



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.passapply.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**

Refer to the exhibit.

```
(MC14-1) #show aaa authentication dot1x Corp-Network
```

```
802.1X Authentication Profile "Corp-Network"
```

Parameter	value
Max authentication failures	0
Enforce Machine Authentication	Enabled
Machine Authentication: Default Machine Role	guest
Machine Authentication Cache Timeout	24 hr(s)
Blacklist on Machine Authentication Failure	Disabled
Machine Authentication: Default User Role	guest
Interval between Identity Requests	5 sec
Quiet Period after Failed Authentication	30 sec
Reauthentication Interval	86400 sec
Use Server provided Reauthentication Interval	Disabled
Use the termination-action attribute from the Server	Disabled
Multicast Key Rotation Time Interval	1800 sec
Unicast Key Rotation Time Interval	900 sec
Authentication Server Retry Interval	5 sec
Authentication Server Retry Count	3
Framed MTU	1100 bytes
Max number of requests sent during an Auth attempt	5
Max Number of Reauthentication Attempts	3
Maximum number of times Held State can be bypassed	0
Dynamic WEP Key Message Retry Count	1
Dynamic WEP Key Size	128 bits
Interval between WPA/WPA2 Key Messages	1000 msec
Delay between EAP-Success and WPA2 Unicast Key Exchange	0 msec
Delay between WPA/WPA2 Unicast Key and Group Key Exchange	0 msec
Time interval after which the PMKSA will be deleted	8 hr(s)
Delete Keycache upon user deletion	Disabled
WPA/WPA2 Key Messages Retry Count	3
Multicast Key Rotation	Disabled
Unicast Key Rotation	Disabled
Reauthentication	Disabled
Opportunistic Key Caching	Enabled

The network administrator must ensure that the configuration will force users to authenticate periodically every eight hours. Which configuration is required to effect this change?

- A. Set the reauth-period to 28800 enable reauthentication in the dot1x profile.
- B. Set the reauth-period to 28800 enable reauthentication in the AAA profile.
- C. Set the reauth-period to 28800 enable reauthentication in both dot1x and AAA profile.



D. Set the reauth-period to 28800 in the dot1x profile and enable reauthentication in the AAA profile.

Correct Answer: A

QUESTION 2

Refer to the exhibit.

```
(MC11) [mynode] #show ap database | exclude =
```

AP Database

Name	Group	AP Type	IP Address	Status	Flags	Switch IP	Standby IP	wired MAC Address	Serial #	Port	FQLN	Outer IP	User
AP21	CAMPUS	355	10.1.145.150	Up 3m:20s	UNI	10.254.13.14	0.0.0.0	xx:xx:xx:xx:xx:xx	CNB30Y301	N/A	N/A	N/A	
AP22	CAMPUS	355	10.1.146.150	Up 32m:23s		10.254.13.14	0.0.0.0	xx:xx:xx:xx:xx:xy	CNB30Y305	N/A	N/A	N/A	

Total Aps:2

```
(MC11) [mynode] #show ap active | exclude =
```

Active AP Table

Name	Group	IP Address	11g Clients	11g Ch/EIRP/MaxEIRP	11a Clients	11a Ch/EIRP/MaxEIRP	AP Type	Flags	Uptime	Outer IP
AP21	CAMPUS	10.1.146.150	0	AP:HT:11/9.0/24.0	0	AP:VHT:153E:/18.0/28.5	355	Aa	32m:30s	N/A

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates local Spectrum override in effect.

Num Aps:1

A network administrator deploys a new Mobility Master (MM) - Mobility Controller (MC) network. To test the solution, the network administrator accesses the console of a pair of APs and statically provisions them. However, one of the APs does not propagate the configured SSIDs. The network administrator looks at the logs and sees the output shown in the exhibit.

Which actions must the network administrator take to solve the problem?

- A. Create another AP group in the MC's configuration, and re-provision one AP with a different group.
- B. Re-provision one of the APs with a different name, and add new entries with the proper group in the whitelist.
- C. Re-provision the AP with a different group, and modify the name of one AP in the whitelist.
- D. Re-provision one of the APs with a different name or modify the name in the whitelist.

Correct Answer: D

QUESTION 3

Users run Skype for Business on wireless clients with no WMM support over an Aruba Mobility Master (MM) - Mobility Controller (MC) based network. When traffic arrives at the wired network, it does not include either L2 or L3 markings.

Which configuration steps should the network administrator take to classify and mark voice and video traffic with UCC heuristics mode?

- A. Enable WMM in a VAP profile, and explicitly permit voice and video UDP ports in a firewall policy.
- B. Confirm OpenFlow is enabled in the user role and VAP profile. Then enable WMM in a SSID profile, and explicitly



permit voice and video UDP ports in a firewall policy.

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

D. Confirm MM is the Openflow controller of MCs and Openflow is enabled in VAP and firewall roles. Enable Skype4Business ALG in UCC profiles.

Correct Answer: A

QUESTION 4

Refer to the exhibit.

```
xx:xx:xx:xx:xx:xx# sh dhcp subnets
```

DHCP Subnet Table

VLAN	Type	Subnet	Mask	Gateway	Mode	Rolemap
124	13	10.21.124.32	255.255.255.224	10.21.124.33	local, split-tunnel	
81	12	0.0.0.0	255.255.255.255	0.0.0.0	remote, full-tunnel	

A network engineer deploys two different DHCP pools in an Instant AP (IAP) cluster for WLANs that will have connectivity to a remote site using Aruba IPsec. Based on the output shown in the exhibit, which IAP-VPN DHCP modes are being used?

- A. distributed L3 and centralized L2
- B. local L3 and centralized L2
- C. local L3 and distributed L2
- D. centralized L3 and distributed L2

Correct Answer: D

QUESTION 5

Refer to the exhibits.



```
(MM1) [md] #configure t
Enter Configuration commands, one per line. End with CNNL/Z

(MM1) [md] (config) #user-role corp-employee
(MM1) ^[md] (config-submode)#access-list session allowall
(MM1) ^[md] (config-submode)#exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #aaa profile corp-employee
(MM1) ^[md] (AAA Profile "corp-employee") #dot1x-default-role corp-employee
(MM1) ^[md] (AAA Profile "corp-employee") #dot1x-server-group Radius
(MM1) ^[md] (AAA Profile "corp-employee") #exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #write memory
```

Saving Configuration...

Configuration saved.

```
(MM1) [md] (config) #cd MC1
(MM1) [20:4c:03:06:e5:c0] (config) #mdc
```




Redirecting to Managed Device Shell

(MC1) [MDC] #show switches

All Switches

IP Address	IPv6 Address	Name	Location	Type	Model	Version	Status	Configuration State	Config Sy
10.1.140.100	None	MC1	Building1.floor1	MD	Aruba7030	8.6.0.2_73853	up	UPDATE SUCCESSFUL	11

Total Switches:1

(MC1) [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/Ph
10.1.141.150	yy:yy:yy:yy:yy:yy	hector.barbosa	guest	00:00:23	802.1x		AP22	wireless	corp-employee/

User Entries: 1/1

Curr/Cum Alloc:3/18 Free:0/15 Dyn:3 AllocErr:0 FreeErr:0

(MC1) [MD] #show aaa profile corp-employee

AAA Profile "corp-employee"

Parameter	Value
Initial role	guest
MAC Authentication Profile	N/A
MAC Authentication Server Group	default
802.1X Authentication Profile	corp-employee_dot1x_aut
802.1X Authentication Server Group	Radius
Download Role from CPPM	Disabled
Set username from dhcp option 12	Disabled
L2 Authentication Fail Through	Disabled
Multiple Server Accounting	Disabled
User idle timeout	N/A
Max IPv4 for wireless user	2
RADIUS Accounting Server Group	N/A
RADIUS Roaming Accounting	Disabled
RADIUS Interim Accounting	Disabled
RADIUS Acct-Session-Id In Access-Request	Disabled
RFC 3576 server	N/A
User derivation rules	N/A
wired to wireless Roaming	Enabled
Reauthenticate wired user on VLAN change	Disabled
Device Type Classification	Enabled
Enforce DHCP	Disabled
PAN Firewall Integration	Disabled
Open SSID radius accounting	Disabled
Apply ageout mechanism on bridge mode wireless clients	Disabled

(MC1) [MDC] #

A network administrator has fully deployed a WPA3 based WLAN with 802.1X authentication. Later he defined corp-employee as the default user-role for the 802.1X authentication method in the aaa profile. When testing the setup he realizes the client gets the "guest" role.

What is the reason "corp-employee" user role was not assigned?

- A. The administrator forgot to map a dot1x profile to the corp-employee aaa profile.
- B. The administrator forgot to enable PEFNG feature set on the Mobility Master.
- C. MC 1 has not received the configuration from the mobility master yet.
- D. The Mobility Master lacks MM-VA licenses; therefore, it shares partial configuration only.



VCE & PDF

PassApply.com

<https://www.passapply.com/hpe6-a79.html>

2024 Latest passapply HPE6-A79 PDF and VCE dumps Download

Correct Answer: C

[Latest HPE6-A79 Dumps](#)

[HPE6-A79 Study Guide](#)

[HPE6-A79 Exam Questions](#)