



# HPE6-A48<sup>Q&As</sup>

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.geekcert.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**

Refer to the exhibits. Exhibit 1

(MM1) [mynode] #show switches

All Switches

IP Address Config ID	Ipv6 Address	Name	Location	Type	Model	Version	Status	Configuration State	Config Sync Time (sec)
10.254.10.14 53	None	MM1	Building1.floor1	master	ArubaMM-VA	8.2.1.0_64044	up	UPDATE SUCCESSFUL	0
10.254.10.14 0	None	MC1	Building1.floor1	MD	Aruba7030	8.2.1.0_64044	up	CONFIG ROLLBACK	0
10.254.10.114 53	None	MM2	Building1.floor1	standby	ArubaMM-VA	8.2.1.0_64044	up	UPDATE SUCCESSFUL	0

Total Switches:3

(MM1) [mynode] #

(MM1) [mynode] #show switches

All Switches

IP Address Config ID	Ipv6 Address	Name	Location	Type	Model	Version	Status	Configuration State	Config Sync Time (sec)
10.254.10.14 53	None	MM1	Building1.floor1	master	ArubaMM-VA	8.2.1.0_64044	up	UPDATE SUCCESSFUL	0
10.1.140.100 0	None	MC1	Building1.floor1	MD	Aruba7030	8.2.1.0_64044	down	CONFIG ROLLBACK	0
10.254.10.114 53	None	MM2	Building1.floor1	standby	ArubaMM-VA	8.2.1.0_64044	up	UPDATE SUCCESSFUL	0

Total Switches: 3

(MM1) [mynode] #

(MM1) [mynode] #encrypt disable

(MM1) [mynode] #show running-config | include localip

Building Configuration...

localip 10.1.140.101 ipsec Aruba123

localip 10.1.140.100 ipsec Aruba 123

localip 10.200.0.20 ipsec 1234567890

localip 10.1.140.102 ipsec Aruba123

(MM1) [mynode] #

(MM1) [mynode] #cd MC1

(MM1) [20:4c:03:06:e5:c0] #show configuration effective | include masterip

masterip 10.254.10.214 ipsec aruba123

controller-ip "masterip" 6633

Exhibit 2 Exhibit 3



(MM1) [20:4c:03:06:e5:c0] #show log system 15

```
Jun 26 13:51:40 :357002: <6573> <WARN> |cfgdist| freelc_node:355 (TID:6573) Status of 10.1.140.100
(20:4c:03:06:e5:c0) is now DOWN
Jun 26 13:51:50 :357002: <6574> <WARN> |cfgdist| handle_read:702 (TID:6574) Status of ::ffff:10.1.140
(20:4c:03:06:e5:c0) is now UP
Jun 26 13:51:50 :371012: <5733> <ERRS> |profmgr| |multiversion| |Adding device 20:4c:03:06:e5:c0 with version
8_2_1_0]
Jun 26 13:52:10 :357002: <6574> <ERRS> |cfgdist| handle_setupconfig:452 (TID:6574) Setup config not received
from device for 10.1.149.100 (20:
4c:03:06:e5:c0) fd(146)
Jun 26 13:52:10 :357002: <6574> <WARN> |cfgdist| freelc_node:355 (TID:6574) Status of 10.1.140.100
(20:4c:03:06:e5:c0) is now DOWN
Jun 26 13:52:20 :357002: <6575> <WARN> |cfgdist| handle_read:702 (TID:6575) Status of ::ffff:10.1.140.100
(20:4c:03:06:e5:c0) is now UP
Jun 26 13:52:20 :371012: <5733> <ERRS> |profmgr| |multiversion| |Adding device 20:4c:03:06:e5:c0 with version
8_2_1_0]
Jun 26 13:52:40 :357002: <6575> <ERRS> |cfgdist| handle_setupconfig:452 (TID:6575) Setup config not received
from device for 10.1.149.100 (20:
4c:03:06:e5:c0) fd(146)
Jun 26 13:52:40 :357002: <6575> <WARN> |cfgdist| freelc_node:355 (TID:6575) Status of 10.1.140.100
(20:4c:03:06:e5:c0) is now DOWN
Jun 26 13:52:50 :357002: <6576> <WARN> |cfgdist| handle_read:702 (TID:6576) Status of ::ffff:10.1.140.100
(20:4c:03:06:e5:c0) is now UP
Jun 26 13:52:50 :371012: <5733> <ERRS> |profmgr| |multiversion| |Adding device 20:4c:03:06:e5:c0 with version 8
_2_1_0]
Jun 26 13:53:10 :357002: <6576> <ERRS> |cfgdist| handle_setupconfig:452 (TID:6576) Setup config not received
from device for 10.1.140.100 (20:
4c:03:06:e5:c0) fd(146)
Jun 26 13:53:10 :357002: <6576> <WARN> |cfgdist| freelc_node:355 (TID:6576) Status of 10.1.140.100
(20:4c:03:06:e5:c0) is now DOWN
Jun 26 13:53:20 :357002: <6577> <WARN> |cfgdist| handle_read:702 (TID:6577) Status of ::ffff:10.1.140.100
(20:4c:03:06:e5:c0) is now UP
Jun 26 13:53:20 :371012: <5733> <ERRS> |profmgr| |multiversion| |Adding device 20:4c:03:06:e5:c0 with version 8
_2_1_0]
```

(MM1) [20:4c:03:06:e5:c0] #





(MC1) #show switches

All Switches

IP Address g ID	IPv6 Address	Name Location	Type	Model	Version	Status	Configuration State	Config Sync	Time (sec)	Conf
10.1.140.100	None	MC1 Building1.floor1	MD	Aruba7030	8.2.1.0_64044	up	CONFIG ROLLBACK	0		0

Total Switches:1

(MC1) #

(MC1)encrypt disable

(MC1) #show running-config | include masterip

Building Configuration ...

masterip 10.254.10.214 ipsec Aruba123

(MC1) #

(MC1) #ping 10.254.10.214

Press 'q' to abort.

Sending 5, 92-byte ICMP Echos to 10.254.10.214, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0.829/1.3608/1.777 ms

(MC1) #show log errorlog 10

```

Jun 26 13:57:50 <cfgm 399816> <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 13:58:00 <cfgm 399816> <3458> <ERRS> |cfgm| Rollback config id 53 as bad
Jun 26 13:58:20 <cfgm 399816> <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 13:58:30 <cfgm 399816> <3458> <ERRS> |cfgm| Rollback config id 53 as bad
Jun 26 13:58:50 <cfgm 399816> <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 13:59:00 <cfgm 399816> <3458> <ERRS> |cfgm| Rollback config id 53 as bad
Jun 26 13:59:20 <cfgm 399816> <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 13:59:30 <cfgm 399816> <3458> <ERRS> |cfgm| Rollback config id 53 as bad
Jun 26 13:59:50 <cfgm 399816> <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 14:00:00 <cfgm 399816> <3458> <ERRS> |cfgm| Rollback config id 53 as bad

```

A network administrator deploys a Mobility Master (MM) pair with the VRRP VIP equal to 10.254.10.214, and attempts to associate MC1 to it. At first, the integration appears to be successful. However after a few minutes the network administrator issues the show switches command and sees that the MC1 is down, even though the device is up and running.

Every time the network administrator reboots the Mobility Controller (MC), the MC shows as being up and then it shows as being down. The network administrator gathers the information shown in the exhibits.

What should the network administrator do to resolve this problem?

- A. Change the localip ipsec key to Aruba123 in the mynode device level from the MM, save, and reboot.
- B. Enable disaster recovery mode in MC1 and change the masterip ipsec key to Aruba 123, save, and reboot.
- C. Change the masterip ipsec key to Aruba123 in the device level from the MM, save, then reboot MC1.
- D. Wipe out the configuration in MC1 and reboot, then run the full-setup configuration dialog all over again.

Correct Answer: B



## QUESTION 2

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 3

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.)

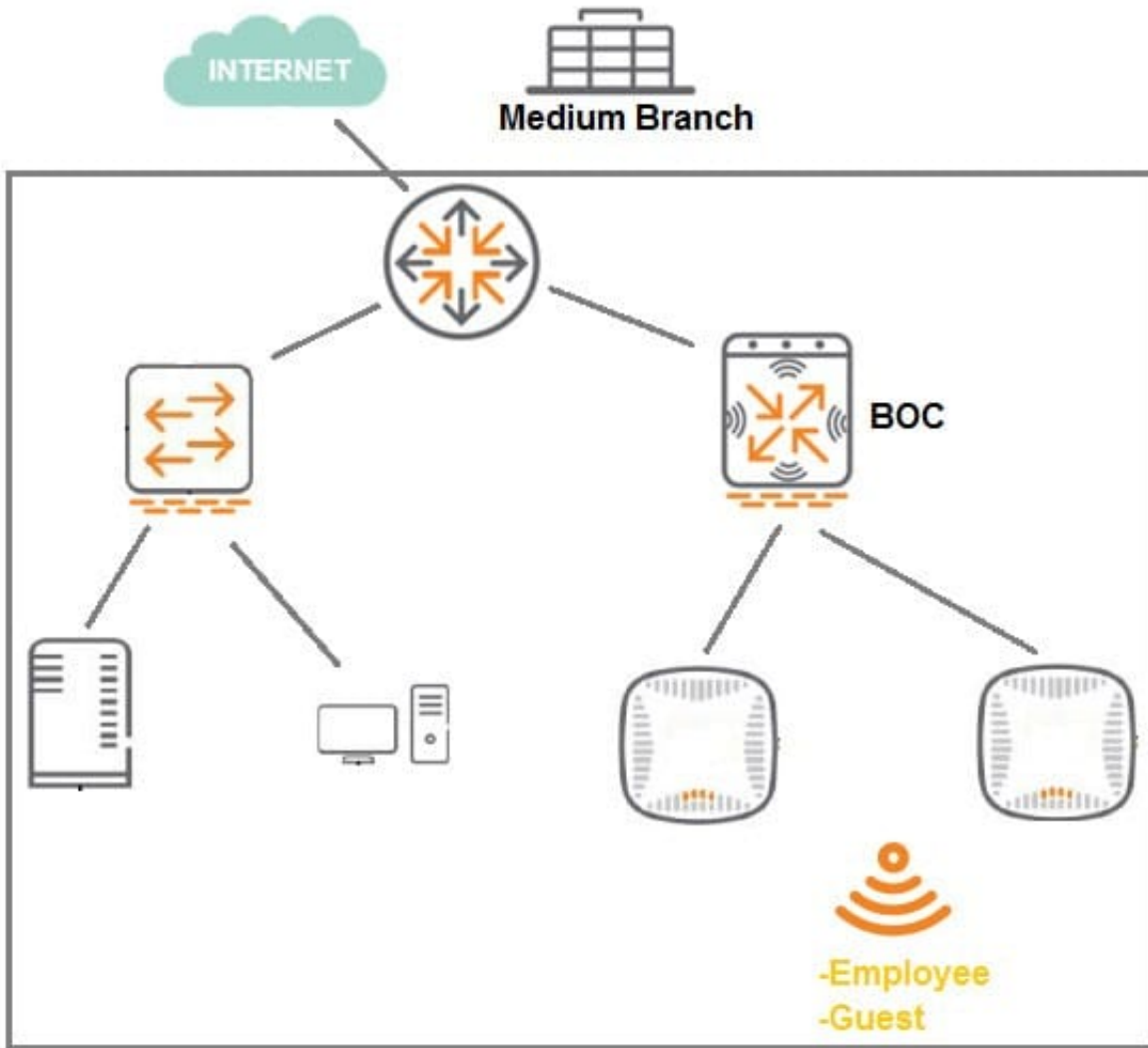
- A. Most Utilized Folders by Maximum Concurrent Clients
- B. Most Utilized by Usage
- C. Top Applications Summary
- D. Most Utilized by Maximum Concurrent Clients
- E. Top 3 Applications For Top 10 Users

Correct Answer: BD

---

## QUESTION 4

Refer to the exhibit.



A 7008 Branch Office Controller (BOC) is deployed in a remote office behind a core router. This core router does not support 802.1q encapsulation. The Mobility Controller (MC) is the gateway for two tunneling mode SSIDs, as shown in the exhibit.

Which two different configuration options ensure that wireless users are able to reach the branch network through the router? (Select two.)

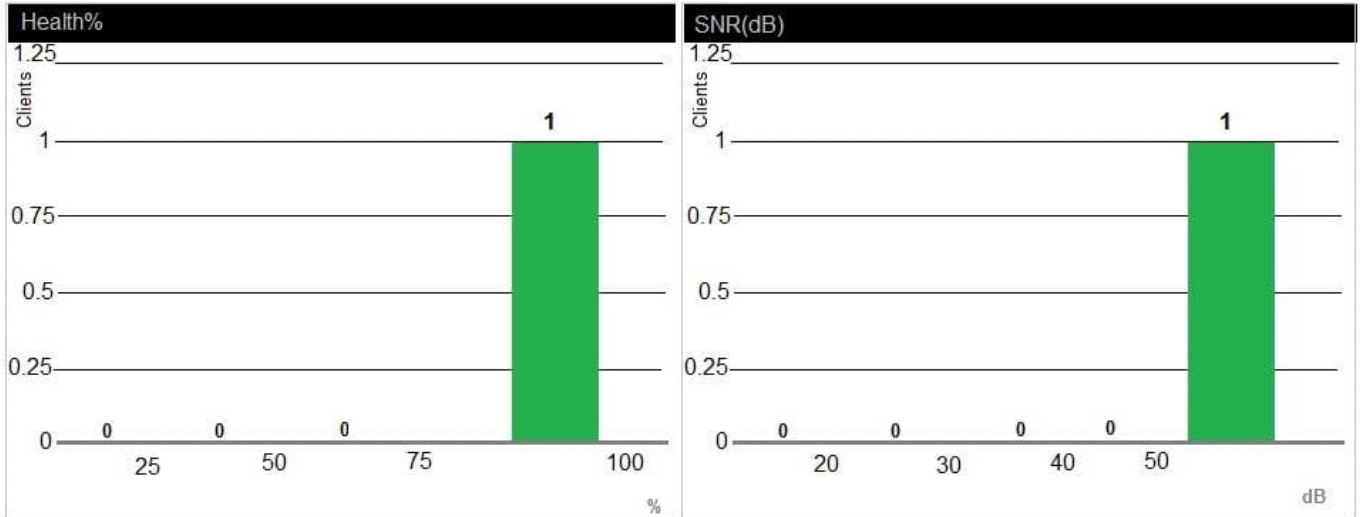
- A. Configure all ports of the BOC as access ports on the controller VLAN, and change the gateway of clients to the core router IP.
- B. Configure the uplink of the BOC as an access port on the controller VLAN, and enable NAT for the SSID VLANs.
- C. Configure the uplink of the BOC as a trunk port, tagging the controller and the SSID VLANs, and enable NAT for the SSID VLANs.
- D. Configure the uplink of the BOC as an access port on the controller VLAN, and add static router in the router for the SSID VLAN subnets.
- E. Configure the uplink of the BOC as a trunk port that permits the controller and the SSID VLANs. The controller VLAN must be native.

Correct Answer: BD



**QUESTION 5**

Refer to the exhibit.



USERNAME	CLIENT NAME	SNR^	SPEED (MBPS)	GOODPUT (MBPS)	HEALTH (%)	USAGE	DEVICE TYPE	ROLE	DEVICE NAME	LOCATION	SSID	CONNECTION
contractor14	-	58	819	32	93	1.84 Kbps	-	guest	AP12	-	contractor	11ac 5GHz

25 per page Page: 1 GO < 1 >

(A48.01114411)

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