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.passapply.com/hpe6-a48.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit.

```
(MM1) [mynode] #show ip interface brief

Interface     IP Address   /  IP Netmask      Admin     Protocol     VRRP-IP
vlan 1        10.254.10.14 /  255.255.255.0  up        up           10.254.10.214
loopback      unassigned   /  unassigned      up        up
mgmt          unassigned   /  unassigned      down      down
(MM1) [mynode] #show vrrp

Virtual Router 140:
        Description MM1
        Admin State UP, VR State BACKUP
        IP Address 10.254.10.214, MAC Address 00:00:5e:00:01:8c, vlan1
        Priority 100, Advertisement 5 sec, Preemption Enable Delay 60
        Auth type PASSWORD, Auth data: ********
        tracking is not enabled
(MM1)  [mynode]#
```

After a recent power outage where MM1 is located, the network administrator could not perform configuration tasks on Mobility Controllers (MC) for several hours. The network administrator decides to acquire another Mobility Master (MM) and deploy L2 MM redundancy. The new MM is assigned the

10.254.10.15 IP address and VRRP is configured in both units. The network administrator verifies that VRRP is running, and prepares to complete the setup with the following scripts.

```
/mm/mynode (MM1):
     master-redundancy
     master-vrrp 140
     peer-ip-address 10.254.10.15 ipsec key123
/mm/mynode (MM2):
     master-redundancy
     master-vrrp 140
     peer-ip-address 10.254.10.14 ipsec key123

/mm (MM1):
database synchronize period 30
```

Which configuration tasks must the network administrator do before applying the script in order to successfully deploy L2 MM redundancy and prevent any other control plane outage?

A. Confirm that the VRRP and master redundancy keys are the same.

B. Change the VIP address of ther VRRP process 140 to 10.254.10.15.

C. Reduce the VRRP priority to 90 and restart the process in MM2.

D. Enable the MM database synchronization in MM2.

Correct Answer: A

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

Refer to the exhibit.

(MM) [mynode] #show airmatch event all-events ap-name AP2

Band	Event Type	Radio	Timestamp	Chan	CBW	New Chan	New CBW	APName
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-25_07:50:05	100	80MHz	149	80MHz	AP2
5GHz	NOISE_DETECT	38:17:c3:10:17:30	2018-07-24_07:48:42	124	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-23_16:44:36	100	80MHz	124	80MHz	AP2
5GHz	NOISE_DETECT	38:17:c3:10:17:30	2018-07-20_19:12:34	157	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-20_10:02:30	100	80 MHz	157	80MHz	AP2
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-20_08:34:31	56	80 MHz	100	80MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-25_08:31:31	11	20MHz	6	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-25_08:31:31	6	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-24_07:46:34	1	20MHz	11	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-24_07:46:33	6	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-23_15:13:15	11	20MHz	6	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-23_15:12:12	1	20MHz	11	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-20_08:07:27	11	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-20_08:07:26	6	20MHz	11	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-19_19:22:45	1	20MHz	6	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-19_19:22:44	11	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-19_10:45:23	1	20MHz	11	20MHz	AP2

A network administrator deploys a Mobility Master (MM)-Mobility Controller (MC) network with APs in different locations. Users in one of the locations report that the WiFi network works fine for several hours, ang then they are suddenly disconnected. The symptom may happen at any time, up to three times every day, and lasts no more than two minutes.

After some research, the network administrator logs into the MM and reviews the output shown in the exhibit.

Based on this information, the network administrator logs into the MM and reviews the output shown in the exhibit.

Based on this information, what is the most likely reason users get disconnected?

A. AirMatch is applying a scheduled optimization solution.

B. Users in the 2.4 GHz band are being affected by high interference.

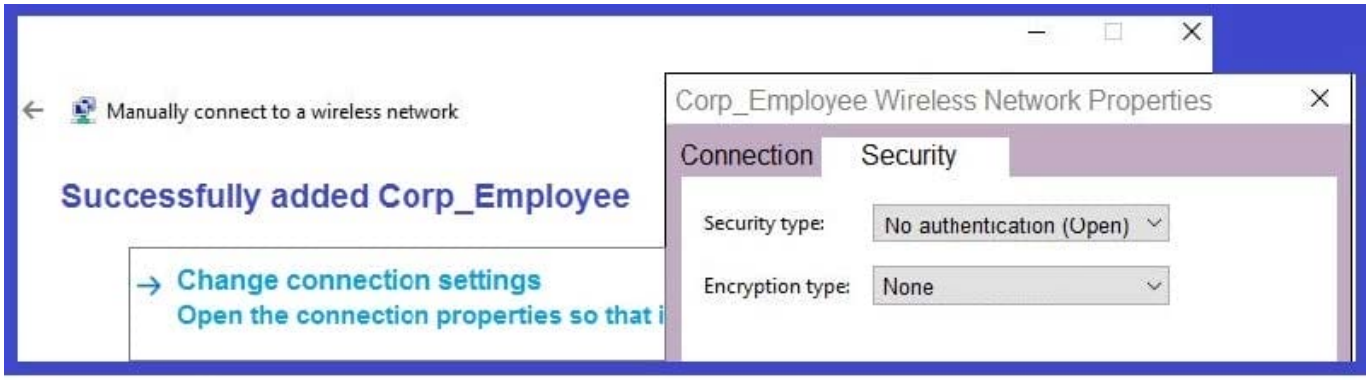
C. Adpative Radio Management is reacting to RF events.

D. AirMatch is reacting to non-scheduled RF events.

Correct Answer: B

QUESTION 4

Refer to the exhibit.



(A48.0.1114234)

A network administrator wants to configure an 802.1x supplicamt for a wireless network that includes the following: AES encryption EAP-MSCHAP v2-based user and machine authentication Validation of server certificate in Microsoft Windows 10

The network administrator creates a WLAN profile and selects the change connection settings option. Then the network administrator changes the security type to Microsoft: Protected EAP (PEAP), and enables user and machine authentication under Additonal Settings.

What must the network administrator do next to accomplish the task?

A. Enable user authentication under Settings.

B. Change the security type to Microsoft. Smart Card or other certificate.

C. Enable server certificate validation under Settings.

D. Enable computer autentication under Settings.

Correct Answer: B

QUESTION 5

Refer to the exhibit.

```
(MC2) #show auth-tracebuf mac 70:4d:7b:10:9e:c6 count 27
Warning: user-debug is enabled on one or more specific MAC addresses:
         only those MAC addresses appear in the trace buffer.

Auth Trace Buffer
-----------------------------
Jun 29 20:56:51  station-up      *    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              - -     wpa2  aes
Jun 29 20:56:51  eap-id-req     <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1 5
Jun 29 20:56:51  eap-start     ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              - -
Jun 29 20:56:51  eap-id-req     <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1 5
Jun 29 20:56:51  eap-id-resp    ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1 7     it
Jun 29 20:56:51  rad-req       ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              42 174  10.1.140.101
Jun 29 20:56:51  eap-id-resp    ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1  7    it
Jun 29 20:56:51  rad-resp      <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      42  88
Jun 29 20:56:51  eap-req       <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              2 6
Jun 29 20:56:51  eap-resp      ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              2 214
Jun 29 20:56:51  rad-req       ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      43  423  10.1.140.101
Jun 29 20:56:51  rad-resp      <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      43  228
Jun 29 20:56:51  eap-req       <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              3 146
Jun 29 20:56:51  eap-resp      ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              3 61
Jun 29 20:56:51  rad-req       ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      44 270  10.1.140.101
Jun 29 20:56:51  rad-resp      <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      44  128
Jun 29 20:56:51  eap-req       <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              4 46
Jun 29 20:56:51  eap-resp      ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              4 46
Jun 29 20:56:51  rad-req       ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      45  255 10.1.140.101
Jun 29 20:56:51  rad-accept    <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      45  231
Jun 29 20:56:51  eap-success   <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              4 4
Jun 29 20:56:51 user repkey change * 70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0        65535 -   204c0306e790000000170008
Jun 29 20:56:51 macuser repkey change * 70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0   65535 - 70:4d:7b:10:9e:c6
Jun 29 20:56:51  wpa2-key1     <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0               -   117
Jun 29 20:56:51  wpa2-key2     ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0               -   117
Jun 29 20:56:51  wpa2-key3      <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0               -   151
Jun 29 20:56:51  wpa2-key4      ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0               -   95
```

A network administrator is validating client connectivity and executes the show command shown in the exhibit. Which authentication method was used by the wireless station?

A. 802.1X user authentication

B. EAP authentication

C. 802.1X machine authentication

D. MAC authentication

Correct Answer: C