HPE6-A79 Q&As

Aruba Certified Mobility Expert Written Exam

Pass HP HPE6-A79 Exam with 100% Guarantee

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

https://www.pass2lead.com/hpe6-a79.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 to the lack of L2 and 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. 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.

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. 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.

Correct Answer: D

QUESTION 2

A network administrator wants to permit explicit SSH, FTP and HHTP(s) access to servers in the 10.100.20.5 to 10.100.20.31 range, all devices in 10.100.21.0/24 network, and a host with IP address 10.100.22.70. The services must work properly at all times.

Which configuration scripts accomplish this task with the fewer number of lines, while avoiding access to other devices not included in these ranges? (Choose two.)

A.

```
ip access-list session access2servers
    user alias file&web_servers svc http permit
    user alias file&web_servers svc-https permit
    user alias file&web_servers svc-ssh permit
    user alias file&web_servers svc-ftp permit
```

B.

```
netdestination file&web_servers
    host 10.100.22.70
    range 10.100.20.5 to 10.100.20.21
    range 10.100.20.22 to 10.100.20.31
    network 10.100.21.0 255.255.255.0
```

C.

```
netdestination file&web_servers
host 10.100.22.70
network 10.100.20.0 255.255.255.0
network 10.100.21.0 255.255.255.0
```

D.

```
netdestination file&web_servers
    host 10.100.22.70
    network 10.100.20.0 255.255.255.0
    network 10.100.21.0 255.255.255.0
```

E.

```
ip access-list session access2servers
    user alias file&web_servers tcp 20 permit
    user alias file&web_servers tcp 21 permit
    user alias file&web_servers tcp 22 permit
    user alias file&web_servers tcp 80 permit
    user alias file&web_servers tcp 443 permit
```

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Correct Answer: AB

QUESTION 3

Refer to the exhibit.

```
(MC1)  [MDC] #show ip access-list no-webapps

ip access-list session no-webapps
no-webapps
----------
Priority  Source  Destination  Service  Application   Action                 TimeRange  Log  Expired  Queue  TOS  802.1p  Blacklist  Mirror  DisScan  IPv4/6  Contract
--------  ------  -----------  -------  -----------   ------                 ---------  ---  -------  -----  ---  ------  ---------  ------  -------  ------  --------
1         user    any                   app facebook  deny senc-deny-response                          Low                                                    4
2         user    any                   app youtube   deny senc-deny-response                          Low                                                    4
3         user    any                   app netflix   deny senc-deny-response                          Low                                                    4
```

A network administrator completes the initial configuration dialog of the Mobility Controllers (MCs) and they join the Mobility Master (MM) for the first time. After the MM-MC association process, network administrator only creates AP groups, VAPs, and roles. Next, the network administrator proceeds with the configuration of the policies and creates the policy shown in the exhibit.

Which additional steps must be done to make sure this configuration takes effect over the contractor users?

A. Apply the policy in the contractors user role. Enable deep packet inspection. Reload the MCs.

B. Enable firewall visibility. Enable web-content classification. Reload the MCs.

C. Apply the policy in the contractors user role. Enable deep packet inspection.

D. Enable firewall visibility. Enable web-content classification. Reload the MMs.

Correct Answer: C

QUESTION 4

A joint venture between two companies results in a fully functional WLAN Aruba solution. The network administrator uses the following script to integrate the WLAN solution with two radius servers, radius1 and radius2.

```
aaa authentication-server radius radius1
   host 10.254.1.1
   key key111
!
aaa authentication-server radius radius2
   host 10.20.2.2
   key key222
!
aaa server-group group-corp
auth-server radius1

aaa profile aaa-corp
authentication-dot1x authenticated
dot1x-server-group group-corp
!
wlan ssid-profile ssid-corp
essid corp
opmode wpa2-aes
!
wlan virtual-ap vap-corp
aaa-profile aaa-corp
ssid-profile ssid-corp
!
ap-group building1
virtual-ap vap-corp
```

While all users authenticate with username@domainname.com type of credentials, radius1 has user accounts with the domain name portion. Which additional configuration is required to authenticate corp1.com users with radius1 and corp2 users with radius2?

A.
```
aaa authentication-server radius radius1
trim-fqdn
!
aaa server-group-corp
 auth-server radius1 match-domain corp1.com
 auth-server radius1 match-domain corp2.com
```

B.
```
aaa authentication-server radius radius1
 trim-fqdn
!
aaa server-group-corp
 auth-server radius1 match-authstring corp1.com
 auth-server radius1 match-authstring corp2.com
```

C.
```
aaa authentication-server radius radius1
!
aaa server-group-corp
 auth-server radius1 match-string corp1.com trim-fqdn
 auth-server radius1 match-string corp2.com
```

D.
```
aaa server-group-corp
 auth-server radius1 match-fqdn corp1.com
 auth-server radius1 trim-fqdn
 auth-server radius2 match-fqdn corp2.com
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 5

Refer to the exhibit.

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


Name: contractor14, IP:10.1.141.150, MAC: xx:xx:xx:xx:xx:xx, Age: 00:00:00
Role: contractor (how: ROLE_DERIVATION_DOT1X_VSA), ACL: 128/0
Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-PEAP, server: ClearPass.23
Authentication Servers: dot1x authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: ROLE_DERIVATION_DOT1X_VSA
```

A network administrator is evaluating a deployment to validate that a user is assigned the proper role and reviews the output in the exhibit. How is the role assigned to user?

A. The MC assigned the role based on Aruba VSAs.

B. The MC assigned the machine authentication default user role.

C. The MC assigned the default role based on the authentication method.

D. The MC assigned the role based on server derivation rules.

Correct Answer: C

QUESTION 6

A network administrator assists with the migration of a WLAN from a third-party vendor to Aruba in different locations throughout the country. In order to manage the solution from a central point, the network administrator decides to deploy redundant Mobility Masters (MMs) in a datacenter that are reachable through the Internet.

Since not all locations own public IP addresses, the security team is not able to configure strict firewall polices at the datacenter without disrupting some MM to Mobility Controller (MC) communications. They are also concerned about exposing the MMs to unauthorized inbound connection attempts.

What should the network administrator do to ensure the solution is functional and secure?

A. Deploy an MC at the datacenter as a VPN concentrator.

B. Block all inbound connections, and instruct the MM to initiate the connection to the MCs.

C. Block all ports to the MMs except UDP 500 and 4500.

D. Install a PEFV license, and configure firewall policies that protect the MM.

Correct Answer: C

QUESTION 7

An organization wants to deploy a WLAN infrastructure that provides connectivity to these client categories:

Employees Contractors Guest users Corporate IoT legacy devices that support no authentication or encryption Employees and contractors must authenticate with company credentials and get network access based on AD group

membership. Guest users are required to authenticate with captive portal using predefined credentials. Only employees will run L2 encryption.

Which implementation plan fulfills the requirements while maximizing the channel usage?

A. Create VAP1 to run WPA2-AES and 802.1x authentication, VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal and L2 fail through.

B. Create a single VAP to run WPA2-AES and 802.1x authentication, MAC authentication L2 fail through, captive portal, and VIA support.

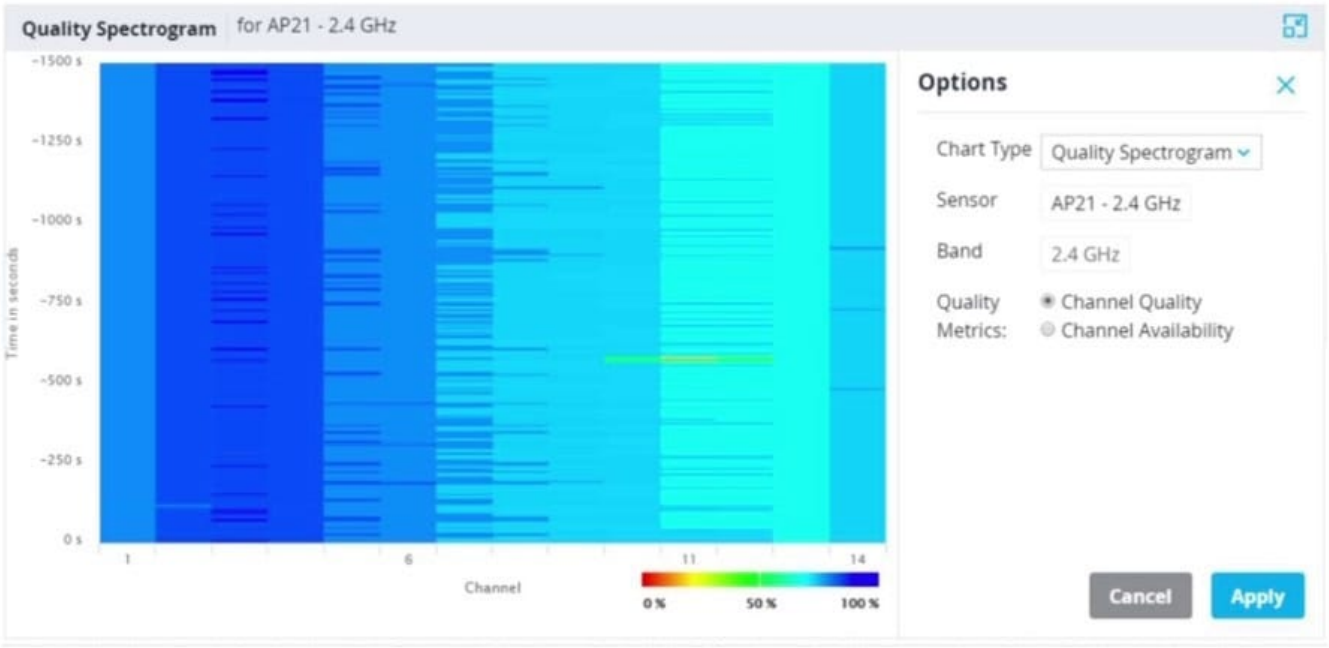
C. Create VAP1 to run WPA2-AES and 802.1x authentication, VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal.

D. Create VAP1 to run WPA2-AES and 802.1x authentication, and VAP2 to run opensystem encryption with MAC authentication and captive portal.

Correct Answer: D

QUESTION 8

Refer to the exhibit.



Based on the output shown in the exhibit, which channel offers the highest quality?

A. Channel 1

B. Channel 6

C. Channel 11

D. Channel 14

Correct Answer: B

QUESTION 9

Refer to the exhibits. Exhibit 1

```
(MC11) [mynode] (config) #show station-table

Station Entry
-------------
    MAC                Name         Role         Age(d:h:m)  Auth  AP name  Essid          Phy   Remote  Profile    User Type
-----------            -----        ----         ----------  ----  -------  -----          ---   ------  --------   ---------
xx:xx:xx:xx:xx:xx      contractor   contractor   00:00:02    Yes   AP22     EmployeesNet   g-HT  No      Employee   WIRELESS

Station Entries: 1
(MC11) [mynode] (config) #show ap client status xx:xx:xx:xx:xx:xx

STA Table
---------
bssid              auth  assoc  aid  l-int  essid          vlan-id  tunnel-id
-----              ----  -----  ---  -----  -----          -------  ---------
xx:xx:xx:xx:xx:xx  y     y      1    1      EmployeesNet   40       0x1000d
State Hash Table
----------------
bssid              state       reason
-----              -----       ------
xx:xx:xx:xx:xx:xx  auth-assoc  0
```

Exhibit 2

```
(MC11) [mynode] (config) #show log network 10

Jun 23 23:37:18 :202541:  <5669> <DBUG> |dhcpwrap| |dhcp| Received DHCP packet from Datapath, Flags 0x100040, 0pcode 0x5a, Vlan 40, Ingress tunnel 13,
Egress vlan 40, SMAC xx:xx:xx:xx:xx:xx
Jun 23 23:37:18 :202534:  <5669> <DBUG> |dhcpwrap| |dhcp| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d:05493d7f10
4vr5 0c:226962794c6573736234 3c:8h534e4120952e30 94:0157940e1e2k2g2r2e2e45e5ev
Jun 23 23:37:18 :202523:  <5669> <DBUG> |dhcpwrap| |dhcp| dhcpreplay: mac=xx:xx:xx:xx:xx:xx dev=eth1 length=300, from_port=68, op=1, giaddr=0.0.0.0
Jun 23 23:37:18 :202532:  <5669> <DBUG> |dhcpwrap| |dhcp| got 1 replay servers
Jun 23 23:37:18 :202533:  <5669> <DBUG> |dhcpwrap| |dhcp| Relayed: DISCOVER server=10.254.1.21 giaddr=192.168.40.1 MAC=xx:xx:xx:xx:xx:xx
Jun 23 23:37:18 :202523:  <5669> <DBUG> |dhcpwrap| |dhcp| dhcpreplay: mac=xx:xx:xx:xx:xx:xx dev=eth1 length=300, from_port=67, op=1, giaddr=192.168.4
0.1
Jun 23 23:37:18 :202085:  <5669> <DBUG> |dhcpwrap| |dhcp| DHCPDISCOVER from xx:xx:xx:xx:xx:xx via eth1: unknown network segment
Jun 23 23:37:18 :202085:  <5669> <DBUG> |dhcpwrap| |dhcp| DHCPDISCOVER from xx:xx:xx:xx:xx:xx 192.168.40.1: unknown network segment
Jun 23 23:37:18 :202541:  <5669> <DBUG> |dhcpwrap| |dhcp| Received DHCP packet from Datapath, Flags 0x42, 0pcode 0x5a, Vlan 1, Ingress local, Egress 0/0/0,
SMAC yy:yy:yy:yy:yy:yy
Jun 23 23:37:18 :202534:  <5669> <DBUG> |dhcpwrap| |dhcp| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d:05493d7f10
4vr5 0c:226962794c6573736234 3c:8h534e4120952e30 94:0157940e1e2k2g2r2e2e45e5ev
```

Exhibit 3

```
(MC11) #show ip interface brief

Interface                IP Address / IP Netmask     Admin  Protocol  VRRP-IP
vlan1                    10.1.140.100 / 255.255.255.0  up     up
vlan 40                  192.168.40.1 / 255.255.255.0  up     up
loopback                 unassigned / unassigned       up     up
(MC11) #
(MC11) #show packet-capture controlpath-pcap

23:37:13.562680 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:13.562887 IP 192.168.40.1.67 > 10.254.1.21.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:18.495551 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:18.495998 IP 192.168.40.1.67 > 10.254.1.21.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:22.987755 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:22.987894 IP 192.168.40.1.67 > 10.254.1.21.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
```

A network administrator wants to allow contractors to access the corporate WLAN named EmployeesNet with the

contractor role in VLAN 40. When users connect, they do not seem to get an IP address. After some verification checks, the network administrator confirms the DHCP server (10.254.1.21) is reachable from the Mobility Controller (MC) and obtains the outputs shown in the exhibits.

What should the network administrator do next to troubleshoot this problem?

A. Permit UDP67 to the contractor role.

B. Remove the IP address in VLAN 40.

C. Configure the DHCP helper address.

D. Confirm there is an IP pool for VLAN 40.

Correct Answer: A

QUESTION 10

Refer to the exhibit.

```
(MC2) #show auth-tracebuf mac xx:xx:xx:xx:xx:xx 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            *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      -    wpa2 aes
Jun 29 20:56:51  eap-id-req           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1      5
Jun 29 20:56:51  eap-start             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      -
Jun 29 20:56:51  eap-id-req            <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1      5
Jun 29 20:56:51  eap-id-resp            ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1      7    it
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          42     174  10.1.140.101
Jun 29 20:56:51  eap-id-resp            ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1      7    it
Jun 29 20:56:51  rad-resp              <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  42     88
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          2      6
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          2      214
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  43     423  10.1.140.101
Jun 29 20:56:51  rad-resp              <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  43     228
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          3      146
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          3      61
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  44     270  10.1.140.101
Jun 29 20:56:51  rad-resp              <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  44     128
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          4      46
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          4      46
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  45     255  10.1.140.101
Jun 29 20:56:51  rad-accept            <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  45     231
Jun 29 20:56:51  eap-success           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          4      4
Jun 29 20:56:51  user repkey change     *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          65535  -    204c0306e790000000170008
Jun 29 20:56:51  macuser repkey change   *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          65535  -    xx:xx:xx:xx:xx:xx
Jun 29 20:56:51  wpa2-key1             <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      117
Jun 29 20:56:51  wpa2-key2             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      117
Jun 29 20:56:51  wpa2-key3             <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      151
Jun 29 20:56:51  wpa2-key4             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      95
```

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

A. EAP authentication

B. 802.1X machine authentication

C. MAC authentication

D. 802.1X user authentication

Correct Answer: D