HPE6-A48.Premium.VCE.75q

Number: HPE6-A48
Passing Score: 925
Time Limit: 120 min
File Version: 19.081

QUESTION 1
Company 1 and Company 2 are medium-sized companies that collaborate in a joint venture. Each company owns a building, and each has their own ArubaOS 8 Mobility Master (MM)-Mobility Controller (MC) deployment. The buildings are located in front of one another. For the initial stage of the project, the companies want to interconnect their networks with fiber, and broadcast each other's SSIDs.

These are the requirements:

- Do not unify the company's network management responsibilities.
- Allow each company to take care of their own SSID setups when broadcasted in the other building.
- Terminate Company 1 user traffic on Company 1 MCs when they connect to Company 2 APs.
- Terminate Company 2 user traffic on Company 2 MCs when they connect to Company 1 APs.

What is needed to meet the solution requirements?

A. Multizone APs
B. Inter MC S2S Ipsec tunnels
C. Multi MC Clusters
D. Inter MC GRE tunnels

Correct Answer: B

QUESTION 2
A network administrator deploys AirWave over a Mobility Master (MM)-Mobility Controller (MC) network to monitor, audit, and report activities. The main areas of concern are with high user density, not enough APs, or not enough channel bandwidth.

Which two report options can the network administrator user to create a weekly report that shows networking equipment with more users and high-demand applications used by top talkers? (Select two.)

A. Most Utilized Folders by Maximum Concurrent Clients
B. Most Utilized by Usage
C. Top Applications Summary
D. Most Utilized by Maximum Concurrent Clients
E. Top 3 Applications For Top 10 Users

Correct Answer: BD

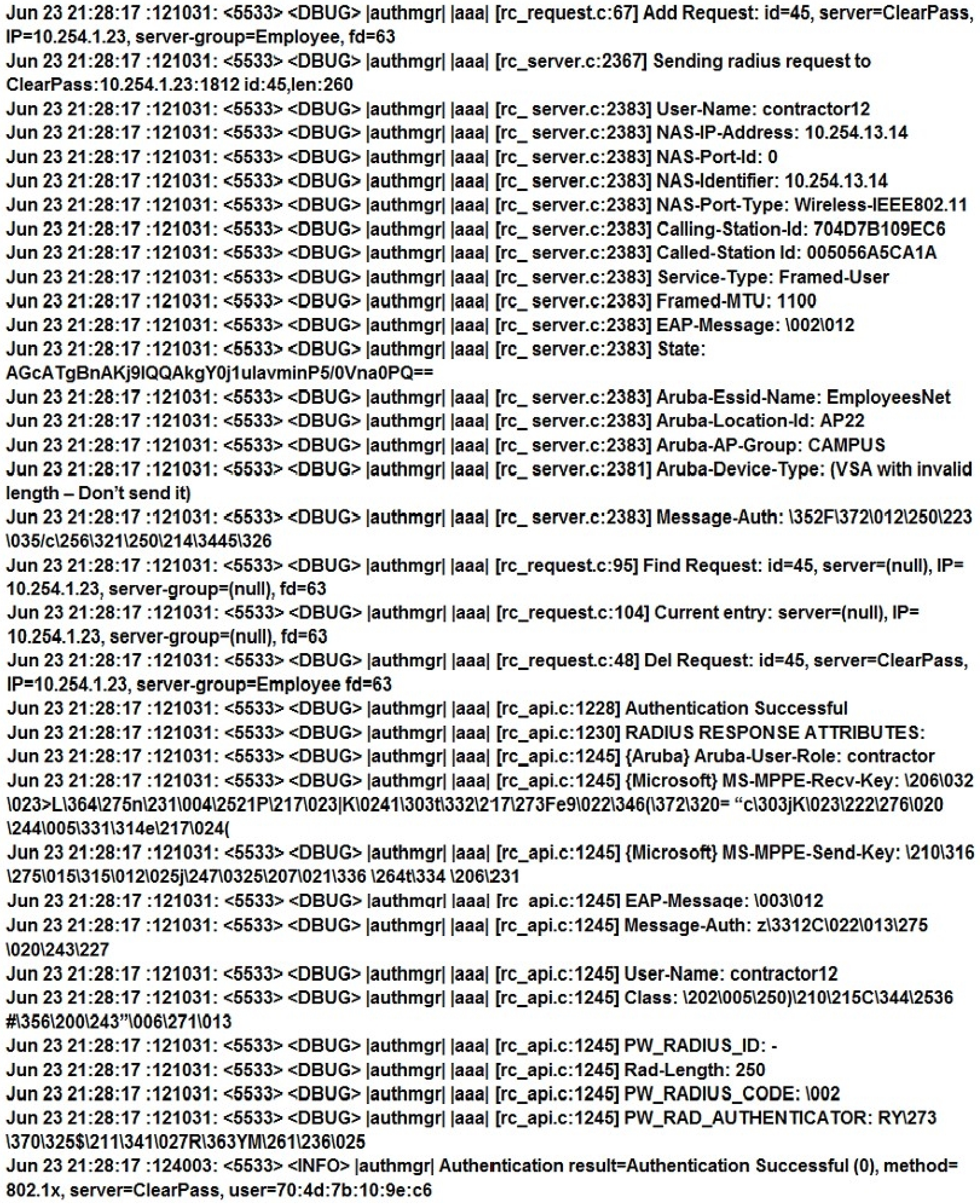
QUESTION 3
Several users are connected to the same WLAN and want to play the same multicast-based video stream. The network administrator wants to reduce bandwidth consumption and at the same time increase the transmit rate to a fixed value for WMM marked video streams in a large-scale network. Broadcast Multicast Optimization (BCMCO) is already on.

Which two configuration steps does the network administrator have to perform to optimize the multicast transmissions? (Select two.)

A. Enable Dynamic Multicast Optimization (DMO) and set forwarding mode to tunnel in the VAP profile.
B. Enable Broadcast Multicast Rate Optimization (BC/MC RO) in the SSID profile.
C. Enable Broadcast Multicast Optimization (BCMCO) and set forwarding mode in the VAP.
D. Disable Broadcast Multicast Optimization (BCMCO) in the VLAN.
E. Set Video Multicast Rate Optimization (VMRO) in the SSID profile.

Correct Answer: AC

QUESTION 4
Refer to the exhibit.



```
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=45, server=ClearPass,
IP=10.254.1.23, server-group=Employee, fd=63
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to
ClearPass:10.254.1.23:1812 id:45,len:260
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] User-Name: contractor12
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] NAS-IP-Address: 10.254.13.14
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] NAS-Port-Id: 0
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] NAS-Identifier: 10.254.13.14
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] NAS-Port-Type: Wireless-IEEE802.11
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] Calling-Station-Id: 704D7B109EC6
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] Called-Station Id: 005056A5CA1A
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] Service-Type: Framed-User
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] Framed-MTU: 1100
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] EAP-Message: \002\012
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] State:
AGcATgBnAKj9lQQAkgY0j1ulavminP5/0Vna0PQ==
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] Aruba-Essid-Name: EmployeesNet
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] Aruba-Location-Id: AP22
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] Aruba-AP-Group: CAMPUS
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2381] Aruba-Device-Type: (VSA with invalid
length – Don’t send it)
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] Message-Auth: \352F\372\012\250\223
\035/c\256\321\250\214\3445\326
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_request.c:95] Find Request: id=45, server=(null), IP=
10.254.1.23, server-group=(null), fd=63
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_request.c:104] Current entry: server=(null), IP=
10.254.1.23, server-group=(null), fd=63
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_request.c:48] Del Request: id=45, server=ClearPass,
IP=10.254.1.23, server-group=Employee fd=63
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1228] Authentication Successful
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] {Aruba} Aruba-User-Role: contractor
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] {Microsoft} MS-MPPE-Recv-Key: \206\032
\023>L\364\275n\231\004\2521P\217\023|K\0241\303t\332\217\273Fe9\022\346(\372\320= “c\303jK\023\222\276\020
\244\005\331\314e\217\024(
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] {Microsoft} MS-MPPE-Send-Key: \210\316
\275\015\315\012\025j\247\0325\207\021\336 \264t\334 \206\231
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] EAP-Message: \003\012
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Message-Auth: z\3312C\022\013\275
\020\243\227
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] User-Name: contractor12
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Class: \202\005\250)\210\215C\344\2536
#\356\200\243”\006\271\013
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RADIUS_ID: -
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Rad-Length: 250
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RADIUS_CODE: \002
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RAD_AUTHENTICATOR: RY\273
\370\325$\211\341\027R\363YM\261\236\025
Jun 23 21:28:17 :124003: <5533> <INFO> |authmgr| Authentication result=Authentication Successful (0), method=
802.1x, server=ClearPass, user=70:4d:7b:10:9e:c6
```

A network administrator wants to allow contractors to access the WLAN named EmployeesNet. In order to restrict network access, the network administrator wants to assign this category of users to the contractor firewall role.

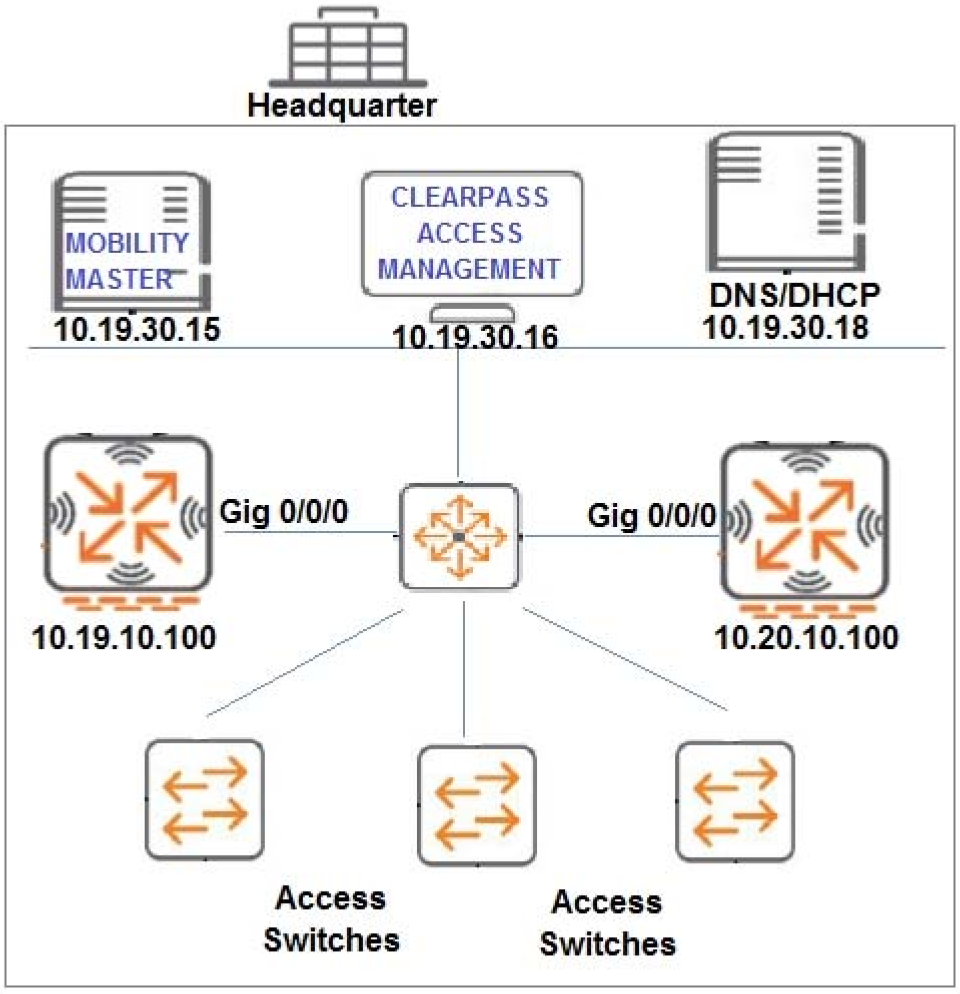
To do this, the network administrator configures ClearPass in a way that it returns the Aruba-User-Role VSA with the contractor value. When testing the solution the network administrator receives the wrong role.

What should the network administrator do to assign the contractor role to contractor users without affecting any other role assignment?

A. Set contractor as the default role in the AAA profile.
B. Create the contractor firewall role in the MC.
C. Create server derivation rules in the server group.
D. Check the Download role from the CPPM option in the AAA profile.

Correct Answer: A

QUESTION 5
Refer to the exhibit.



A network administrator is in charge of a wired and wireless Aruba network where access control is needed for both connection methods. For the wired solution, the network administrator wants the users authentication to be performed at the switches, while tunneling their traffic to MC1 whenever possible for firewall policy enforcement. The network administrator configures and tests ClearPass as the RADIUS server in the switches.

Which switch configuration scripts should the network administrator use next to achieve this goal?

A. tunneled-node-server
controller-ip 10.19.10.100
backup-controller-ip 10.20.10.100
mode role-based
aaa authentication port-access eap-radius
aaa port-access authenticator 1-22
aaa port-access authenticator active

B. tunneled-node-server
controller-ip 10.20.10.100
backup-controller-ip 10.19.10.100
mode port-based
aaa authentication port-access eap-radius
aaa port-access authenticator 1-22
aaa port-access authenticator active

C. tunneled-node-server
controller-ip 10.20.10.100
backup-controller-ip 10.19.10.100
aaa authentication port-access eap-radius
aaa port-access authenticator 1-22
aaa port-access authenticator active

D. tunneled-node-server
controller-ip 10.19.10.100
backup-controller-ip 10.20.10.100
aaa authentication port-access eap-radius
aaa port-access authenticator 1-22
aaa port-access authenticator active

Correct Answer: C

QUESTION 6
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.

B. 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.

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

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: A