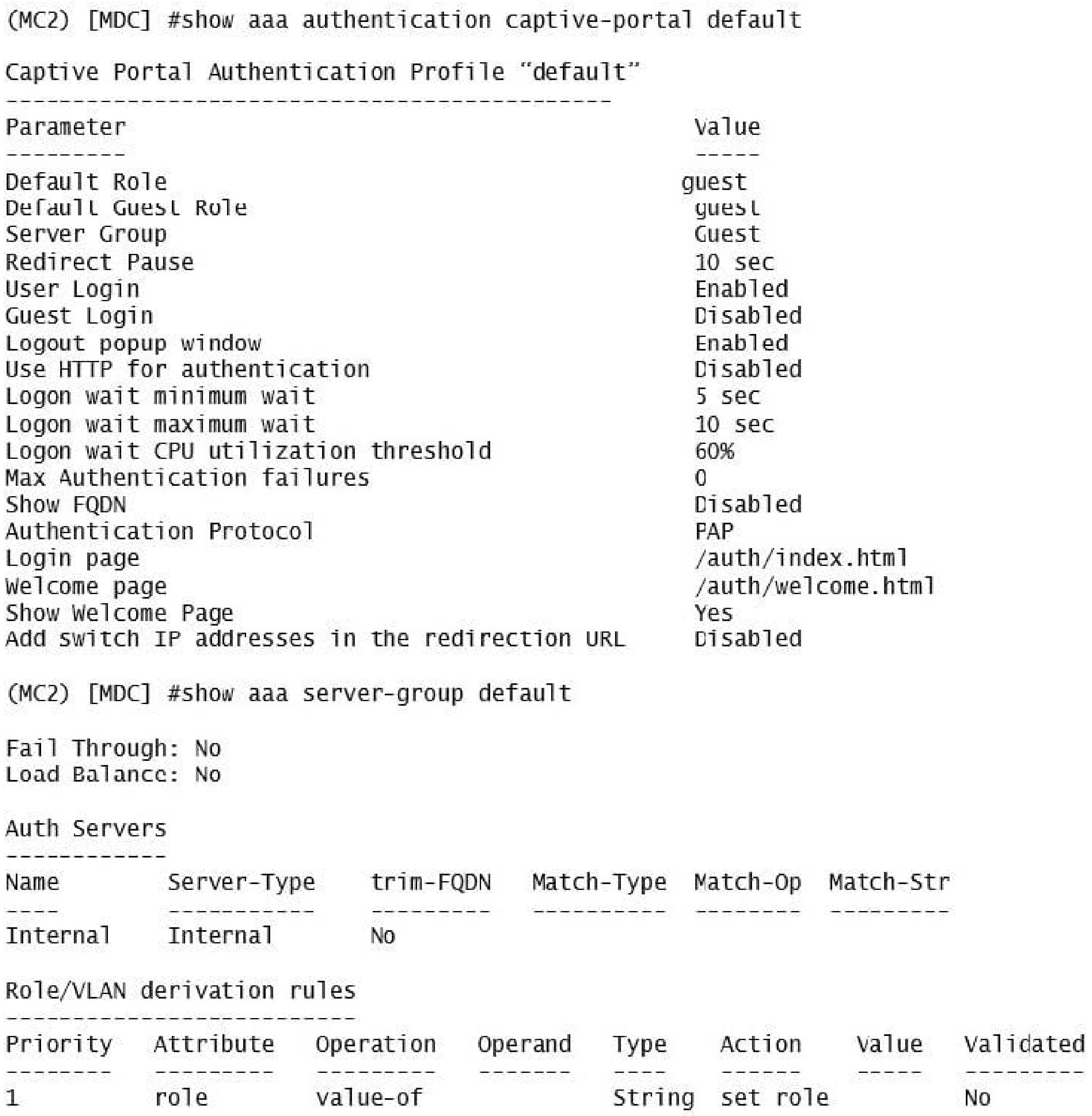


```
(MC2) [MDC] #show rights guest-guest-logon

Valid = 'Yes'
CleanedUp = 'No'
Derived Role = 'guest-guest-logon'
  Up BW:No Limit   Down BW:No Limit
  L2TP Pool = default-l2tp-pool
  PPTP Pool = default-pptp-pool
  Number of users referencing it = 2
  Periodic reauthentication: Disabled
  DPI Classification: Enabled
  Youtube education: Disabled
  Web Content Classification: Enabled
  IP-Classification Enforcement: Enabled
  ACL Number = 98/0
  Openflow: Enabled
  MaxSessions = 65535

  Check CP Profile for Accounting = TRUE
  Captive Portal profile = default
```



```
(MC2) [MDC] #show aaa authentication captive-portal Guest

Captive Portal Authentication Profile “Guest”
---------------------------------------------
Parameter                                       Value
---------                                       -----
Default Role                                    guest
Default Guest Role                              guest
Server Group                                    Guest
Redirect Pause                                  10 sec
User Login                                      Enabled
Guest Login                                     Disabled
Logout popup window                             Enabled
Use HTTP for authentication                     Disabled
Logon wait minimum wait                         5 sec
Logon wait maximum wait                         10 sec
Logon wait CPU utilization threshold            60%
Max Authentication failures                     0
Show FQDN                                       Disabled
Authentication Protocol                         PAP
Login page                                      https://cp.mycompany.com/guest/web_login.php
Welcome page                                    /auth/welcome.html
Show Welcome Page                               Yes
```

Exhibit 4



```
(MC2) [MDC] #show aaa authentication captive-portal default

Captive Portal Authentication Profile "default"
---------------------------------------------
Parameter                                            Value
---------                                            -----
Default Role                                        guest
Default Guest Role                                   guest
Server Group                                         Guest
Redirect Pause                                       10 sec
User Login                                           Enabled
Guest Login                                          Disabled
Logout popup window                                  Enabled
Use HTTP for authentication                          Disabled
Logon wait minimum wait                              5 sec
Logon wait maximum wait                              10 sec
Logon wait CPU utilization threshold                 60%
Max Authentication failures                          0
Show FQDN                                            Disabled
Authentication Protocol                              PAP
Login page                                           /auth/index.html
Welcome page                                         /auth/welcome.html
Show Welcome Page                                    Yes
Add switch IP addresses in the redirection URL       Disabled

(MC2) [MDC] #show aaa server-group default

Fail Through: No
Load Balance: No

Auth Servers
------------
Name        Server-Type    trim-FQDN    Match-Type  Match-Op  Match-Str
----        -----------    ---------    ----------  --------  ---------
Internal    Internal       No

Role/VLAN derivation rules
--------------------------
Priority   Attribute    Operation    Operand    Type    Action    Value   Validated
--------   ---------    ---------    -------    ----    ------    -----   ---------
1          role         value-of                String  set role          No
```

A captive portal-based solution is deployed in a Mobility Master (MM) - Mobility Controller (MC) network. A wireless station connects to the network and attempts the authentication process. The outputs are shown in the exhibits. Which names correlate with the authentication and captive portal servers?

A. ClearPass.23 is the authentication server, and cp.mycompany.com is the captive portal server.

B. ClearPass.23 is the authentication server, and MC2 is the captive portal server.

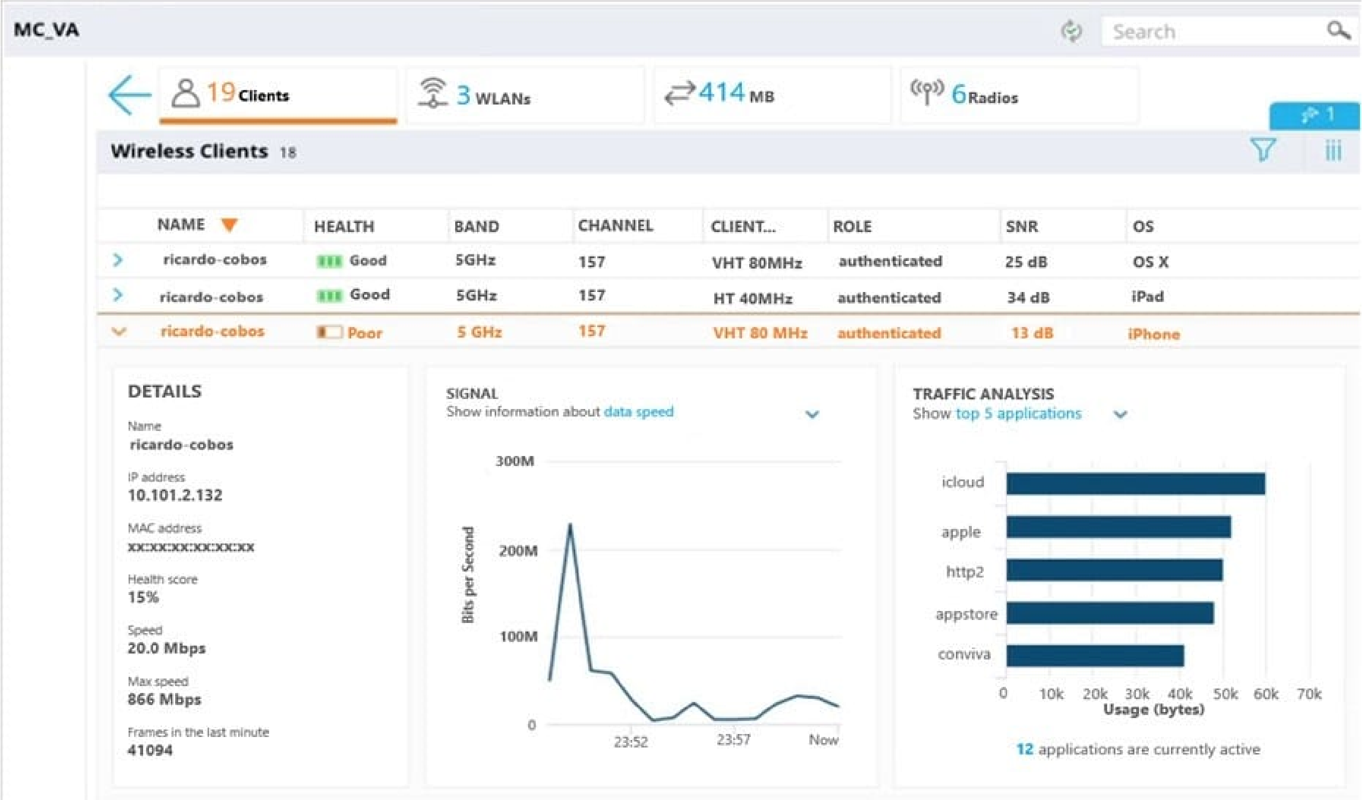
C. Internal database in MC2 is the authentication server, and cp.mycompany.com is the captive portal server.

D. cp.mycompany.com is the authentication server, and ClearPass.23 is the captive portal server.

Correct Answer: A

QUESTION 2

Refer to the exhibits.



MC_VA

Search

19 Clients | 3 WLANs | 414 MB | 6 Radios

Wireless Clients 18

	NAME	HEALTH	BAND	CHANNEL	CLIENT...	ROLE	SNR	OS
>	ricardo-cobos	Good	5GHz	157	VHT 80MHz	authenticated	25 dB	OS X
>	ricardo-cobos	Good	5GHz	157	HT 40MHz	authenticated	34 dB	iPad
⌄	ricardo-cobos	Poor	5 GHz	157	VHT 80 MHz	authenticated	13 dB	iPhone

DETAILS

Name
ricardo-cobos

IP address
10.101.2.132

MAC address
xx:xx:xx:xx:xx:xx

Health score
15%

Speed
20.0 Mbps

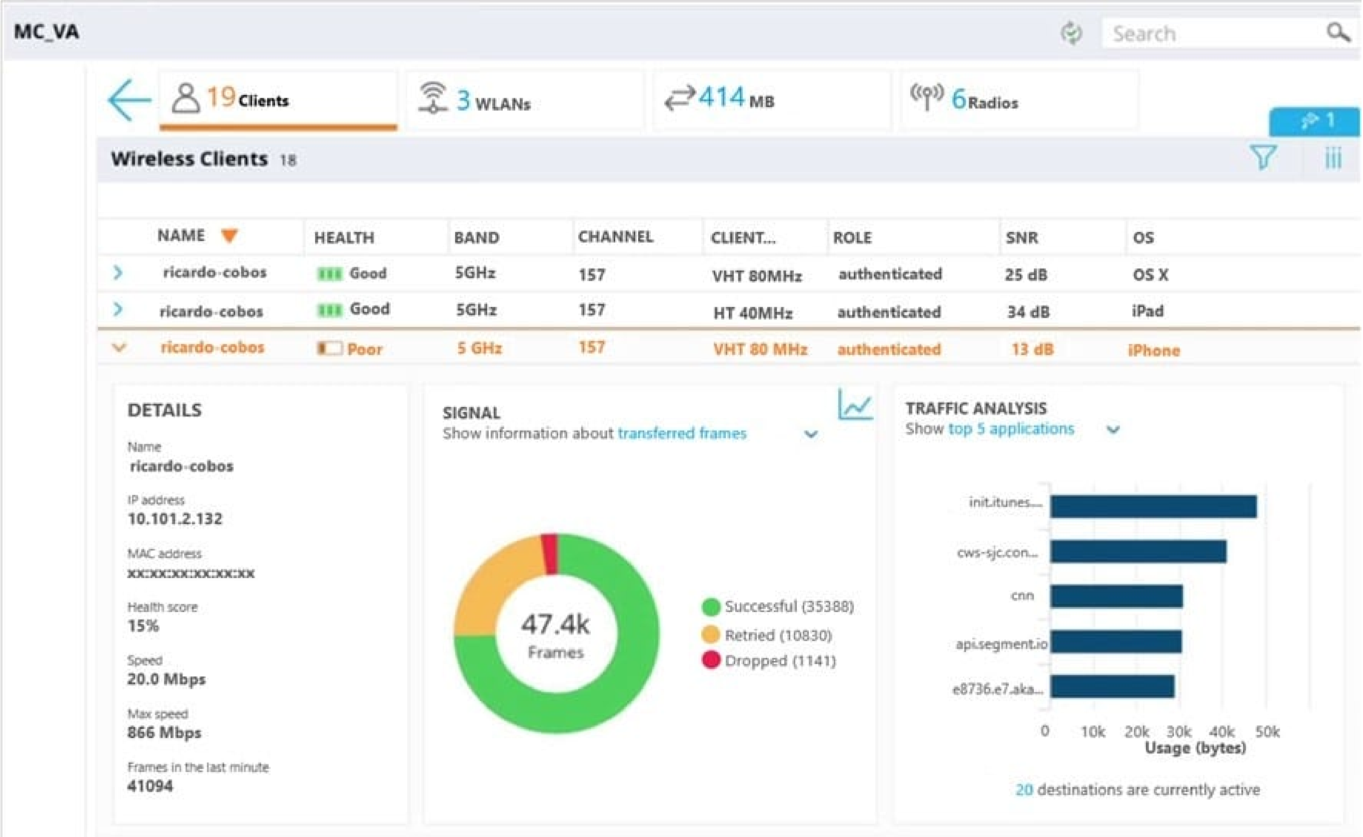
Max speed
866 Mbps

Frames in the last minute
41094

SIGNAL
Show information about data speed

TRAFFIC ANALYSIS
Show top 5 applications

12 applications are currently active



MC_VA

19 Clients | 3 WLANs | 414 MB | 6 Radios

Wireless Clients 18

	NAME	HEALTH	BAND	CHANNEL	CLIENT...	ROLE	SNR	OS
>	ricardo-cobos	Good	5GHz	157	VHT 80MHz	authenticated	25 dB	OS X
>	ricardo-cobos	Good	5GHz	157	HT 40MHz	authenticated	34 dB	iPad
⌄	ricardo-cobos	Poor	5 GHz	157	VHT 80 MHz	authenticated	13 dB	iPhone

DETAILS

Name
ricardo-cobos

IP address
10.101.2.132

MAC address
xx:xx:xx:xx:xx:xx

Health score
15%

Speed
20.0 Mbps

Max speed
866 Mbps

Frames in the last minute
41094

SIGNAL
Show information about transferred frames

TRAFFIC ANALYSIS
Show top 5 applications

20 destinations are currently active

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.

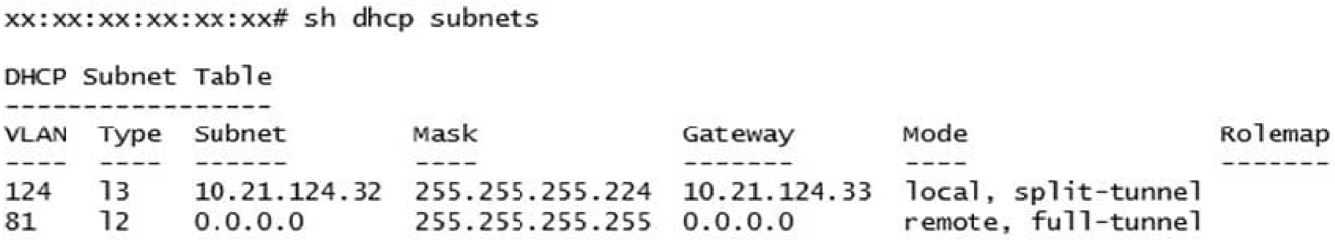
C. Since SNR is good, then the high retransmit rate must be due a hidden node scenario or high interference.

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 3

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

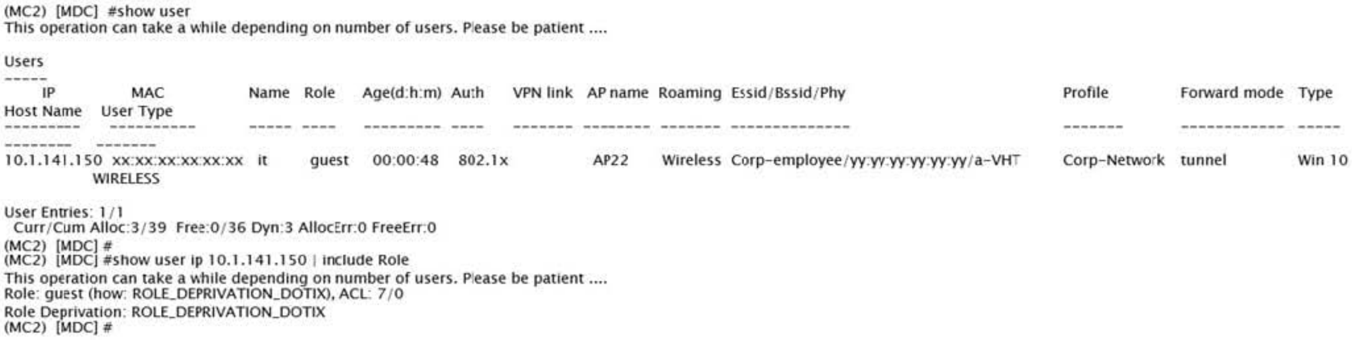
C. local L3 and distributed L2

D. centralized L3 and distributed L2

Correct Answer: D

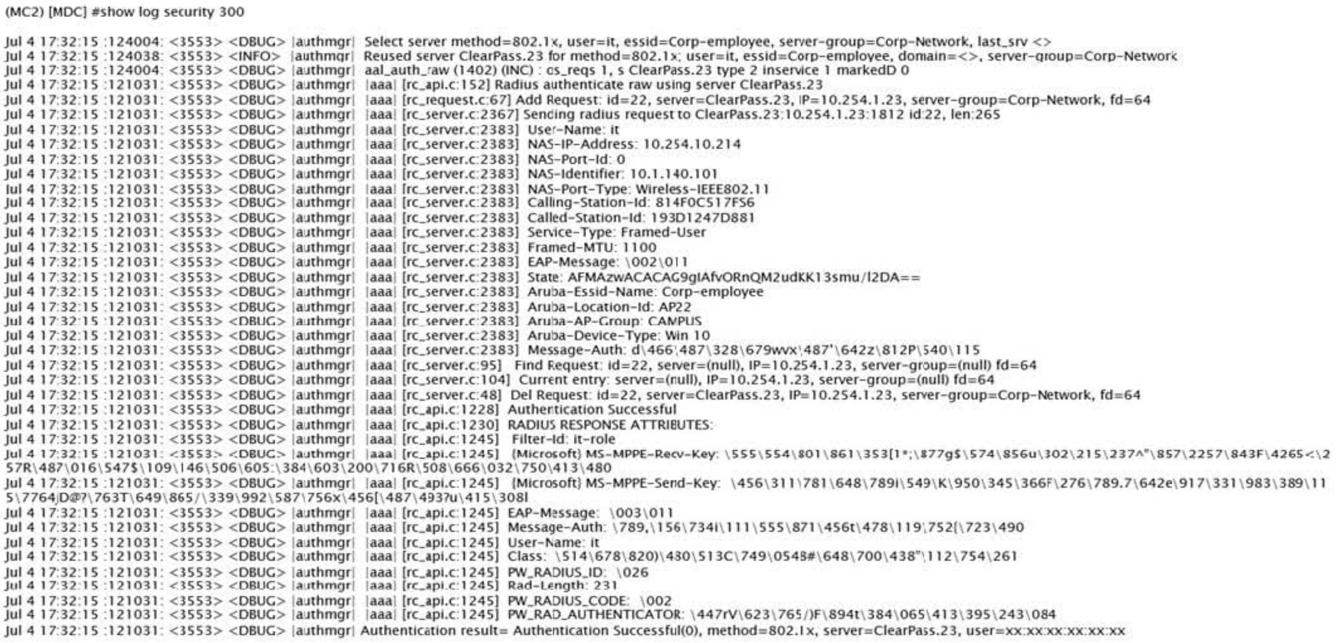
QUESTION 4

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) : cs_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/I2DA==
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$\574\856u\302\215\237^"\857\2257\843F\4265<\2
57R\487\016\547$\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\11
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)\430\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?

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

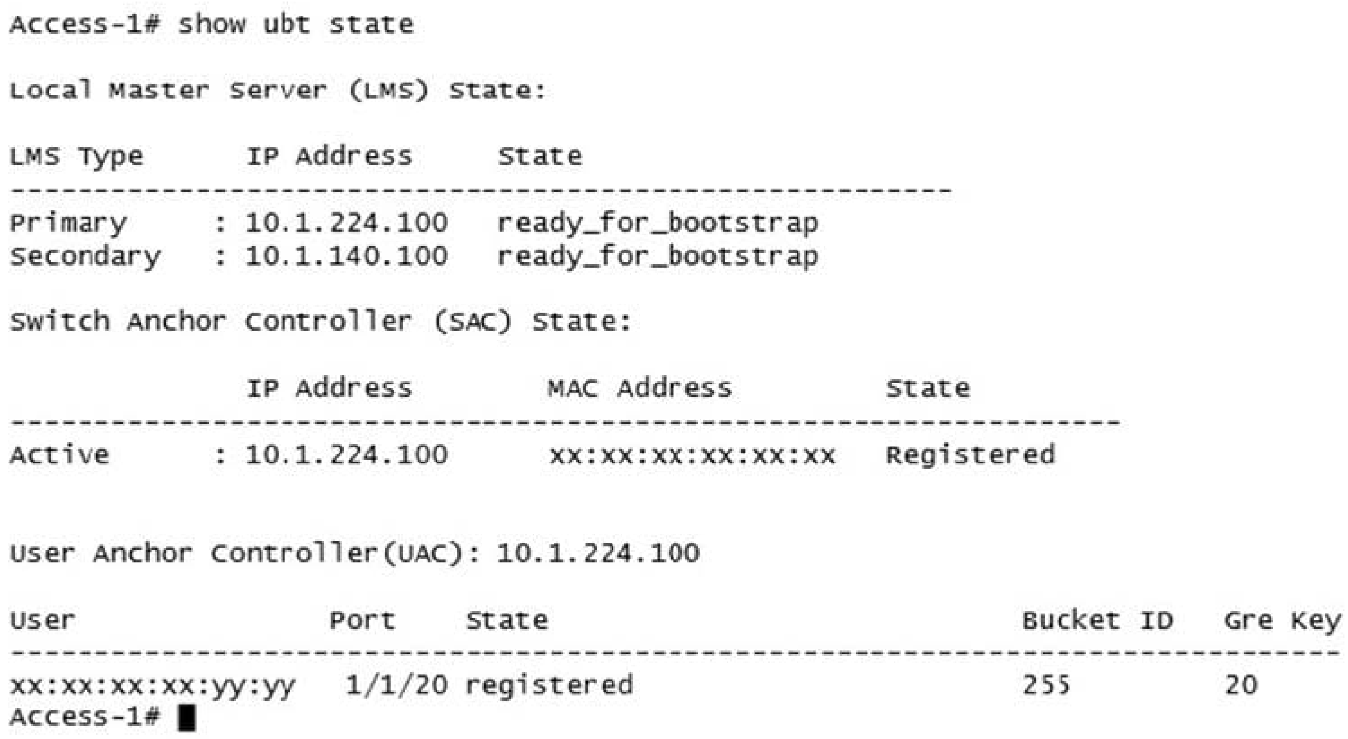
D. aaa server-group ClearPass set role condition Filter-Id equals it_department set-value it-role

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

Correct Answer: C

QUESTION 5

Refer to the exhibit.



```
Access-1# show ubt state

Local Master Server (LMS) State:

LMS Type        IP Address       State
---------------------------------------------------------
Primary      : 10.1.224.100   ready_for_bootstrap
Secondary    : 10.1.140.100   ready_for_bootstrap

Switch Anchor Controller (SAC) State:

                IP Address         MAC Address          State
-------------------------------------------------------------------
Active       : 10.1.224.100      xx:xx:xx:xx:xx:xx   Registered


User Anchor Controller(UAC): 10.1.224.100

User                 Port     State                              Bucket ID    Gre Key
---------------------------------------------------------------------------------------
xx:xx:xx:xx:yy:yy   1/1/20 registered                           255          20
Access-1# █
```

Based on the output shown in the exhibit, with which Aruba devices has Access-1 established tunnels?

A. a pair of standalone MCs

B. a pair of switches running VXLAN

C. a pair of MCs within a L3 cluster

D. a single standalone MC

Correct Answer: C