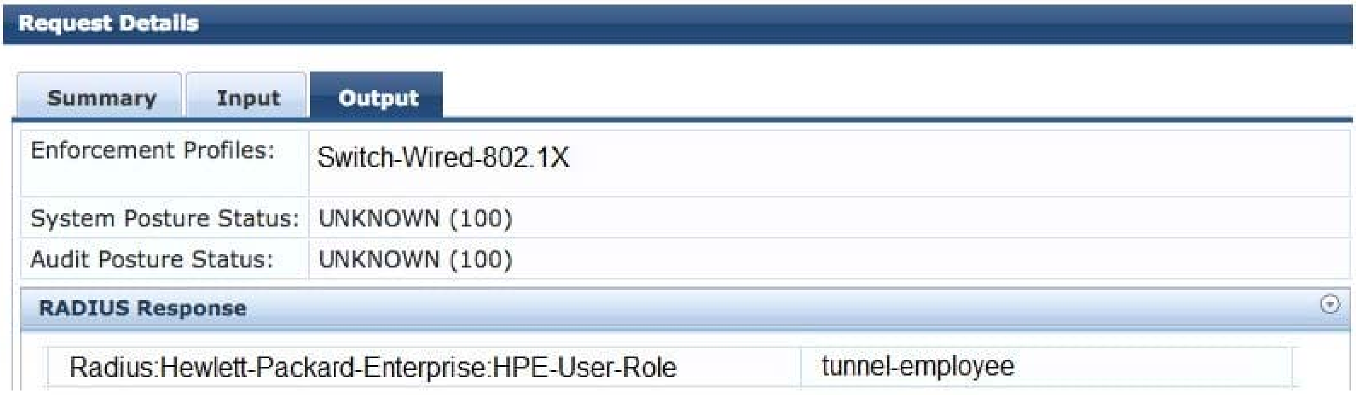
HPE6-A48$^{Q\&As}$

Aruba Certified Mobility Expert 8 Written Exam

Pass HP HPE6-A48 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibits. Exhibit 1



Request Details

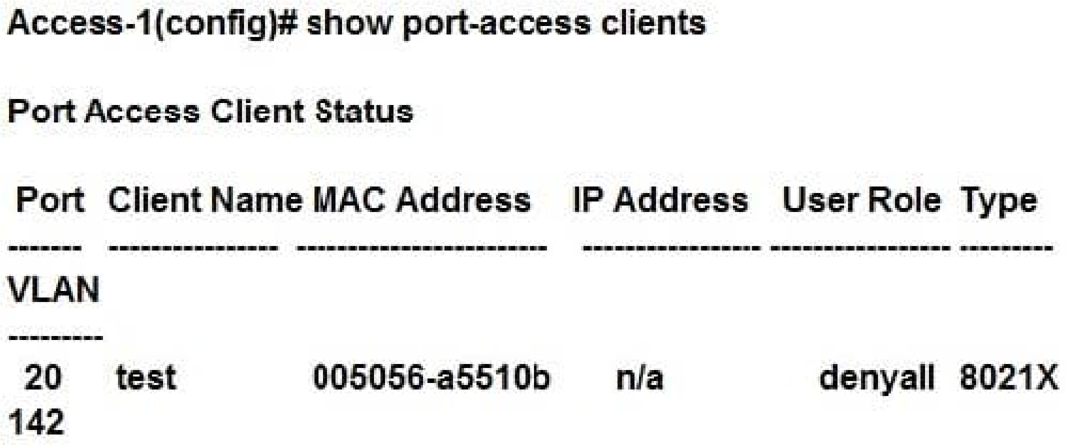
Enforcement Profiles:	Switch-Wired-802.1X
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

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.

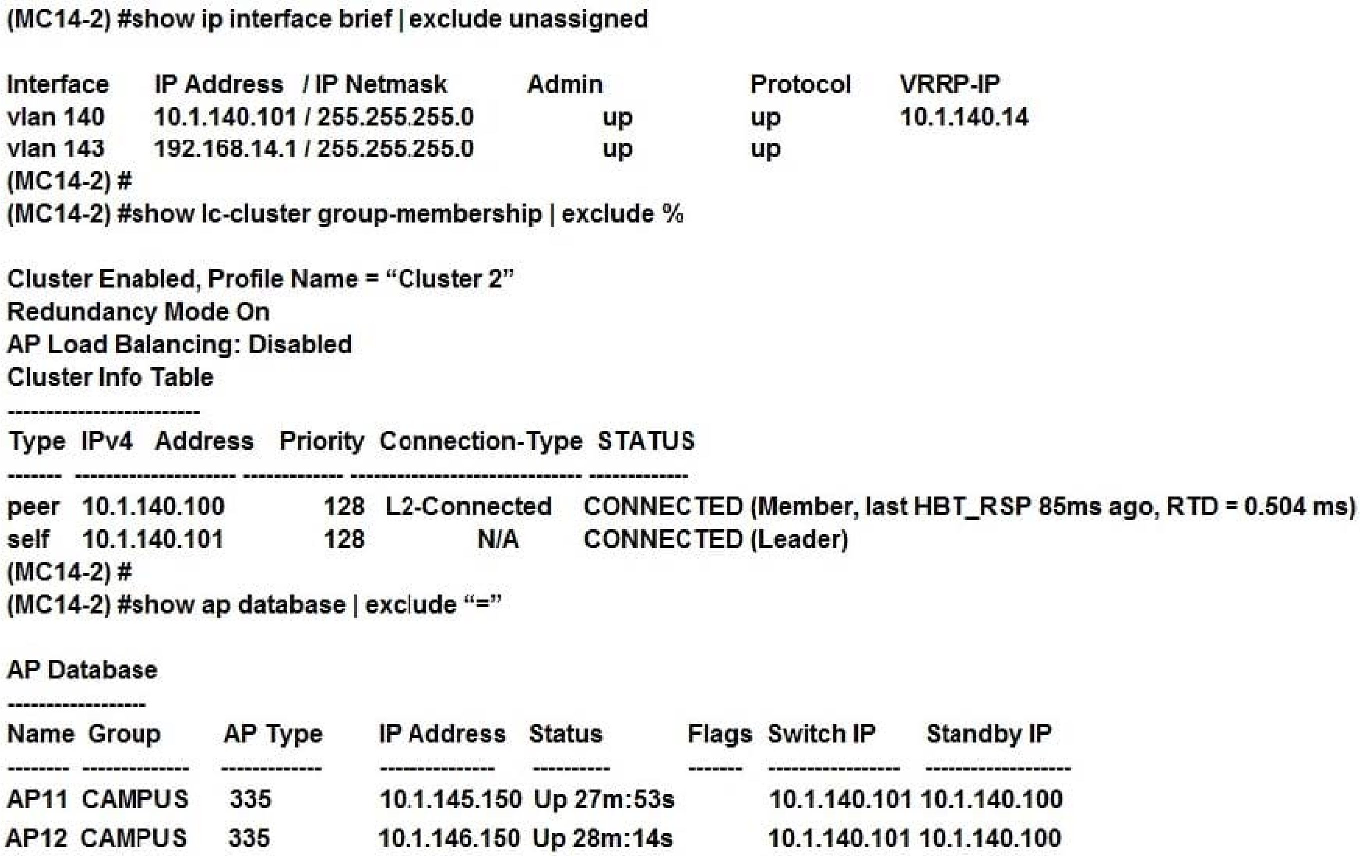
D. RADIUS Access Accept messages time out in the switch.

Correct Answer: B

QUESTION 2

Refer to the exhibits.

Exhibit 1



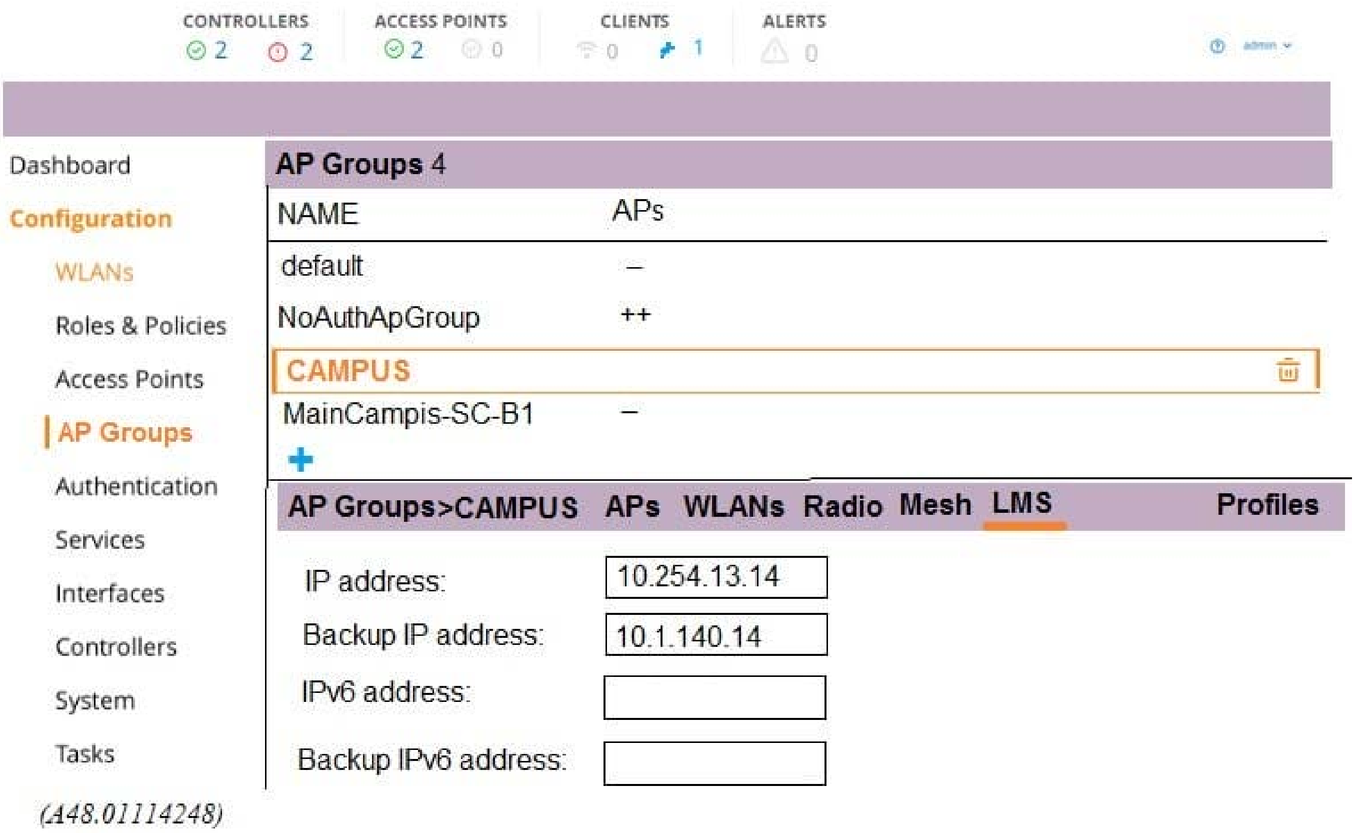
```
(MC14-2) #show ip interface brief | exclude unassigned

Interface    IP Address   / IP Netmask       Admin          Protocol     VRRP-IP
vlan 140     10.1.140.101 / 255.255.255.0         up        up           10.1.140.14
vlan 143     192.168.14.1 / 255.255.255.0         up        up
(MC14-2) #
(MC14-2) #show lc-cluster group-membership | exclude %

Cluster Enabled, Profile Name = "Cluster 2"
Redundancy Mode On
AP Load Balancing: Disabled
Cluster Info Table
------------------------
Type  IPv4   Address   Priority  Connection-Type  STATUS
------- -------------------- ------------ ----------------------------- ------------
peer   10.1.140.100          128   L2-Connected    CONNECTED (Member, last HBT_RSP 85ms ago, RTD = 0.504 ms)
self   10.1.140.101          128            N/A    CONNECTED (Leader)
(MC14-2) #
(MC14-2) #show ap database | exclude "="

AP Database
-----------------
Name  Group       AP Type       IP Address   Status           Flags  Switch IP      Standby IP
-------- ------------- ------------- -------------- ---------- ------- ---------------- ------------------
AP11  CAMPUS       335          10.1.145.150  Up 27m:53s             10.1.140.101 10.1.140.100
AP12  CAMPUS       335          10.1.146.150  Up 28m:14s             10.1.140.101 10.1.140.100
```

Exhibit 2



AP Groups 4

NAME	APs
default	–
NoAuthApGroup	++
CAMPUS	
MainCampis-SC-B1	–

AP Groups>CAMPUS APs WLANs Radio Mesh LMS Profiles

IP address: 10.254.13.14

Backup IP address: 10.1.140.14

IPv6 address:

Backup IPv6 address:

A network administrator deploys a test environment with two Mobility Masters (MMs), two two-member Mobility Controller (MC) clusters, and two CAPs, with the intention of testing several ArubaOS features, Cluster members run VRRP for AP boot redundancy. Based on the information shown in the exhibits, what is the current status of the APs?

A. APs are currently communicating with LMS IP, and 10.1.140.100 is S-AAC.

B. APs are currently communicating with BLMS IP, and 10.1.140.101 is A-AAC.

C. APs are currently communicating with BLMS IP, and 10.1.140.101 is S-AAC.

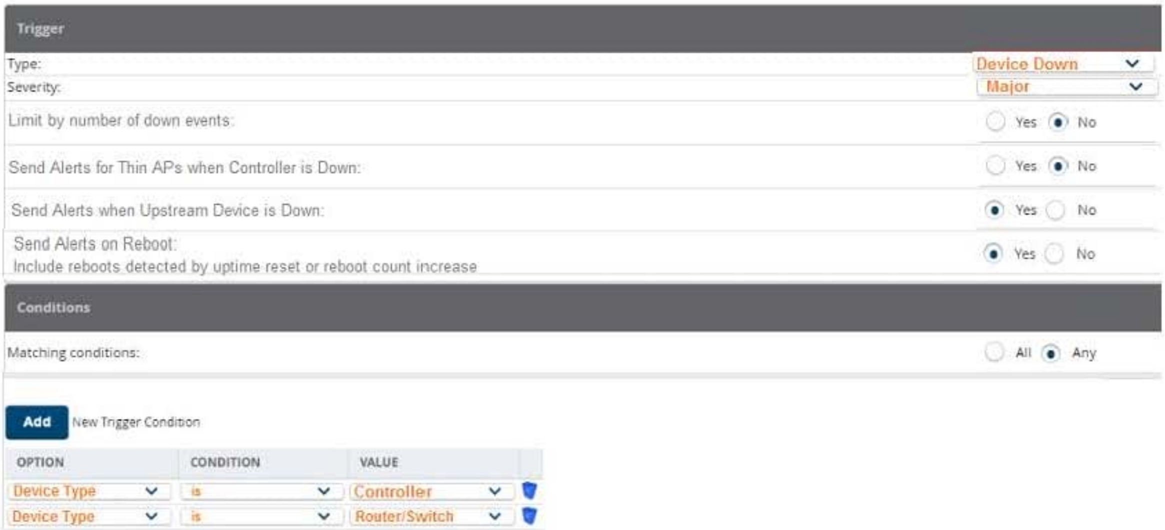
D. APs are currently communicating with BLMS IP, and 10.1.140.100 is A-AAC.

Correct Answer: B

QUESTION 3

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

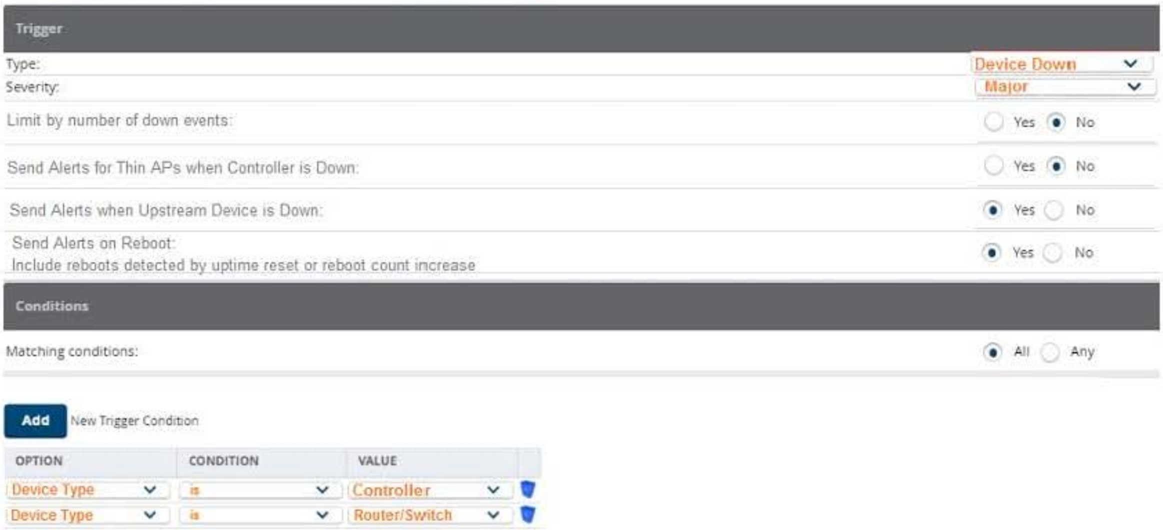
Conditions

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

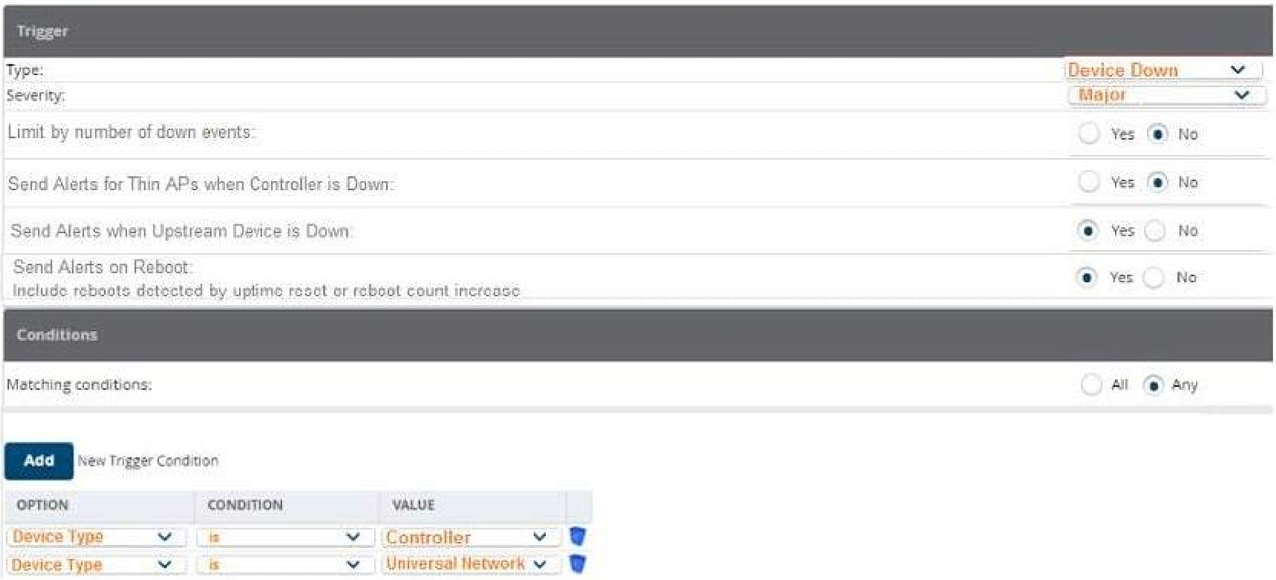
Conditions

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: ● Yes ○ No
Include reboots detected by uptime reset or reboot count increase

Conditions

Matching conditions: ○ All ● Any

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

A. Option A

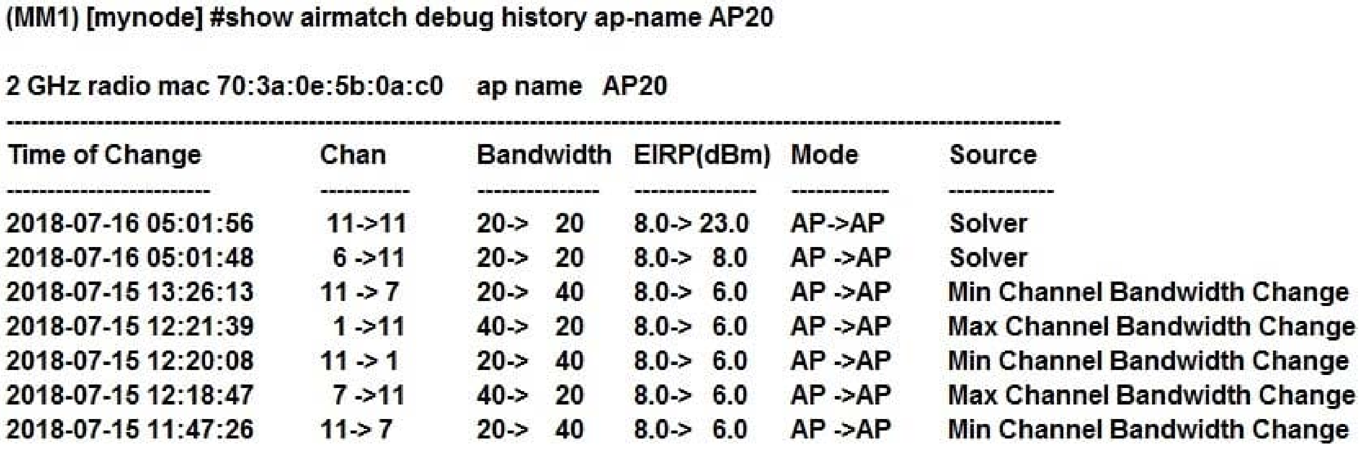
B. Option B

C. Option C

Correct Answer: B

QUESTION 4

Refer to the exhibit.



```
(MM1) [mynode] #show airmatch debug history ap-name AP20

2 GHz radio mac 70:3a:0e:5b:0a:c0    ap name   AP20
---------------------------------------------------------------------------------------------------------------
Time of Change          Chan        Bandwidth  EIRP(dBm)  Mode       Source
--------------------    ----------  ---------  ---------  ---------  -----------
2018-07-16 05:01:56      11->11     20->  20   8.0-> 23.0  AP->AP    Solver
2018-07-16 05:01:48       6 ->11    20->  20   8.0->  8.0  AP ->AP   Solver
2018-07-15 13:26:13     11 -> 7     20->  40   8.0->  6.0  AP ->AP   Min Channel Bandwidth Change
2018-07-15 12:21:39      1 ->11     40->  20   8.0->  6.0  AP ->AP   Max Channel Bandwidth Change
2018-07-15 12:20:08     11 -> 1     20->  40   8.0->  6.0  AP ->AP   Min Channel Bandwidth Change
2018-07-15 12:18:47      7 ->11     40->  20   8.0->  6.0  AP ->AP   Max Channel Bandwidth Change
2018-07-15 11:47:26     11-> 7      20->  40   8.0->  6.0  AP ->AP   Min Channel Bandwidth Change
```

Help desk staff receive reports from users that there is inefficient wireless service in a location serviced by AP20, AP21, and AP22, and open a ticket. A few hours later, the users report that there is a drastic improvement in service. The staff still wants to determine the cause of the problem so the next day thay start monitoring the tasks.

They access the Mobility Master (MM), and obtain the output shown in the exhibit.

What could be the cause of the problem that the users reported?

A. AirMatch was running an initial incremental optimization.

B. An operator used AirMatch to manually freeze AP channel and power.

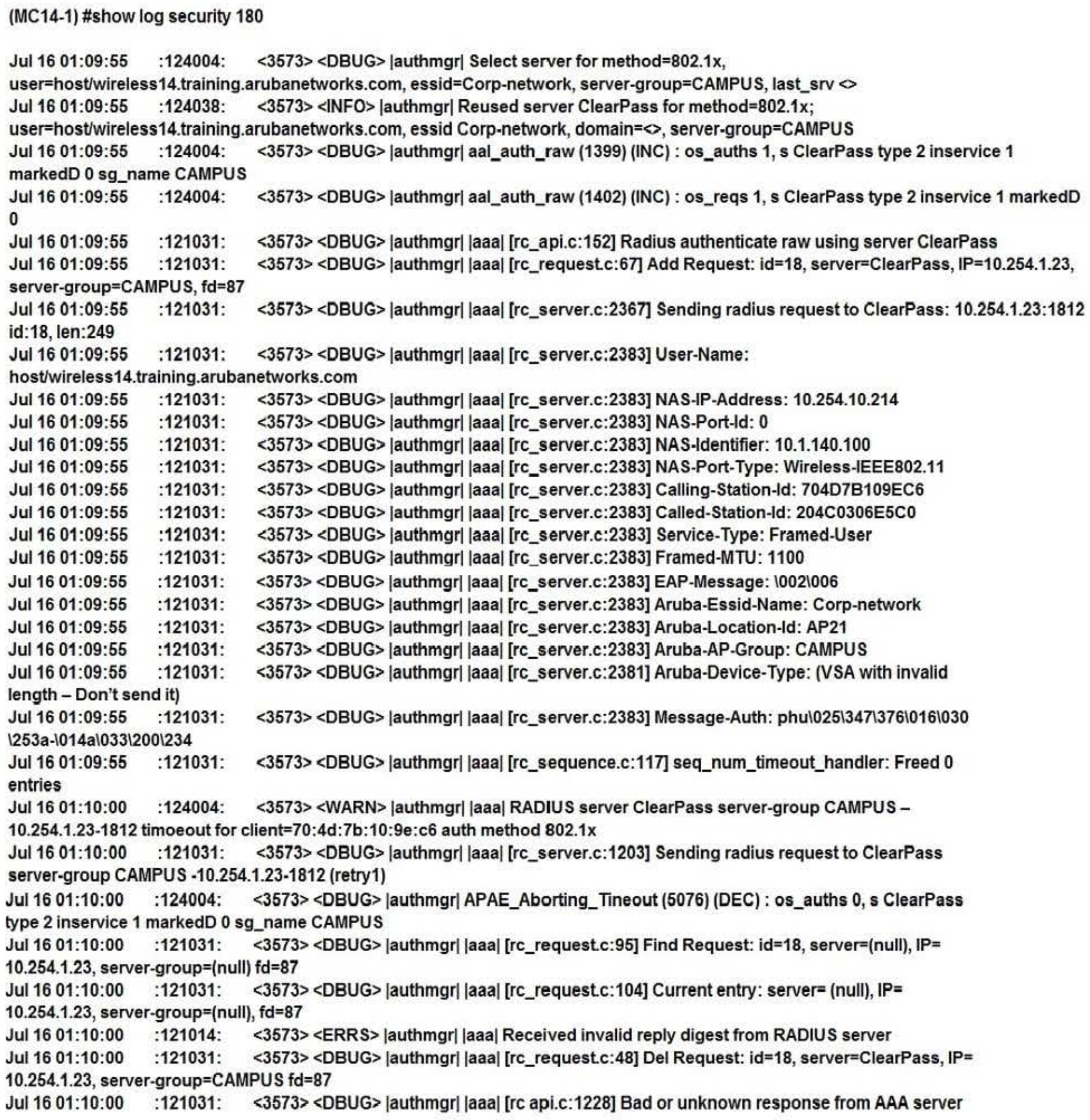
C. An operator manually assigned settings in the radio profile.

D. AirMatch was running a full on-demand optimization.

Correct Answer: B

QUESTION 5

Refer to the exhibit.



```
(MC14-1) #show log security 180

Jul 16 01:09:55     :124004:     <3573> <DBUG> |authmgr| Select server for method=802.1x,
user=host/wireless14.training.arubanetworks.com, essid=Corp-network, server-group=CAMPUS, last_srv <>
Jul 16 01:09:55     :124038:     <3573> <INFO> |authmgr| Reused server ClearPass for method=802.1x;
user=host/wireless14.training.arubanetworks.com, essid Corp-network, domain=<>, server-group=CAMPUS
Jul 16 01:09:55     :124004:     <3573> <DBUG> |authmgr| aal_auth_raw (1399) (INC) : os_auths 1, s ClearPass type 2 inservice 1
markedD 0 sg_name CAMPUS
Jul 16 01:09:55     :124004:     <3573> <DBUG> |authmgr| aal_auth_raw (1402) (INC) : os_reqs 1, s ClearPass type 2 inservice 1 markedD
0
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_api.c:152] Radius authenticate raw using server ClearPass
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=18, server=ClearPass, IP=10.254.1.23,
server-group=CAMPUS, fd=87
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass: 10.254.1.23:1812
id:18, len:249
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] User-Name:
host/wireless14.training.arubanetworks.com
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-IP-Address: 10.254.10.214
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Id: 0
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Identifier: 10.1.140.100
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Type: Wireless-IEEE802.11
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Calling-Station-Id: 704D7B109EC6
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Called-Station-Id: 204C0306E5C0
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Service-Type: Framed-User
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Framed-MTU: 1100
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] EAP-Message: \002\006
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Essid-Name: Corp-network
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Location-Id: AP21
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-AP-Group: CAMPUS
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2381] Aruba-Device-Type: (VSA with invalid
length – Don't send it)
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Message-Auth: phu\025\347\376\016\030
\253a-\014a\033\200\234
Jul 16 01:09:55     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_sequence.c:117] seq_num_timeout_handler: Freed 0
entries
Jul 16 01:10:00     :124004:     <3573> <WARN> |authmgr| |aaa| RADIUS server ClearPass server-group CAMPUS –
10.254.1.23-1812 timoeout for client=70:4d:7b:10:9e:c6 auth method 802.1x
Jul 16 01:10:00     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_server.c:1203] Sending radius request to ClearPass
server-group CAMPUS -10.254.1.23-1812 (retry1)
Jul 16 01:10:00     :124004:     <3573> <DBUG> |authmgr| APAE_Aborting_Tineout (5076) (DEC) : os_auths 0, s ClearPass
type 2 inservice 1 markedD 0 sg_name CAMPUS
Jul 16 01:10:00     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_request.c:95] Find Request: id=18, server=(null), IP=
10.254.1.23, server-group=(null) fd=87
Jul 16 01:10:00     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_request.c:104] Current entry: server= (null), IP=
10.254.1.23, server-group=(null), fd=87
Jul 16 01:10:00     :121014:     <3573> <ERRS> |authmgr| |aaa| Received invalid reply digest from RADIUS server
Jul 16 01:10:00     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc_request.c:48] Del Request: id=18, server=ClearPass, IP=
10.254.1.23, server-group=CAMPUS fd=87
Jul 16 01:10:00     :121031:     <3573> <DBUG> |authmgr| |aaa| [rc api.c:1228] Bad or unknown response from AAA server
```

A network administrator deploys a new WLAN named Corp-Network. The security suite is WPA2 with 802.1X. A new ClearPass server is used as the authentication server. Connection attempts to this WLAN are rejected, and no trace of the attempt is seen in the ClearPass Policy Manager Access Tracker. However, the network administrator is able to see the logs shown in the exhibit.

What must the network administrator do to solve the problem?

A. Add the correct network device IP address in ClearPass.

B. Change the ClearPass server IP address in the MC.

C. Fix the RADIUS shared secret in the MC.

D. Disable machine authentication in the MC and client PC.

Correct Answer: D

Latest HPE6-A48 Dumps HPE6-A48 VCE Dumps HPE6-A48 Practice Test