



HPE6-A48^{Q&As}

Aruba Certified Mobility Expert 8 Written Exam

Pass HP HPE6-A48 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.lead4pass.com/hpe6-a48.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



QUESTION 1

Users run encrypted Skype for Business traffic with no WMM support over an Aruba Mobility Master (MM) Mobility Controller (MC) based network. When voice, video, and application sharing traffic arrive at the wired side of the network, all the flows look alike due the lack of L2 or L3 markings.

How can the network administrator identify these flows and mark QoS accordingly?

A. Confirm the MC is the Openflow controller of the MMs and Openflow is enabled in VAP and the firewall roles. Then enable WMM in a VAP profile.

B. Confirm the MM is the Openflow controller of the MCs and Openflow is enabled in VAP and the firewall roles. Then integrate the MM with the Skype4Business SDN API, and enable the Skype4Business ALG

in the UCC Profiles.

C. Confirm the MC is the OpenFlow controller of the MMs and Openflow is enabled in VAP and the firewall roles. Then enable the Skype4Business ALG in the UCC profiles.

D. Use a media firewall policy that match these three flows, and use permit and TOS actions with 56, 40, and 34 values for voice, video, and application sharing, respectively. Then enable the Skype4Business ALG in the UCC profiles.

Correct Answer: D

QUESTION 2

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.

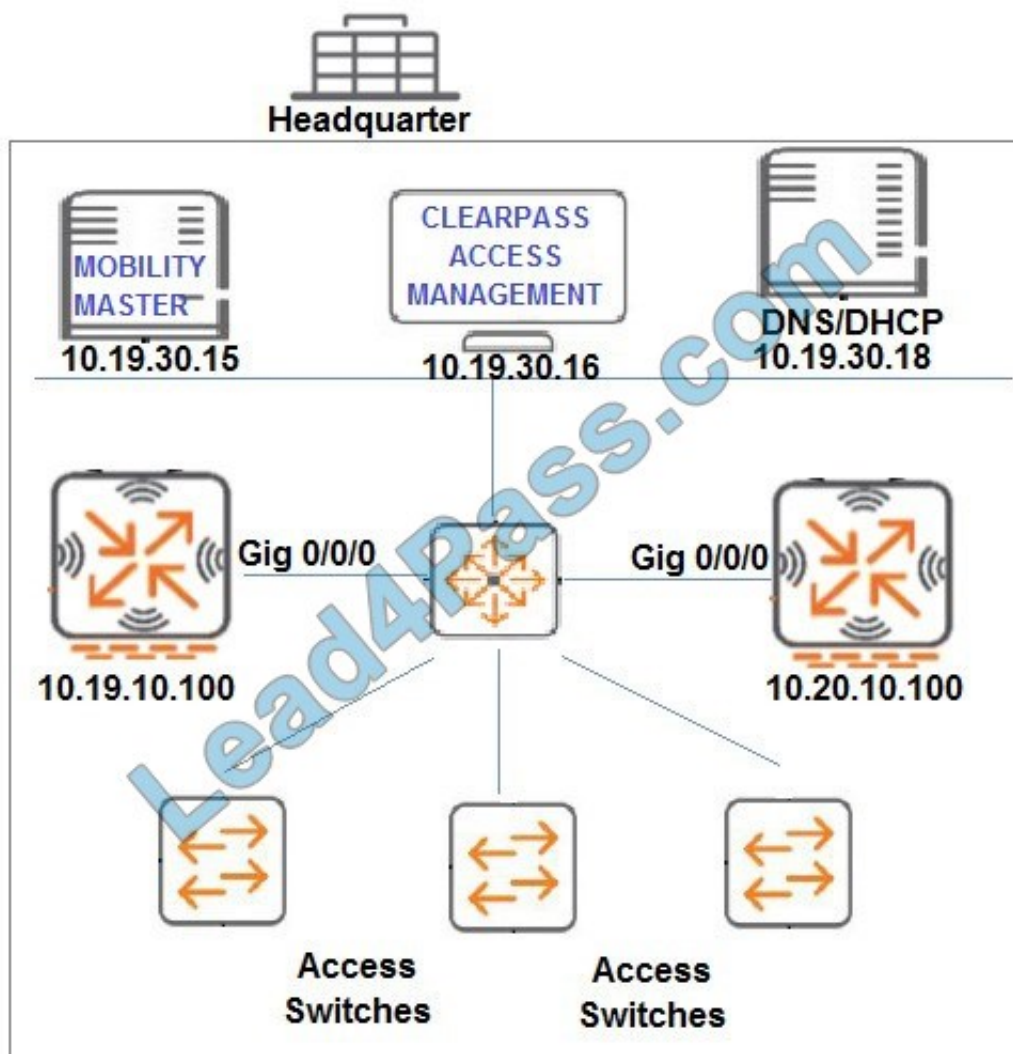
D. Disable Broadcast Multicast Optimization (BCMCO) in the VLAN.

E. Set Video Multicast Rate Optimization (VMRO) in the SSID profile.

Correct Answer: AC

QUESTION 3

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 4

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 5

Refer to the exhibits. Exhibit1

(MC1) (MDC) #show ap database

AP Database

Name	Group	AP Type	IP Address	Status	Flags	Switch IP	Standby IP
AP1	MainCampus-SC-B1	335	10.1.145.150	Up 4h:14m:10s	21	10.1.140.100	10.1.140.101
AP12	CAMPUS	335	10.1.146.150	Up 13m:19s	2	10.1.140.100	10.1.140.101

Flags: 1 = 802.1x, authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1.= 802.1x use factory cert; 2 = Using IKE version 2

B = Built-in AP; C = Cellular RAP; D = Dirty or no config

E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication

G = No such group; I = Inactive; J = USB cert at AP; L = Unlicensed

M = Mesh node

N = Duplicate name; P = PPPoE AP; R = Remote AP; R- = Remote AP requires Auth;

S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode

Y = Mesh Recovery

c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support

i = Indoor; o = Outdoor; s = LACP striping; u = Custom-cert RAP; z = Datazone AP

Total APs:2

Exhibit 2



(MC11) [mynode] #show ap database

AP Database

Name	Group	AP Type	IP Address	Status	Flags	Switch IP	Standby IP
70:3a:0e:cd:b0:a4	default	335	10.1.145.150	Down	2	10.254.13.14	0.0.0.0
a8:bd:27:c5:c3:3a	default	335	10.1.147.2	Down	2	10.254.13.14	0.0.0.0
AP12	CAMPUS	335	10.1.146.150	Up 21m:37s	2z	10.254.13.14	0.0.0.0

Based on outputs shown in the exhibits, what is the reason that AP12 is seen by two different controllers?

- A. AP12 connects to a high availability group. MC1 is the active controller, and MC11 is the standby controller.
- B. AP12 is a multizone AP. MC1 is part of the primary zone, and MC11 is part of the datazone.
- C. AP12 connects to an MC cluster. MC1 is the A-AAC, and MC2 is S-AAC.
- D. AP12 is in the middle of the boot process. MC1 is the master IP controller, and MC11 is the LMS IP controller.

Correct Answer: B

QUESTION 6

A software development company has 700 employees who work from home. The company also has small offices located in different cities throughout the world. During working hours, they use RAPs to connect to a datacenter to upload software code as well as interact with databases.

In the past two months, brief failures have occurred in the 7240XM Mobility Controller (MC) that runs ArubaOS 8.3 and terminates the RAPs. These RAPs disconnect, affecting the users connected to the RAPs. This also causes problems with code uploads and database synchronizations. Therefore, the company decides to add a second 7240XM controller for redundancy.

How should the network administrator deploy both controllers in order to provide redundancy while preventing failover events from disconnecting users?

- A. Connect both controllers with common VLANs, and create an L2-connected cluster using public addresses in the internet VLAN.
- B. Connect both controllers with common VLANs, and create an HA fast failover group with public addresses in the internet VLAN.
- C. Connect both controllers with different VLANs, and create an L2-connected cluster using private addresses in the internet VLAN.
- D. Connect both controllers with common VLANs, and configure LMS/BLMS values equal to public addresses in the internet VLAN.

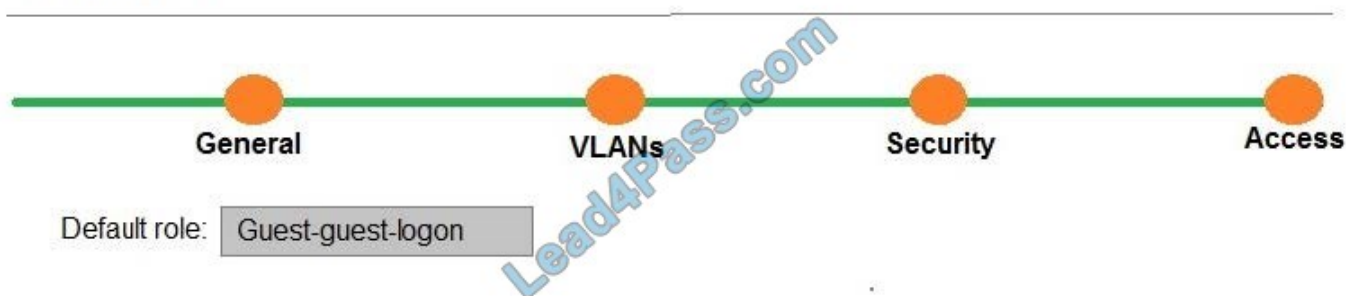
Correct Answer: A

QUESTION 7



Refer to the exhibit.

New WLAN



(A48.01114253)

A network administrator completes the task to create a WLAN, as shown in the exhibit. The network administrator selects the options to use guest as primary usage and Internal captive portal with authentication in the security step. Next, the network administrator creates a policy that denies access to the internal network.

Which additional step must the network administrator complete in order to prevent authenticated users from reaching internal corporate resources while allowing Internet access?

- A. Apply the policy on the guest-guest-logon role.
- B. Apply the policy on the authenticated role.
- C. Apply the policy on the guest role.
- D. Create a policy that permits dhcp, dns, and http access.

Correct Answer: D

QUESTION 8

Refer to the exhibits.

Exhibit 1

**CONTROLLERS** | **ACCESS POINTS** | **CLIENTS** | **ALERTS**

1 | 1 | 2 | 0 | 1 | 0 | 0

> **MC14-1**

Name:	MC14-1
Reachability:	Unreachable
Health:	Good
Uptime:	-
Model:	Aruba7030-US
Serial Number:	CRDD12919
Country:	-
Group:	md > Westcoast > SantaClara > Building1
Configuration State:	-
Configuration Version:	-

(A48.01114452)

Exhibit 2 A network administrator adds a new Mobility Controller (MC) to the production Mobility Master (MM) and deploys APs that start broadcasting the employees SSID in the West wing of the building. Suddenly, the employed report client disconnects. When accessing the MM the network administrator notices that the MC is unreachable, then proceeds to access the MC's console and obtains the outputs shown in the exhibits.



top2 – 22:23:48 up 6:11, 0 users, load average: 0.11, 0.10, 0.08

Tasks: 202 total, 2 running, 198 sleeping, 0 stopped, 2 zombie

Cpu(s): 1.2%us, 2.9%sy, 0.2%ni, 95.6%id, 0.1wa, 0.0%hi, 0.1%si, 0.0%st

Mem: 3085600k total, 1831312k used, 1254288k free, 19488k buffers

Swap: 1048544k total, 0k used, 1048544k free, 889680k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3556	root	20	0	147m	79m	15m	R	85	2.7	0:39.54	profmgr
3017	root	20	0	9472	3952	2656	S	23	0.1	1:30.44	syslogd
3565	root	10	-10	132m	36m	13m	S	15	1.2	0:37.09	auth
4007	root	20	0	68208	8896	5920	S	10	0.3	0:23.41	ofa
3497	root	20	0	334m	137m	10m	S	6	4.6	11:31.80	fpapps
3894	root	20	0	124m	23m	5472	S	6	0.8	0:10.00	dds
4125	root	20	0	52640	6496	3296	S	6	0.2	0:28.97	vrrp
13	root	20	0	0	0	0	S	4	0.0	0:02.05	events/1
3583	root	20	0	173m	25m	9696	S	4	0.8	1:47.79	stm
12505	root	20	0	3104	1680	1248	R	4	0.1	0:00.03	top2
3511	root	20	0	51088	6288	3712	S	2	0.2	0:04.90	pim
3807	root	20	0	220m	71m	5568	S	2	2.4	0:18.20	fw_visibility
1	root	20	0	4160	1104	912	S	0	0.0	0:03.13	init
2	root	20	0	0	0	0	S	0	0.0	0:00.00	kthreadd

What should the network administrator do next to solve the current problem?

- A. Decommission the MC from the MM, and add it again.
- B. Open a TAC case, and send the output of tar crash.
- C. Verify the license pools in the MM.
- D. Kill two zombie processes, then reboot the MC.

Correct Answer: D

QUESTION 9

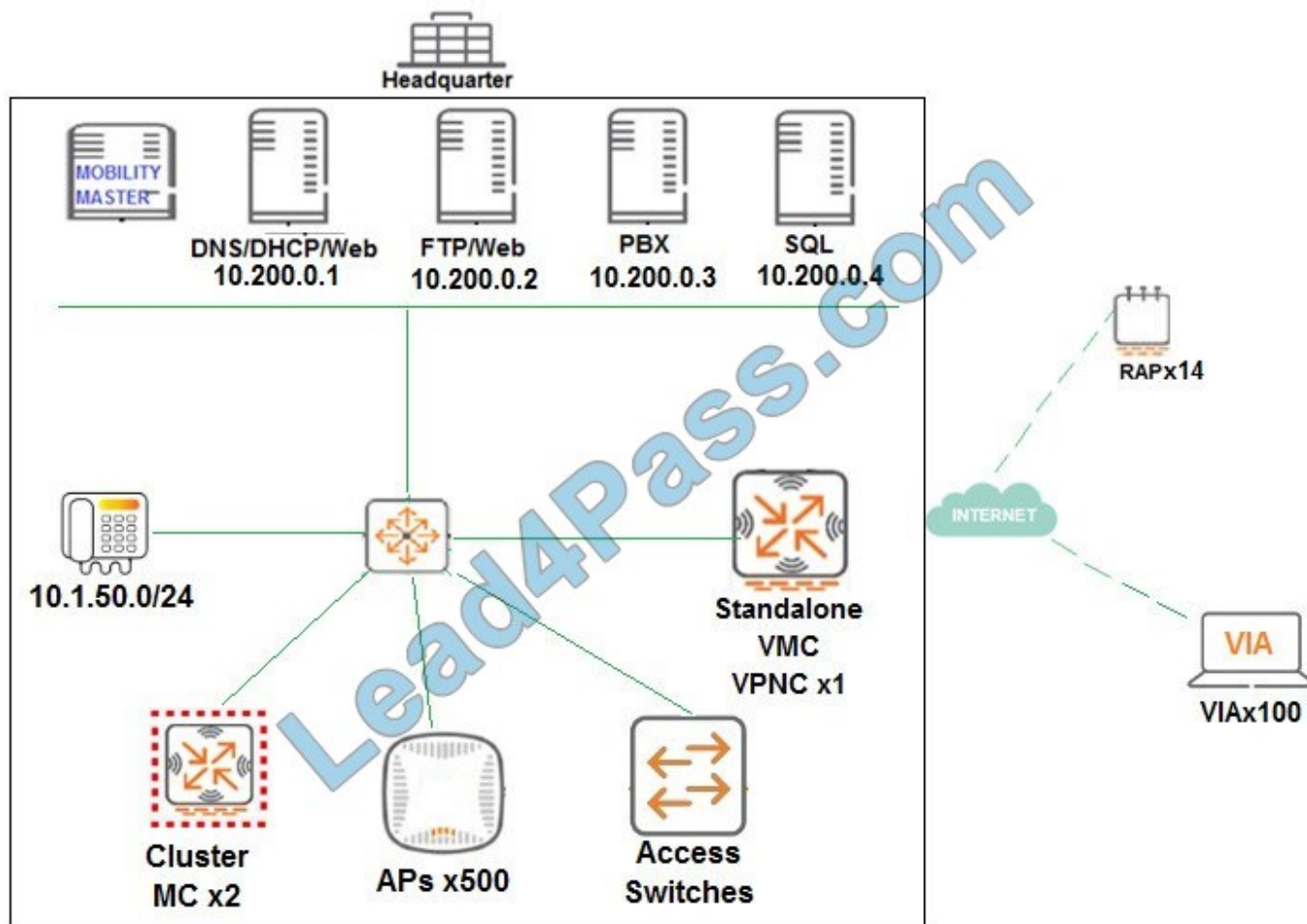
A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM) Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access. Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ. Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment. Local Internet access should be granted.



Refer to the exhibit.



Refer to the scenario and the exhibit.

What is the minimal license capacity in use to support this proposal?



- ☐ A.

<u>License</u>	<u>Number</u>
MM-VA	502
Access Points	514
PEF	514
RF Protect	514
VIA	100
- ☐ B.

<u>License</u>	<u>Number</u>
MM-VA	503
MC-VA	14
Access Points	514
PEF	514
VIA	100
- ☐ C.

<u>License</u>	<u>Number</u>
MM-VA	517
MC-VA	114
Access Points	514
PEF	514
VIA	100
- ☐ D.

<u>License</u>	<u>Number</u>
MM-VA	502
MC-VA	14
Access Points	514
PEF	514
RF Protect	500
VIA	100

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

QUESTION 10

A foreign exchange broker in a shared office space uses an Aruba Mobility Master (MM)-Mobility Controller (MC) architecture along with ClearPass and AirWave. The corporate network is FXBroker121, but users report that they cannot access the FXBroker111 SSID. The team suspects that a rogue AP is in place and a malicious user tried to disguise the WLAN name.

How can the organization's network administrator identify and locate the potential rogue AP?

- A. Create an AirWave RAPIDS rule with a Suspected Rogue classification and the SSID Matches FXBroker111 condition, then access any RAPID List entry that matches the rule and click on Location.
- B. Use ClearPass Event viewer and search for entries with the FXBroker111 Aruba-Essid-Name VSA attribute, then obtain the value of the Aruba-AP-Group attribute.
- C. Use ClearPass Event viewer and search for entries with the FXBroker111 Aruba-Essid-Name VSA attribute, then obtain the value of the Aruba-Location-id attribute.
- D. Create an AirWave RAPIDS rule with a Suspected Rogue classification and the SSID Does Not Match FXBroker121 condition, then access any RAPIDS List entry that matches the rule and click on Location.

Correct Answer: B

QUESTION 11

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  78:4d:7b:10:9e:c6  it      guest      00:00:48      8021x-User      AP12      Wireless      Corp-employee/78:3a:8e:5b:6a:d2/a-VHT      Corp-Network      tunnel      Win
10      WIRELESS
```

```
User Entries: 1/1
Curr/Cum Alloc:3/39 Free:0/36 Dym: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> <DEBUG> [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> <DEBUG> [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> <DEBUG> [authmgr] [aaa] [rc_api.c:152] Radius
authenticate raw using server ClearPass.23
Jul 4 17: 32:15 :124004: <3553> <DEBUG> [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> <DEBUG> [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> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] User Name:
it
Jul 4 17: 32:15 :124004: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] NAS-IP-
Address: 10.254.10.214
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] NAS-Port-
Id: 0
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] NAS-
Identifier: 10.1.140.101
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] NAS-Port-
Type: Wireless-IEEE802.11
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] Calling-
Station-Id: 704D7B109EC6
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] Called-
Station-Id: 204C0306E790
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] Service-
Type: Framed-User
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] Framed-MTU:
1100
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] EAP-Message:
\002\011
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] State:
AFMAZwACACAG9IAfvORnQM2udKK13smu/12DA==
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] Aruba-Essid-
Name: Corp-employee
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] Aruba-
Location-Id: AP22
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] Aruba-AP-
Group: CAMPUS
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_server.c:2383] Aruba-
Device-Type: Win 10
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [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> <DEBUG> [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> <DEBUG> [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> <DEBUG> [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> <DEBUG> [authmgr] [aaa] [rc_api.c: 1228]
Authentication Successful
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_api.c: 1230] RADIUS
RESPONSE ATTRIBUTES
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_api.c: 1245]
Filter-Id: it-role
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_api.c: 1245]
{Microsoft} MS-MPPE-Recv-Key: \222\331\207\347\242[0*;\255gS\262\276u\302\205\264^"
\207\271Q\270E\3120<\2
04R\370\011\317S\007\275\203\302: \201\360\002\307B\305\222\032\240\317\340
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [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> <DEBUG> [authmgr] [aaa] [rc_api.c: 1245]
4\2264 j00? \177Y\325\331/\226\366\325\315z\342[\346\343?o\241\0151
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_api.c: 1245] EAP-
Message: \003\011
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_api.c: 1245] User-
Name: it
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [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> <DEBUG> [authmgr] [aaa] [rc_api.c: 1245]
FW_RADIUS_ID: \026
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_api.c: 1245] Rad-Length:
231
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_api.c: 1245]
FW_RADIUS_CODE: \002
Jul 4 17: 32:15 :121031: <3553> <DEBUG> [authmgr] [aaa] [rc_api.c: 1245]
FW_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.

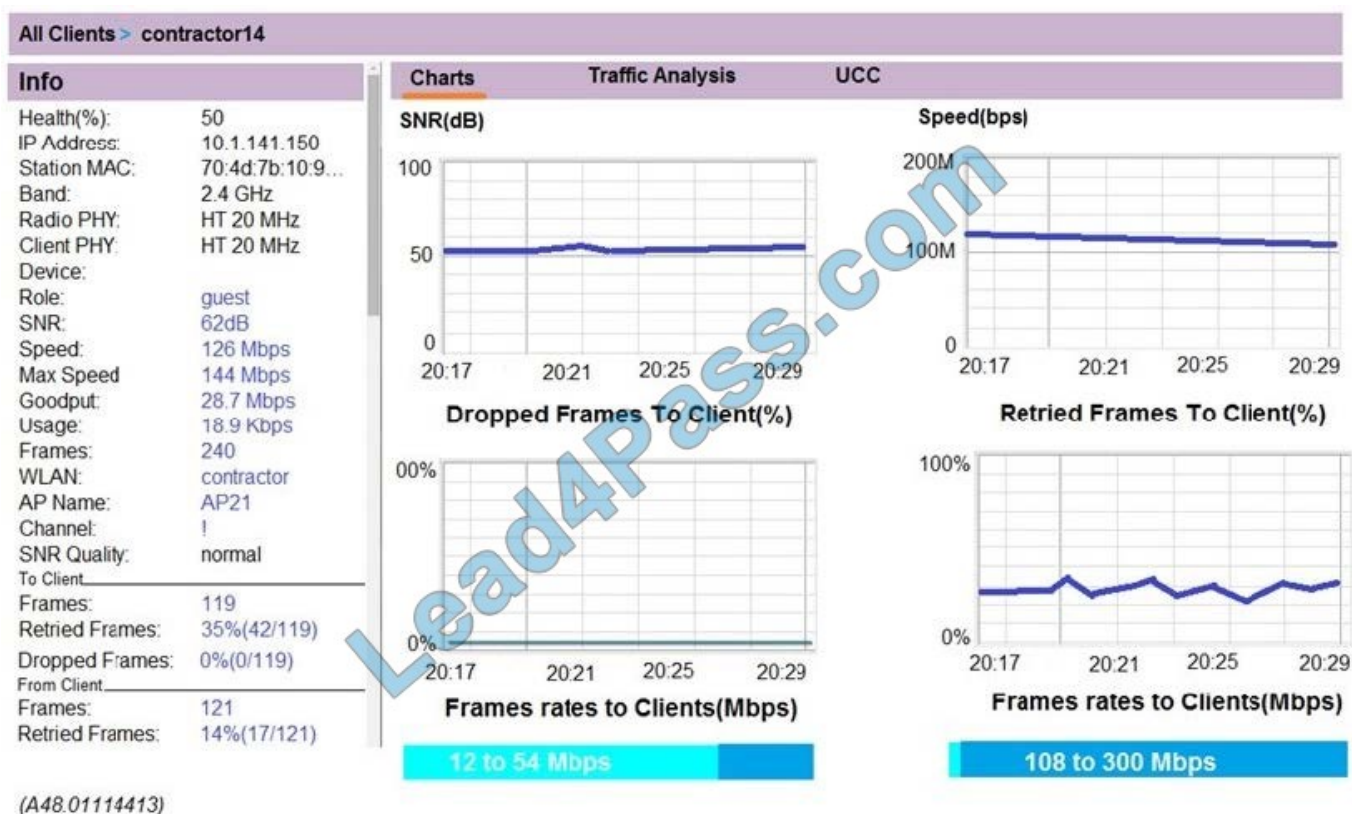
Which configuration is required to map the users into the proper role, based on standard attributes returned by the RADIUS server in the Access Accept message?

- 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 12

Refer to the exhibit.



A user reports show response time to a network administrator and suggests that there might be a problem with the WLAN. The user's laptop supports 802.11n in the 2.4 GHz band only. The network administrator finds the user on the Mobility Master (MM) and reviews the output shown in the exhibit.

What can the network administrator conclude after analyzing the data?

- A. Client health is low, and retried frames are high. It is possible there is high channel utilization.

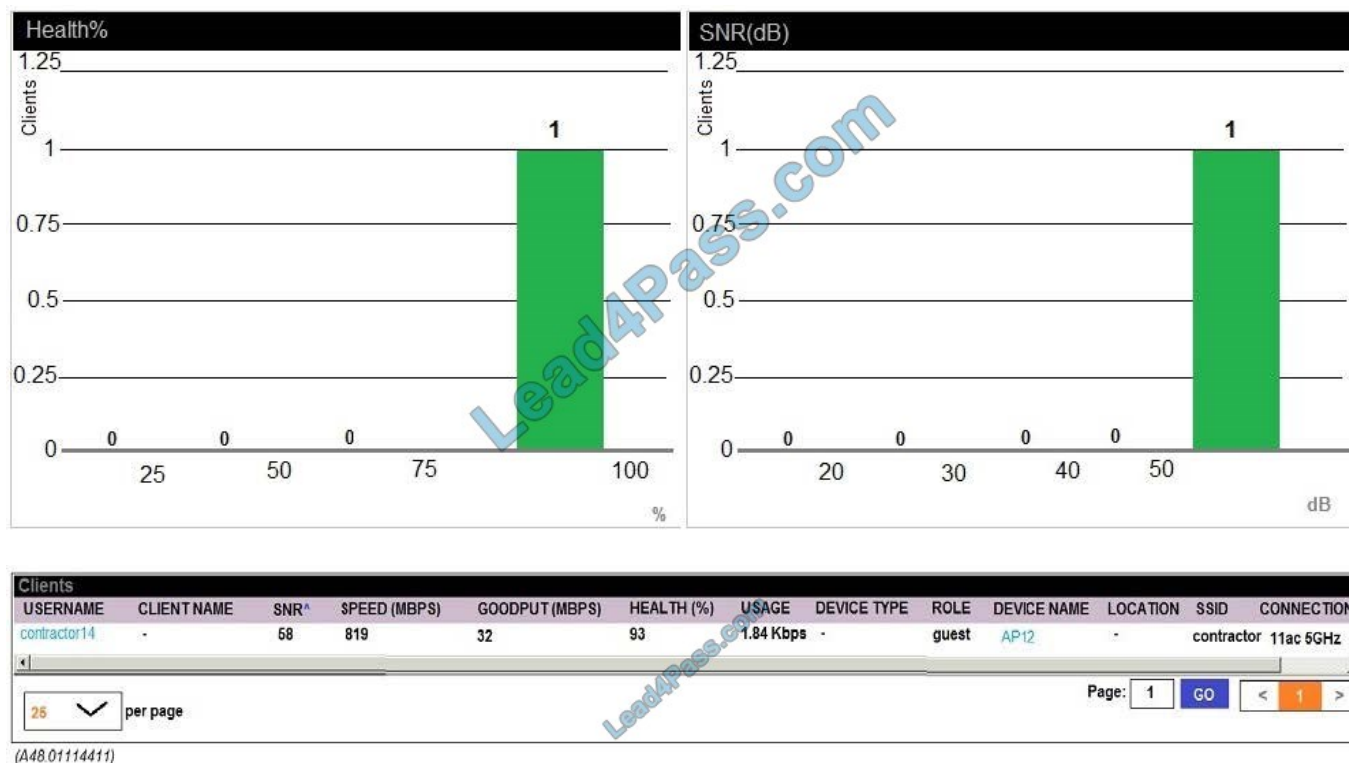


- B. Client health is low, but SNR is high. It is possible data in the dashboard is not accurate and needs to be updated.
- C. The speed is good. Client health seems to be related to a problem with the client NIC.
- D. The network is low because of low SNR. TX power must be increased in both the client and the AP.

Correct Answer: B

QUESTION 13

Refer to the exhibit.



A network administrator receives a call from a contractor that was recently given wireless access to the network. The user reports that the response time is slow and suggests there might be a problem with the WLAN. The network administrator checks RF performance in AirWave to find the user and sees the output shown in the exhibit.

What can the network administrator conclude after analyzing the data?

- A. Client health and CNR are high, therefore, it is unlikely the client is experiencing an RF-related issue.
- B. Goodput is low in relation to connection speed, which suggests a channel with high utilization, another channel should be used.
- C. Client health and SNR are high but usage is low; therefore, there might be packet drops.
- D. Client health is low, which suggests that there are packet drops and collisions in the RF environment.

Correct Answer: B



VCE & PDF

Lead4Pass.com

<https://www.lead4pass.com/hpe6-a48.html>

2022 Latest lead4pass HPE6-A48 PDF and VCE dumps Download

[Latest HPE6-A48 Dumps](#)

[HPE6-A48 VCE Dumps](#)

[HPE6-A48 Braindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.	 Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.	 Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © lead4pass, All Rights Reserved.