Vendor:HP

Exam Code:HPE6-A48

Exam Name: Aruba Certified Mobility Expert 8 Written Exam

Version: Demo

QUESTION 1

An airline wants to invest in an Aruba Mobility (MM)-Mobility Controller (MC) solution for the three hubs it has throughout the country. A single MM is located in the datacenter at one of the hubs. The MCs in the other two hubs reach the MM through a site-to-site IPSec VPN.

The operations team does not want to lose monitoring and configuration control of the MCs if something happens to the datacenter where the MM resides.

Which solution ensures that there is management access to the MCs in case of an MM failure due to a datacenter outage?

A. Deploy another MM in a different location, and enable L2 redundancy.

B. Install AirWave Management Platform, and enable Read and Write Management access on devices.

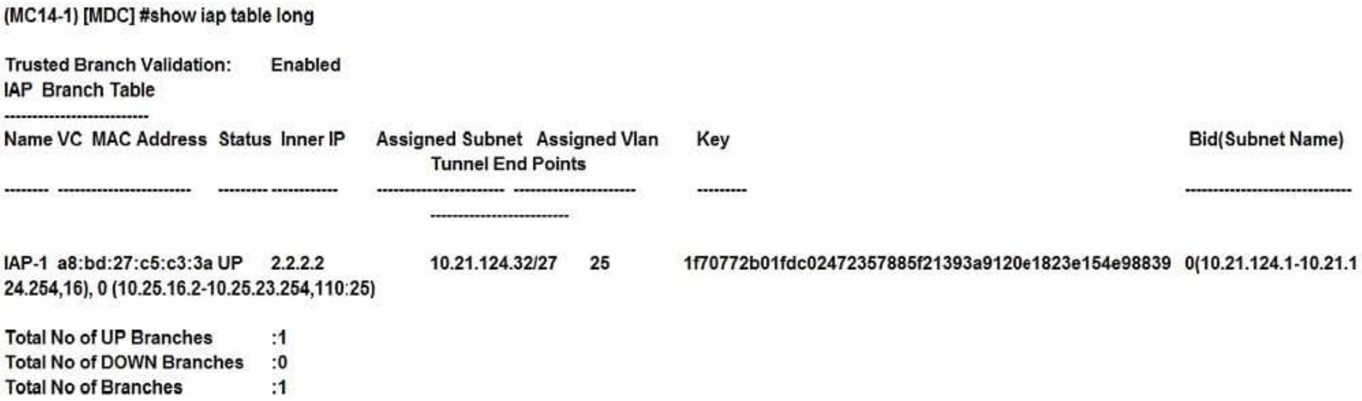
C. Deploy another MM in a different location, and enable L3 redundancy.

D. Deploy a local MM on each hub, and synchronize the configuration between all MMs.

Correct Answer: B

QUESTION 2

Refer to the exhibit.



```
(MC14-1) [MDC] #show iap table long

Trusted Branch Validation:      Enabled
IAP  Branch Table
-------------------------
Name VC  MAC Address  Status  Inner IP     Assigned Subnet   Assigned Vlan      Key                                                          Bid(Subnet Name)
                                                   Tunnel End Points
-------- ----------------------  --------- -----------   -------------------- --------------------       ---------                                                   ----------------------------
                                                   ------------------------

IAP-1  a8:bd:27:c5:c3:3a UP     2.2.2.2            10.21.124.32/27     25          1f70772b01fdc02472357885f21393a9120e1823e154e98839  0(10.21.124.1-10.21.1
24.254,16), 0 (10.25.16.2-10.25.23.254,110:25)

Total No of UP Branches         :1
Total No of DOWN Branches       :0
Total No of Branches            :1
```

A network administrator configures an Instant AP (IAP) to establish an Aruba IPSec tunnel across the Internet, and configures two DHCP pools for wireless users.

Based on the output shown in the exhibit, which device behaves as a DHCP server for the users?

A. Mobility Master

B. Mobility Controller

C. External server

D. DSL modem

E. Virtual Controller

Correct Answer: B

QUESTION 3

Refer to the exhibits.

Exhibit 1

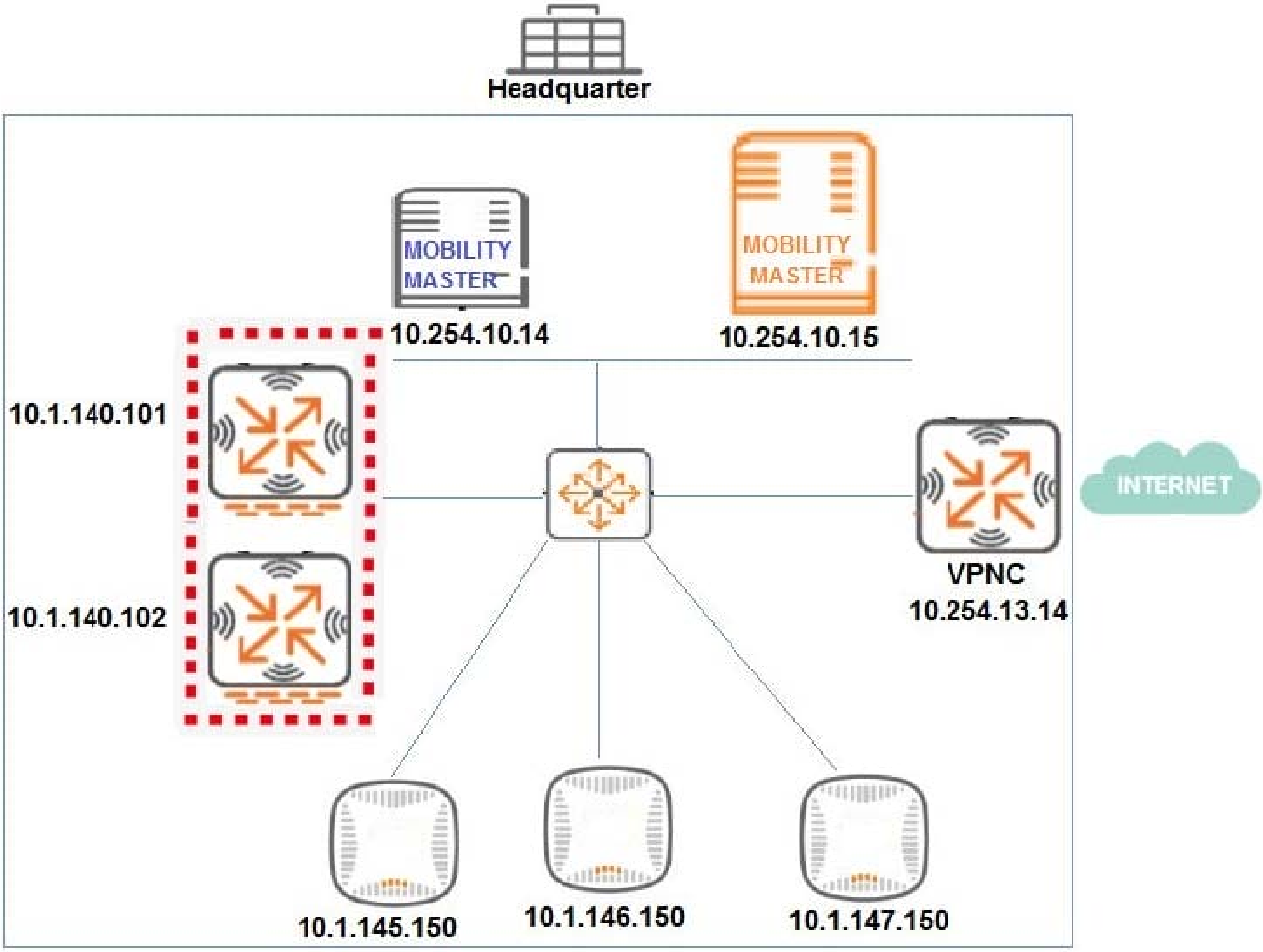
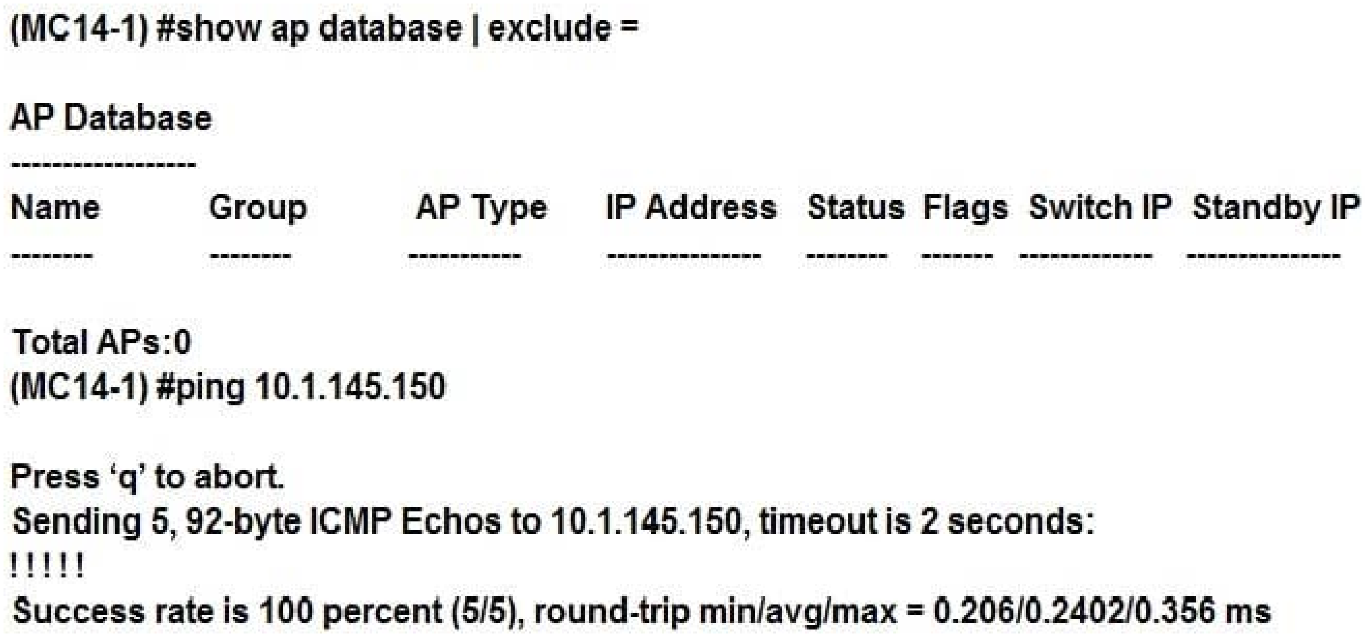


Exhibit 2



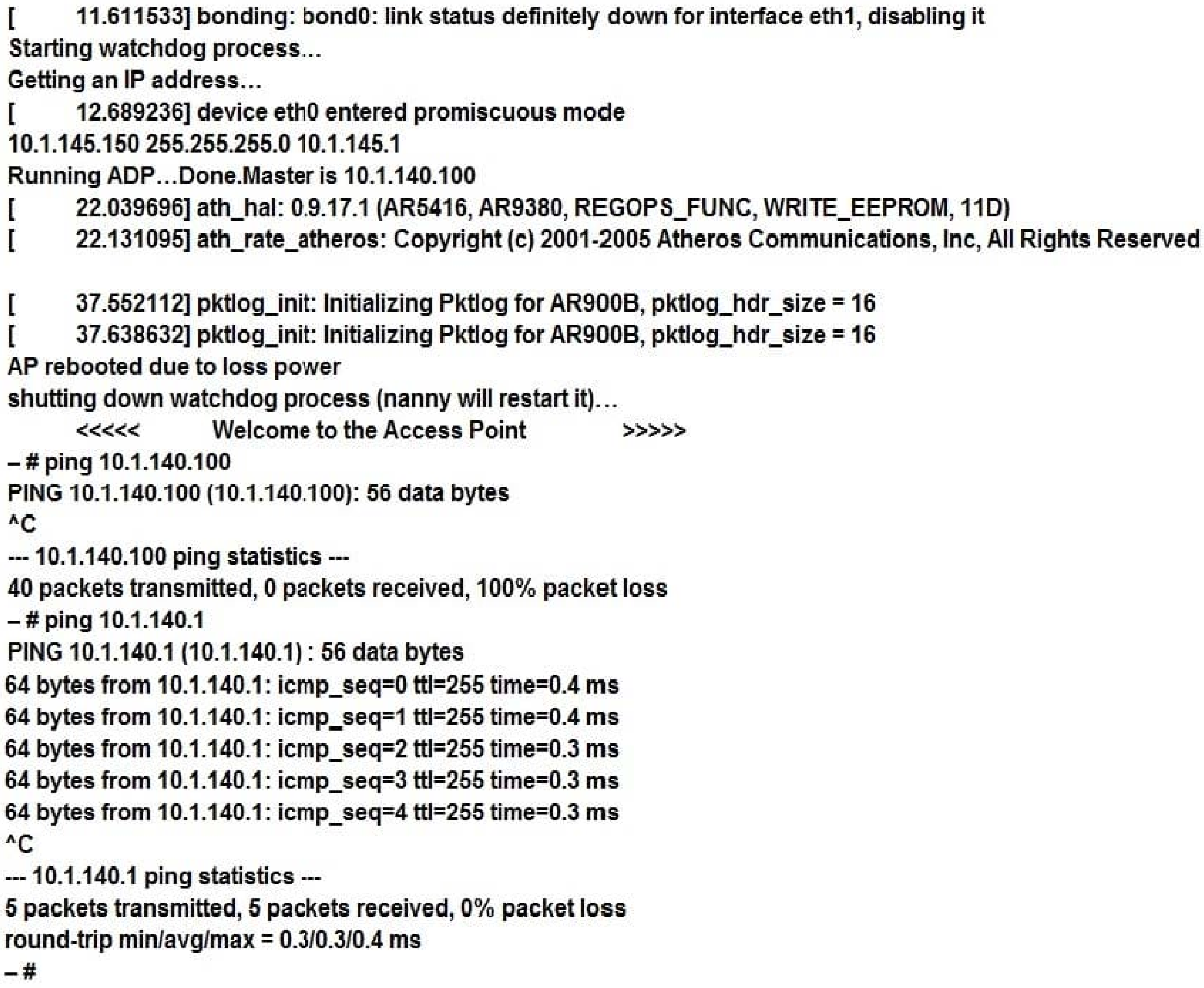
```
(MC14-1) #show ap database | exclude =

AP Database
-------------------
Name        Group       AP Type      IP Address      Status   Flags   Switch IP     Standby IP
--------    --------    -----------  ---------------  --------  -------  -------------  ---------------

Total APs:0
(MC14-1) #ping 10.1.145.150

Press ‘q’ to abort.
Sending 5, 92-byte ICMP Echos to 10.1.145.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.206/0.2402/0.356 ms
```

Exhibit 3



```
[        11.611533] bonding: bond0: link status definitely down for interface eth1, disabling it
Starting watchdog process...
Getting an IP address...
[        12.689236] device eth0 entered promiscuous mode
10.1.145.150 255.255.255.0 10.1.145.1
Running ADP...Done.Master is 10.1.140.100
[        22.039696] ath_hal: 0.9.17.1 (AR5416, AR9380, REGOPS_FUNC, WRITE_EEPROM, 11D)
[        22.131095] ath_rate_atheros: Copyright (c) 2001-2005 Atheros Communications, Inc, All Rights Reserved

[        37.552112] pktlog_init: Initializing Pktlog for AR900B, pktlog_hdr_size = 16
[        37.638632] pktlog_init: Initializing Pktlog for AR900B, pktlog_hdr_size = 16
AP rebooted due to loss power
shutting down watchdog process (nanny will restart it)...
        <<<<<         Welcome to the Access Point          >>>>>
– # ping 10.1.140.100
PING 10.1.140.100 (10.1.140.100): 56 data bytes
^C
--- 10.1.140.100 ping statistics ---
40 packets transmitted, 0 packets received, 100% packet loss
– # ping 10.1.140.1
PING 10.1.140.1 (10.1.140.1) : 56 data bytes
64 bytes from 10.1.140.1: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 10.1.140.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.1.140.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 10.1.140.1: icmp_seq=3 ttl=255 time=0.3 ms
64 bytes from 10.1.140.1: icmp_seq=4 ttl=255 time=0.3 ms
^C
--- 10.1.140.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.4 ms
– #
```

A network engineer deploys a Master Controller (MC) cluster at Headquarter to offer high levels of redundancy, and prepares the wired side of the network. This preparation includes the VLAN, DHCP Settings, and unicast routing services that APs require to reach the cluster.

The network engineer waits for 20 minutes after connecting the APs and sees that no SSIDs are advertised. The network engineer logs into one of the MCs and one of the AP\\'s consoles to obtain the outputs shown in the exhibits.

What can the network engineer do to fix the APs discovery process, to ensure the best scalability even if one MC fails?

A. Reprovision the APs with a different Master IP.

B. Modify the IP address in one of the MCs.

C. Modify option 43 in the DHCP pool.

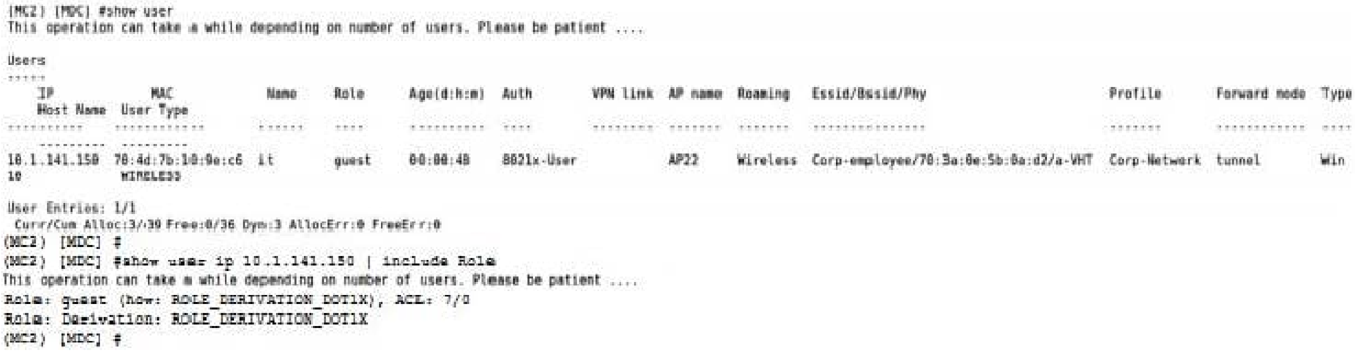
D. Create a VRRP instance in the MCs.

Correct Answer: C

QUESTION 4

Refer to the exhibits.

Exhibit1

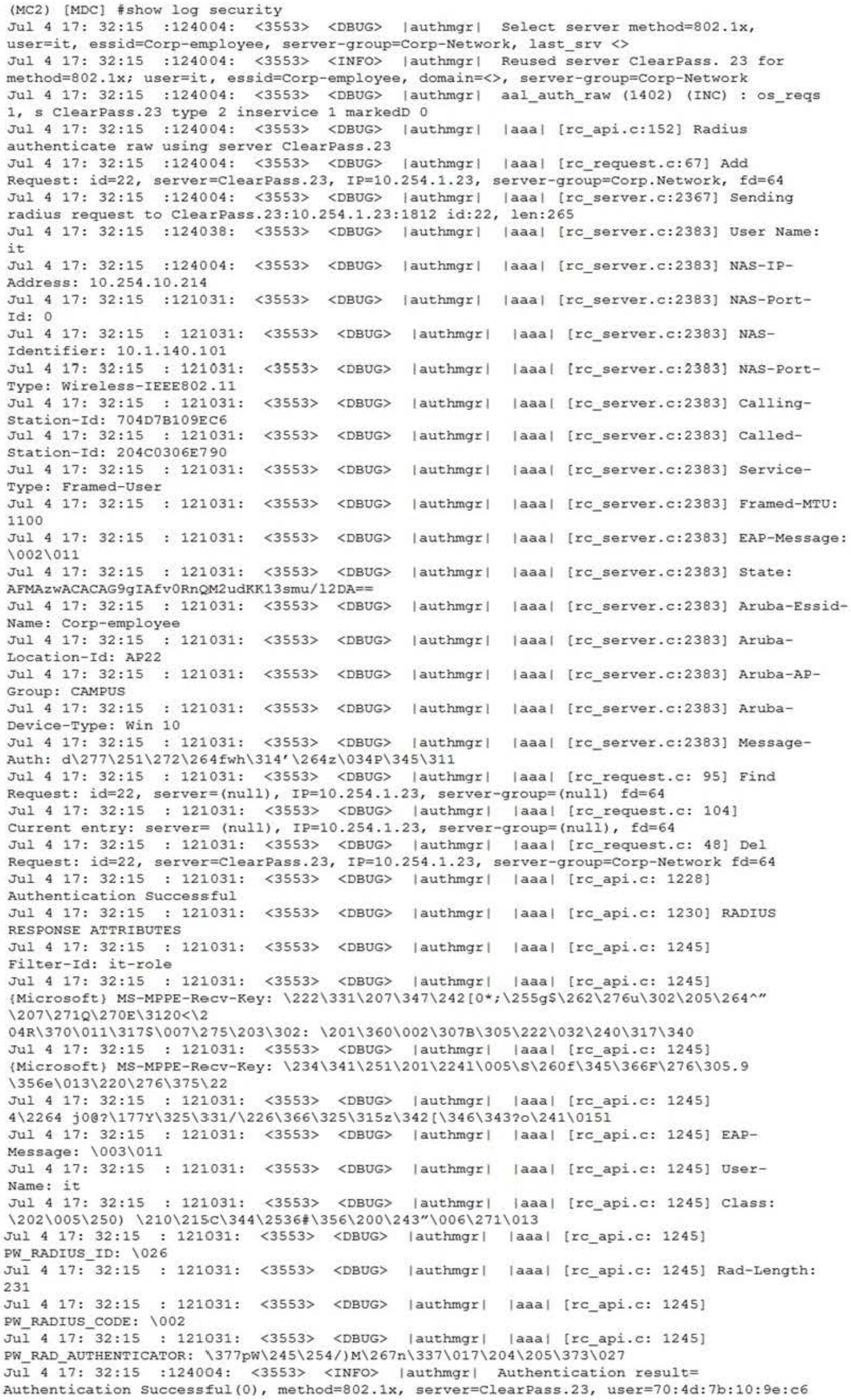


```
(MC2) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

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  70:4d:7b:10:9e:c6  it      guest    00:00:48    8021x-User            AP22     Wireless  Corp-employee/70:3a:0e:5b:0a:d2/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_DERIVATION_DOT1X), ACL: 7/0
Role: Derivation: ROLE_DERIVATION_DOT1X
(MC2) [MDC] #
```

Exhibit2



```
(MC2) [MDC] #show log security
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  :124004:  <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  :124004:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c:152] Radius
authenticate raw using server ClearPass.23
Jul 4 17: 32:15  :124004:  <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  :124004:  <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  :124038:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] User Name:
it
Jul 4 17: 32:15  :124004:  <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: 704D7B109EC6
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Called-
Station-Id: 204C0306E790
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:
AFMAzwACACAG9gIAfv0RnQM2udKK13smu/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\277\251\272\264fwh\314'\264z\034P\345\311
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_request.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_request.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_request.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: \222\331\207\347\242[0*;\255g$\262\276u\302\205\264^"
\207\271Q\270E\3120<\2
04R\370\011\317$\007\275\203\302: \201\360\002\307B\305\222\032\240\317\340
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c: 1245]
{Microsoft} MS-MPPE-Recv-Key: \234\341\251\201\2241\005\S\260f\345\366F\276\305.9
\356e\013\220\276\375\22
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c: 1245]
4\2264 j0@?\177Y\325\331/\226\366\325\315z\342[\346\343?o\241\0151
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] User-
Name: it
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c: 1245] Class:
\202\005\250) \210\215C\344\2536#\356\200\243"\006\271\013
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: \377pW\245\254/)M\267n\337\017\204\205\373\027
Jul 4 17: 32:15  :124004:  <3553>  <INFO>  |authmgr|  Authentication result=
Authentication Successful(0), method=802.1x, server=ClearPass.23, user=70:4d:7b:10:9e:c6
```

A network administrator integrates a current Mobility Master (MM)-Mobility Controller (MC) deployment with a RADIUS infrastructure. After using the RADIUS server to authenticate a wireless user, the network administrator realizes that the client machine is not falling into the it_department role, as shown in 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 GROUP-RADIUS set role condition Filter-Id equals it-role set-value it_department

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

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

Correct Answer: B

QUESTION 5

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

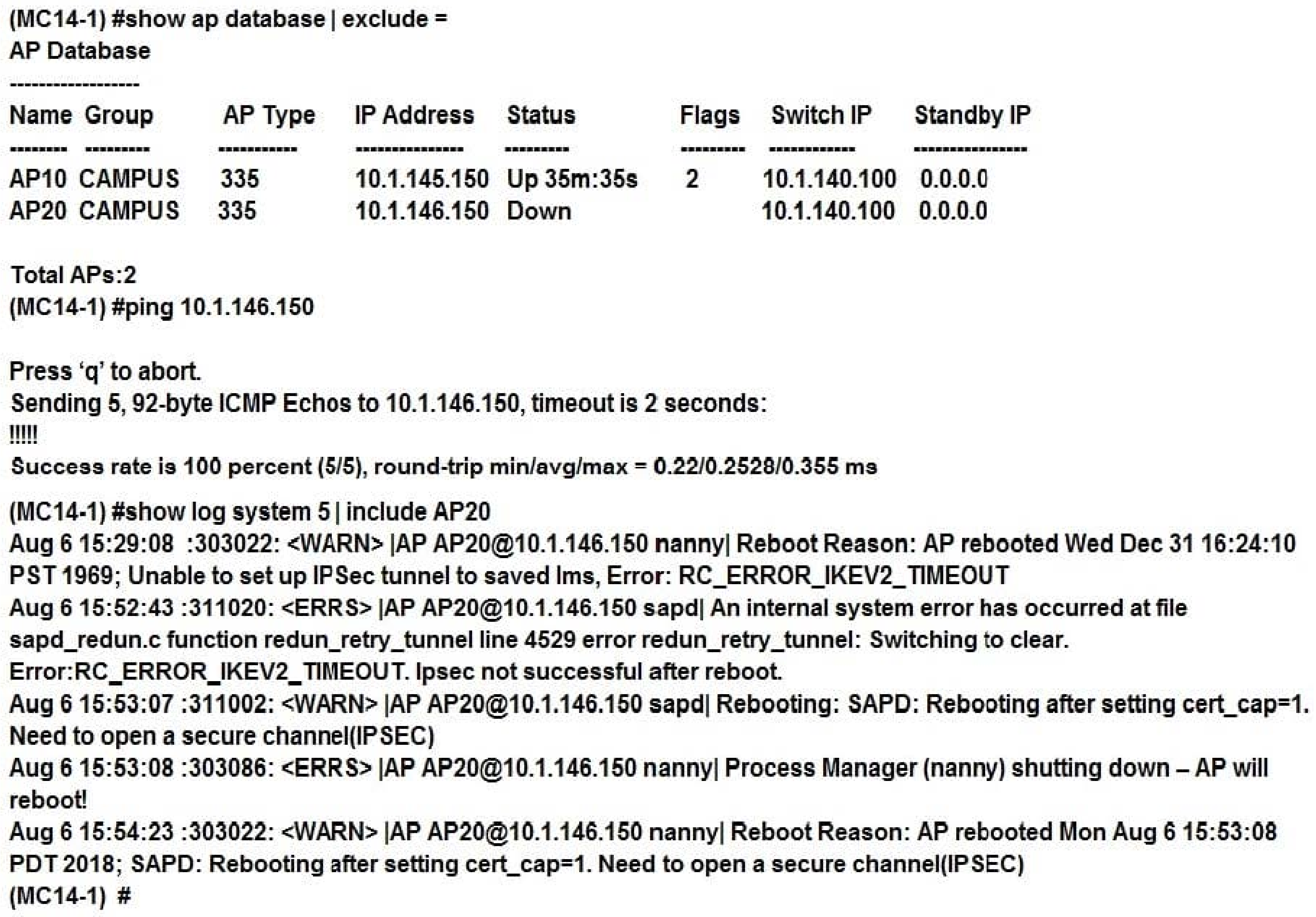
D. Most Utilized by Maximum Concurrent Clients

E. Top 3 Applications For Top 10 Users

Correct Answer: BD

QUESTION 6

Refer to the exhibit.



```
(MC14-1) #show ap database | exclude =
AP Database
------------------
Name  Group      AP Type    IP Address     Status        Flags   Switch IP      Standby IP
--------  ---------    -----------    ---------------    ---------       ---------   ------------   ---------------
AP10  CAMPUS    335        10.1.145.150   Up 35m:35s     2      10.1.140.100   0.0.0.0
AP20  CAMPUS    335        10.1.146.150   Down                  10.1.140.100   0.0.0.0

Total APs:2
(MC14-1) #ping 10.1.146.150

Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 10.1.146.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.22/0.2528/0.355 ms
(MC14-1) #show log system 5 | include AP20
Aug 6 15:29:08  :303022: <WARN> |AP AP20@10.1.146.150 nanny| Reboot Reason: AP rebooted Wed Dec 31 16:24:10
PST 1969; Unable to set up IPSec tunnel to saved lms, Error: RC_ERROR_IKEV2_TIMEOUT
Aug 6 15:52:43 :311020: <ERRS> |AP AP20@10.1.146.150 sapd| An internal system error has occurred at file
sapd_redun.c function redun_retry_tunnel line 4529 error redun_retry_tunnel: Switching to clear.
Error:RC_ERROR_IKEV2_TIMEOUT. Ipsec not successful after reboot.
Aug 6 15:53:07 :311002: <WARN> |AP AP20@10.1.146.150 sapd| Rebooting: SAPD: Rebooting after setting cert_cap=1.
Need to open a secure channel(IPSEC)
Aug 6 15:53:08 :303086: <ERRS> |AP AP20@10.1.146.150 nanny| Process Manager (nanny) shutting down – AP will
reboot!
Aug 6 15:54:23 :303022: <WARN> |AP AP20@10.1.146.150 nanny| Reboot Reason: AP rebooted Mon Aug 6 15:53:08
PDT 2018; SAPD: Rebooting after setting cert_cap=1. Need to open a secure channel(IPSEC)
(MC14-1)  #
```

A network administrator deploys a Mobility Master (MM)-Mobility Controller (MC) solution in the headquarters. The network administrator prepares the wired side of the network with the proper VLAN, DHCP settings, and routing services to ensure that APs can reach the MCs.

The network administrator connects two APs in different IP segments and waits for 20 minutes, but SSIDs are advertised in one of the APs only. The engineer logs into the MC console and sees the output shown in the exhibit.

What is the reason that the AP20 is not broadcasting SSIDs?

A. IPSec traffic is being blocked.

B. IKE traffic is being dropped.

C. PAPI traffic is being blocked.

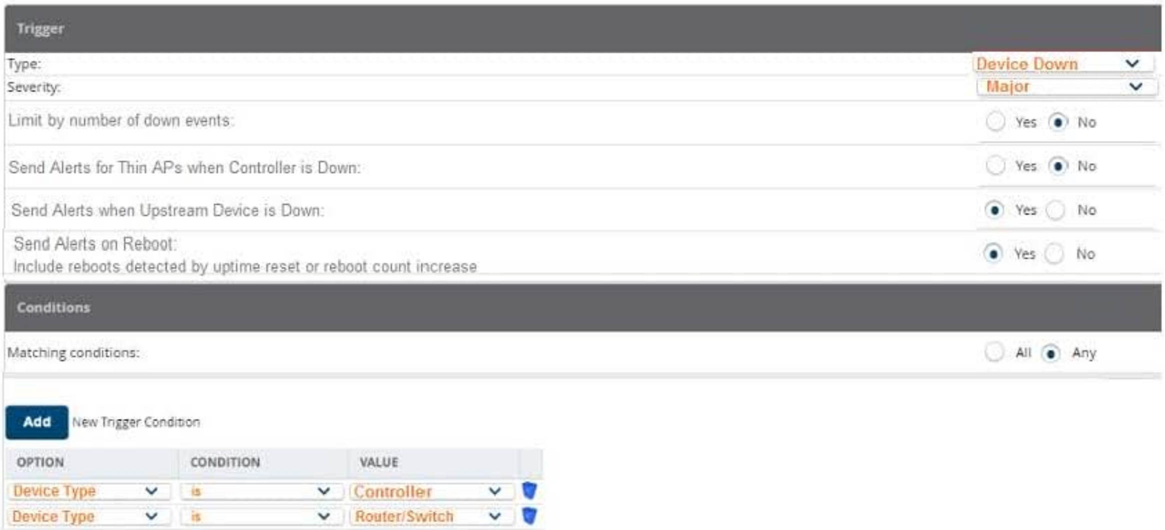
D. GRE traffic is being blocked.

Correct Answer: B

QUESTION 7

A network administrator wants to receive a major alarm every time a controller or an Aruba switch goes down for either a local or an upstream device failure. Which alarm definition must the network administrator create to accomplish this?

○ A.



Trigger

Type:	Device Down
Severity:	Major
Limit by number of down events:	○ Yes ● No
Send Alerts for Thin APs when Controller is Down:	○ Yes ● No
Send Alerts when Upstream Device is Down:	● Yes ○ No
Send Alerts on Reboot: Include reboots detected by uptime reset or reboot count increase	● Yes ○ No

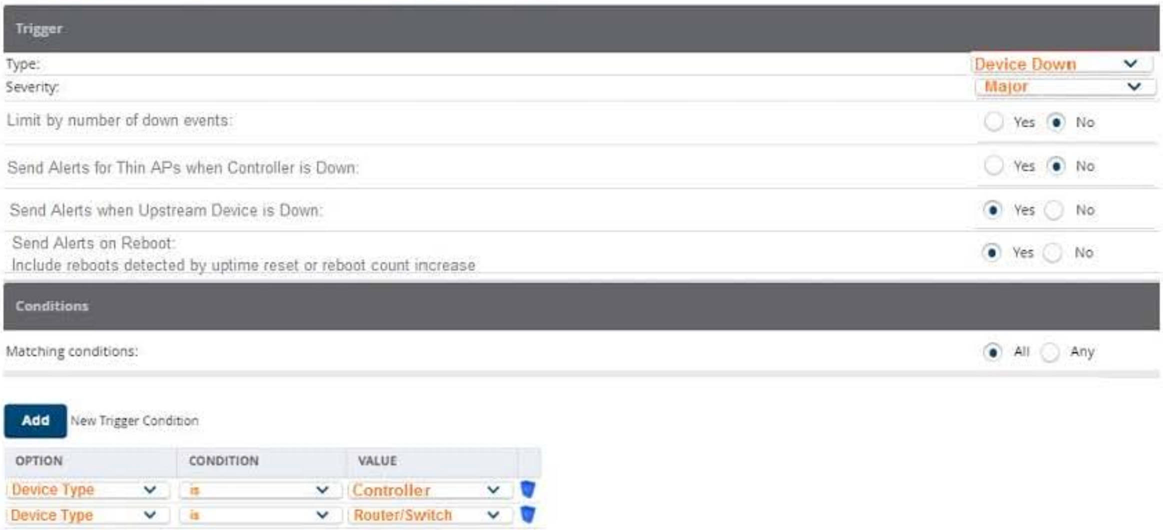
Conditions

Matching conditions: ○ All ● Any

Add New Trigger Condition

OPTION	CONDITION	VALUE
Device Type	is	Controller
Device Type	is	Router/Switch

○ B.



Trigger

Type:	Device Down
Severity:	Major
Limit by number of down events:	○ Yes ● No
Send Alerts for Thin APs when Controller is Down:	○ Yes ● No
Send Alerts when Upstream Device is Down:	● Yes ○ No
Send Alerts on Reboot: Include reboots detected by uptime reset or reboot count increase	● Yes ○ No

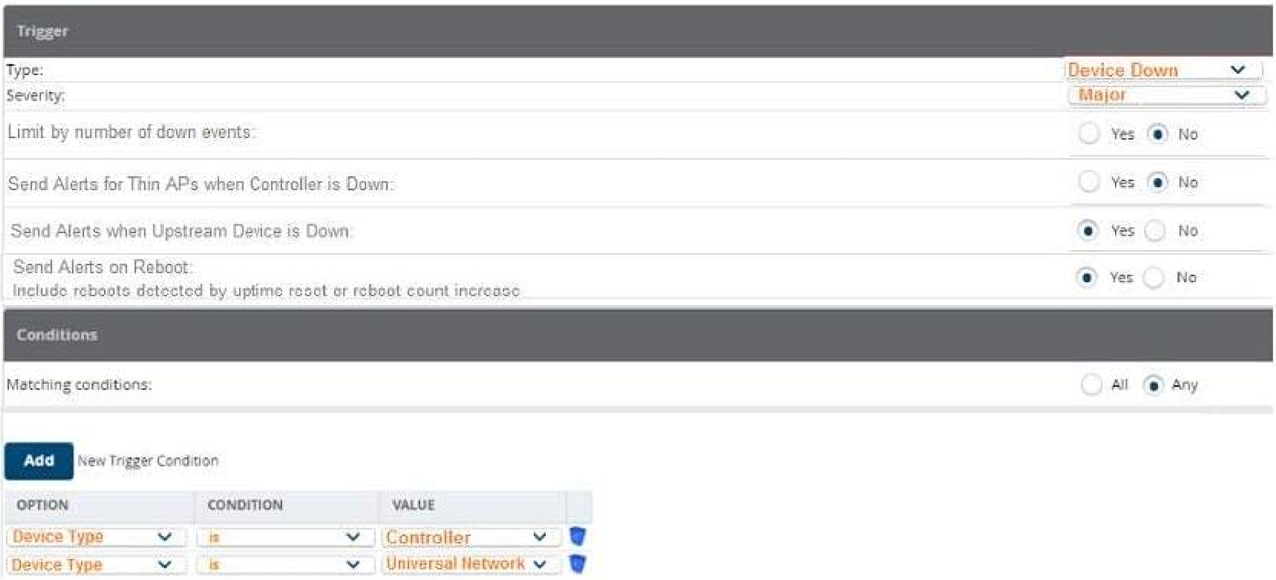
Conditions

Matching conditions: ● All ○ Any

Add New Trigger Condition

OPTION	CONDITION	VALUE
Device Type	is	Controller
Device Type	is	Router/Switch

○ C.



Trigger

Type: Device Down

Severity: Major

Limit by number of down events: ○ Yes ● No

Send Alerts for Thin APs when Controller is Down: ○ Yes ● No

Send Alerts when Upstream Device is Down: ● Yes ○ No

Send Alerts on Reboot:
Include reboots detected by uptime reset or reboot count increase ● Yes ○ No

Conditions

Matching conditions: ○ All ● Any

Add New Trigger Condition

OPTION	CONDITION	VALUE
Device Type	is	Controller
Device Type	is	Universal Network

A. Option A

B. Option B

C. Option C

Correct Answer: B

QUESTION 8

A network administrator deploys APs with radios in Air Monitor mode and detects several APs and SSIDs that belong to stores next door. The Mobility Master (MM) classifies the APs and SSIDs as potential rogues. The network administrator wants to prevent the Air Monitor from applying countermeasures against these APs.

How can the network administrator accomplish this?

A. Select the BSSID and click reclassify, then select neighbor.

B. Run the Define WIP Policy task, and define the BSSIDs of the neighboring APs as interfering.

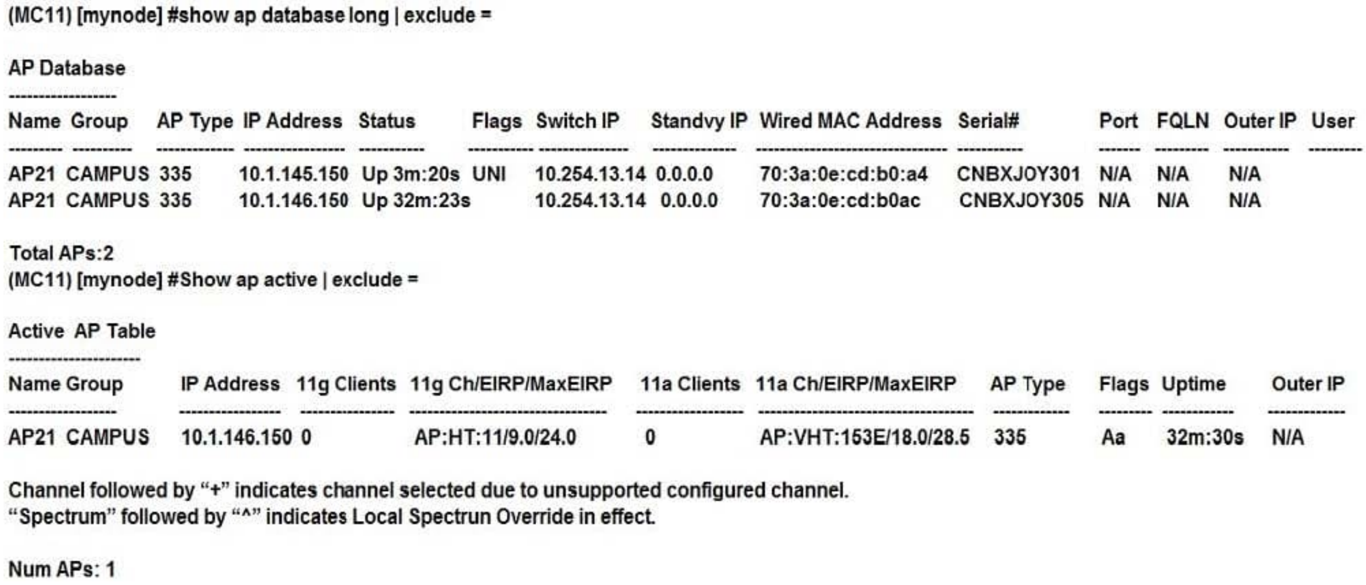
C. Select the BSSID and click reclassify, then select interfering.

D. Run the Define WIP Policy task, and define the BSSIDs of the neighboring APs as Authorized.

Correct Answer: A

QUESTION 9

Refer to the exhibit.



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

AP Database
------------------
Name  Group    AP Type  IP Address    Status        Flags  Switch IP     Standvy IP  Wired MAC Address  Serial#      Port  FQLN  Outer IP  User
------ -------  -------- ------------- ------------  ------ ------------- ----------- ------------------ ----------   ----  ----  --------  -----
AP21  CAMPUS  335      10.1.145.150  Up 3m:20s     UNI    10.254.13.14  0.0.0.0     70:3a:0e:cd:b0:a4  CNBXJOY301   N/A   N/A   N/A
AP21  CAMPUS  335      10.1.146.150  Up 32m:23s           10.254.13.14  0.0.0.0     70:3a:0e:cd:b0ac   CNBXJOY305   N/A   N/A   N/A

Total APs:2
(MC11) [mynode] #Show ap active | exclude =

Active  AP Table
----------------------
Name Group       IP Address    11g Clients  11g Ch/EIRP/MaxEIRP   11a Clients  11a Ch/EIRP/MaxEIRP      AP Type  Flags  Uptime    Outer IP
-----------      ------------  -----------  -------------------   -----------  -----------------------  -------  -----  --------  --------
AP21  CAMPUS     10.1.146.150  0            AP:HT:11/9.0/24.0     0            AP:VHT:153E/18.0/28.5    335      Aa     32m:30s   N/A

Channel followed by "+" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrun Override in effect.

Num APs: 1
```

A network administrator deploys a new Mobility Master (MM)-Mobility Controller (MC) network. To test the solution, the network administrator accessess some of the AP consoles and statistically provisions them. However, these APs do not propagate the configured SSIDs. The network administrator looks at the logs and sees the output shown in the exhibit.

Which actions must the network administrator take to solve the problem?

A. Reprovision one of the APs with a different name, and add new entries with the proper group in the whitelist.

B. Reprovision the AP with a different group, and modify the name of one AP in the whitelist.

C. Create another AP group in the MC\\'s configuration and reprovision one AP with a different group.

D. Reprovision one of the APs with a different name, and modify the name of one AP in the whitelist.

Correct Answer: B

QUESTION 10

An organization owns a fully functional multi-controller Aruba network with a Virtual Mobility Master (VMM) in VLAN 20. They have asked a network consultant to deploy a redundant MM on a different server. The solution must offer the lowest convergence time and require no human interaction in case of failure.

The servers host other virtual machines and are connected to different switches that implement ACLs to protect them. The organization grants the network consultant access to the servers only, and appoints a network administrator to assist with the deployment.

What must the network administrator do so the network consultant can successfully deploy the solution? (Select three.)

A. Reserve one IP address for the second MM and another IP address for its gateway

B. Configure an ACL entry that permits IP protocol 50, UDP port 500, and multicast IP 224.0.0.18.

C. Allocate VLAN 20 to the second server, and extend it throughout the switches.

D. Reserve one IP address for the second MM and another for the VIP.

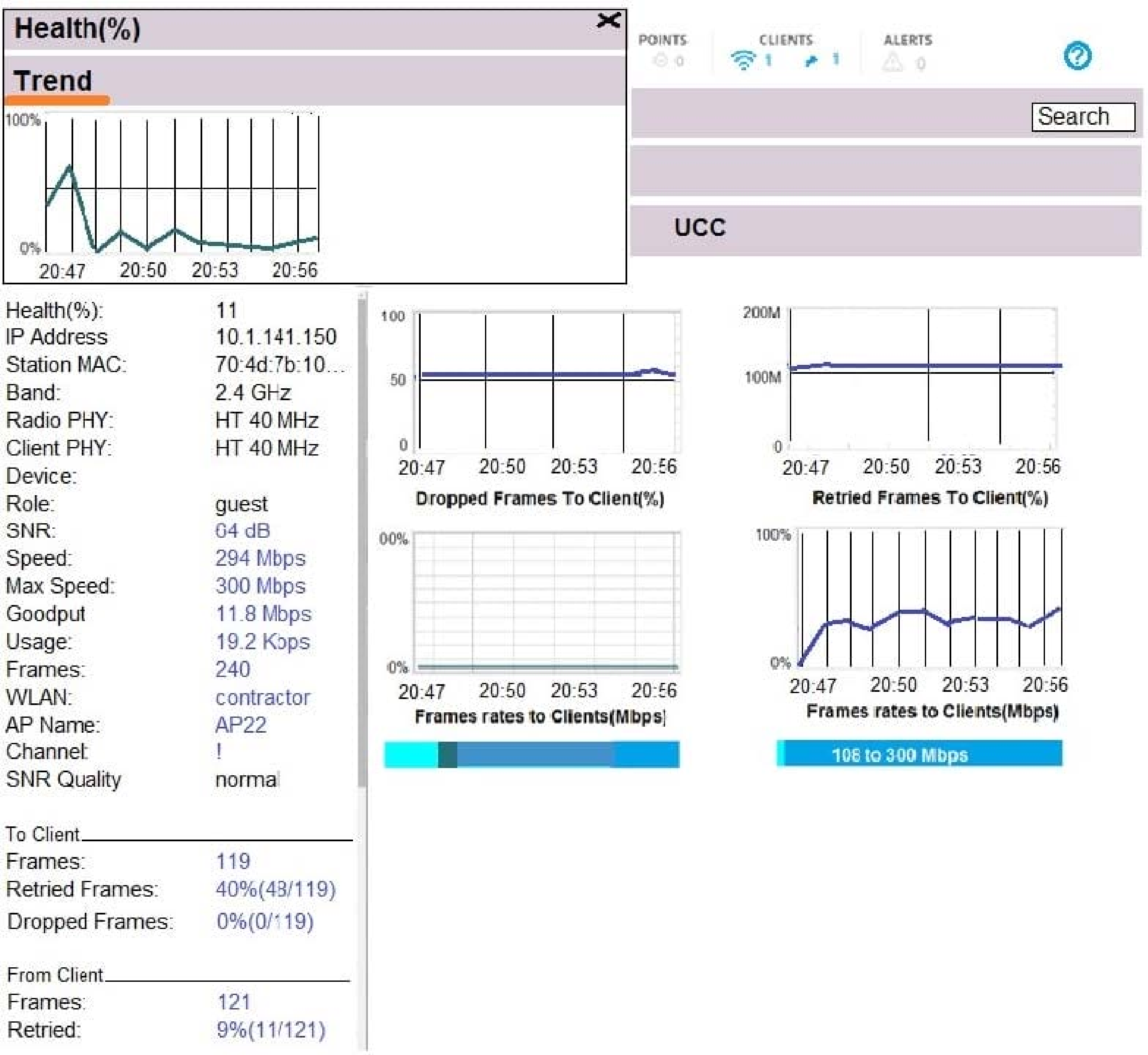
E. Configure an ACL entry that permits UDP 500, UDP 4500, and multicast IP 224.0.0.1.

F. Allocate another VLAN to the second server, and permit routing between them.

Correct Answer: ACE

QUESTION 11

Refer to the exhibit.



Health(%):	11
IP Address	10.1.141.150
Station MAC:	70:4d:7b:10...
Band:	2.4 GHz
Radio PHY:	HT 40 MHz
Client PHY:	HT 40 MHz
Device:	
Role:	guest
SNR:	64 dB
Speed:	294 Mbps
Max Speed:	300 Mbps
Goodput	11.8 Mbps
Usage:	19.2 Kbps
Frames:	240
WLAN:	contractor
AP Name:	AP22
Channel	!
SNR Quality	normal
To Client	
Frames:	119
Retried Frames:	40%(48/119)
Dropped Frames:	0%(0/119)
From Client	
Frames:	121
Retried:	9%(11/121)

A user\\'s laptop only operates in the 2.4 GHz band and supports 802.11n. This user reports that the network is slow at the cafeteria that is serviced by three APs, and suggests that there might be a problem with the WLAN. The network administrator finds the user in the MM, and obrains the output shown in the exhibit.

What should the network administrator do to optimize the client connection?

A. Disable lower transmit rates in the SSID profile.

B. Change the channel being used in the radio profile.

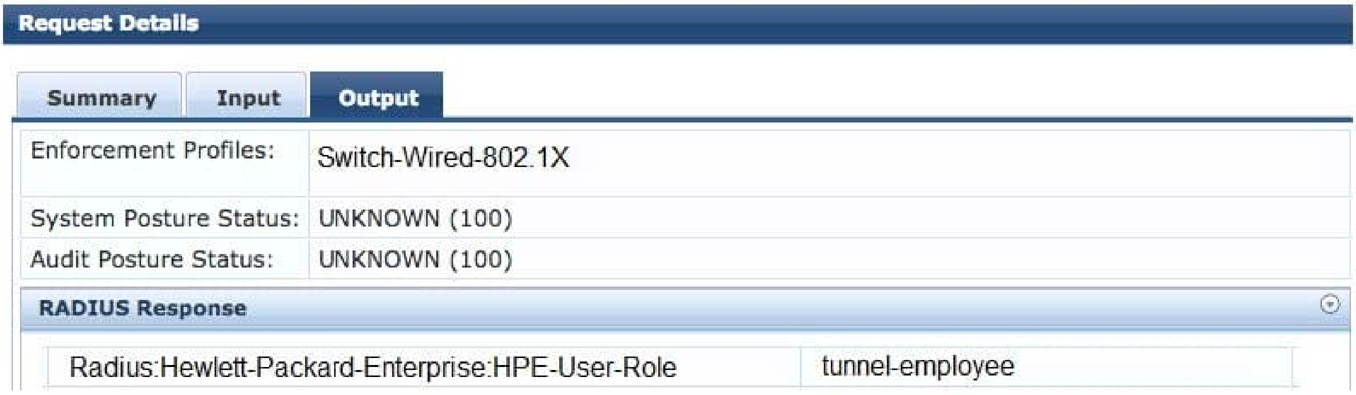
C. Reduce Min/Max channel bandwidth in the radio profile.

D. Reduce Min/Max EIRP in the ARM profile.

Correct Answer: A

QUESTION 12

Refer to the exhibits. Exhibit 1



Request Details

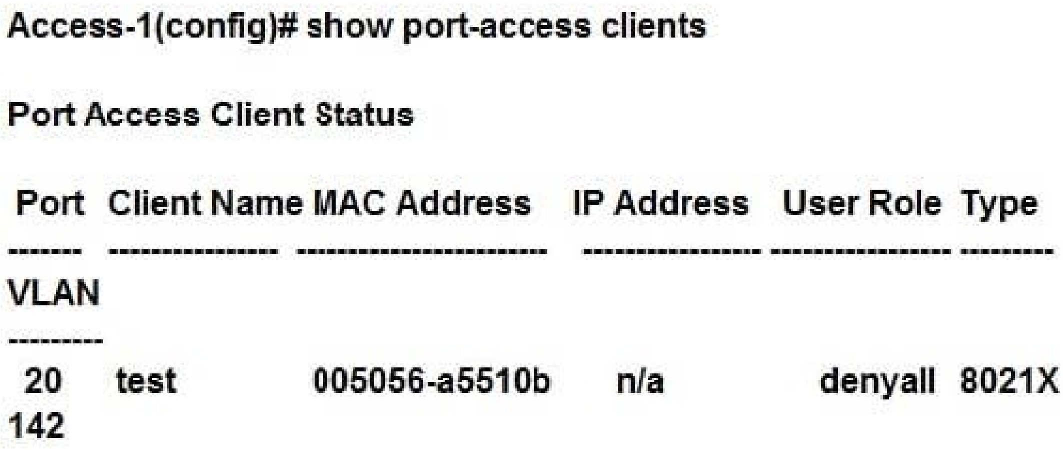
Enforcement Profiles:	Switch-Wired-802.1X
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Hewlett-Packard-Enterprise:HPE-User-Role	tunnel-employee

(A48.01114558)

Exhibit 2



```
Access-1(config)# show port-access clients

Port Access Client Status

 Port  Client Name MAC Address     IP Address   User Role  Type
------- ----------- --------------- ------------ ---------- ---------
VLAN
---------
  20    test         005056-a5510b    n/a          denyall  8021X
142
```

A network administrator deploys role-based tunneled node in a corporate network to unify the security policies enforcement. When users authenticate with 802.1X, ClearPass shows Accept results, and sends the HPE-User-Role attribute as expected. However, the switch always applies the denyall role.

Why does the switch fail to allocate the tunnel-employee role?

A. Denyall is a secondary role contained within tunnel-employee.

B. The switch is not configured with primary tunneled-node user role.

C. The switch is not configured with secondary tunneled-node user role.

D. RADIUS Access Accept messages time out in the switch.

Correct Answer: B