DUMPSHQ

Free Questions for HPE6-A79 by dumpshq

Shared by Whitehead on 07-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A network administrator is in charge of a Mobility Master (MM) -- Mobility Controller (MC) based network security. Recently the Air Monitors detected a Rogue AP in the network and the administrator wants to enable ''Tarpit'' based wireless containment.

What profile must the administrator enable ''tarpit'' wireless containment on?

Options:

A) IDS Unauthorized device profile

B) IDS profile

C) IDS General profile

D) IDS DOS profile

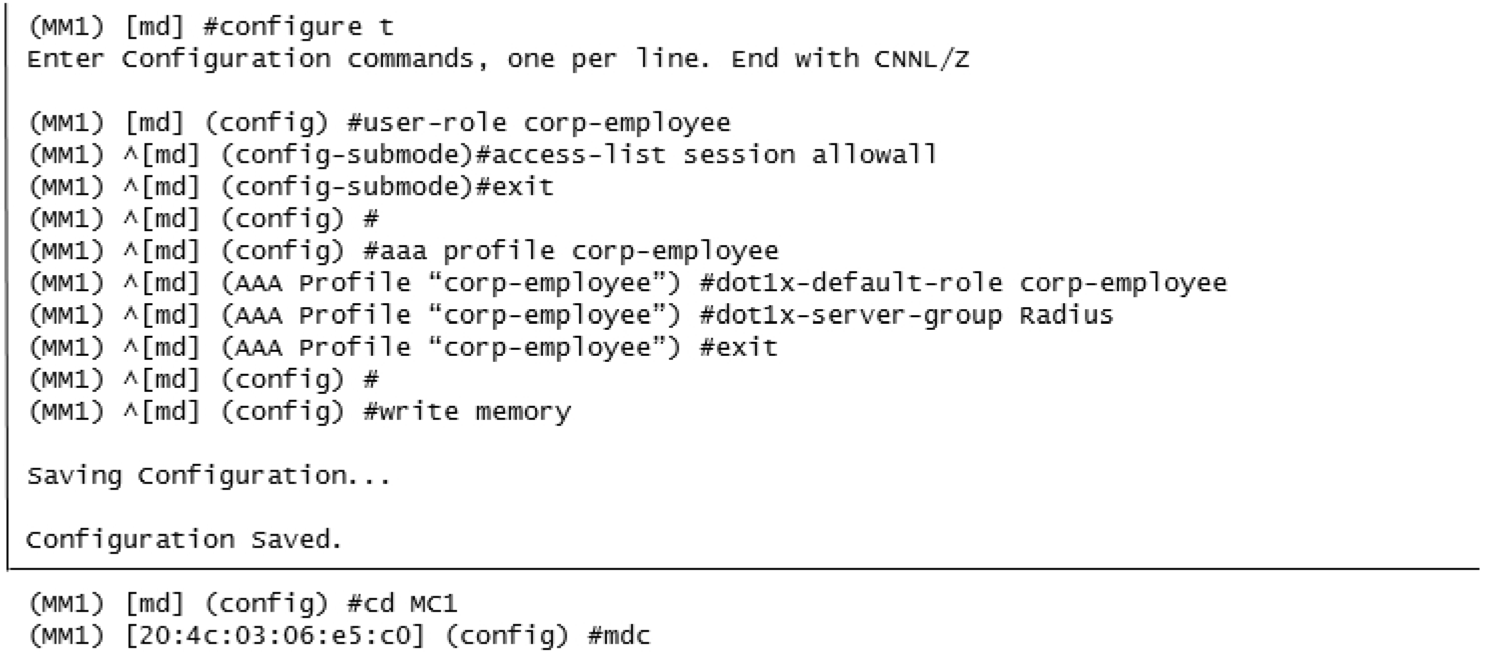
Answer:

A

Question 2

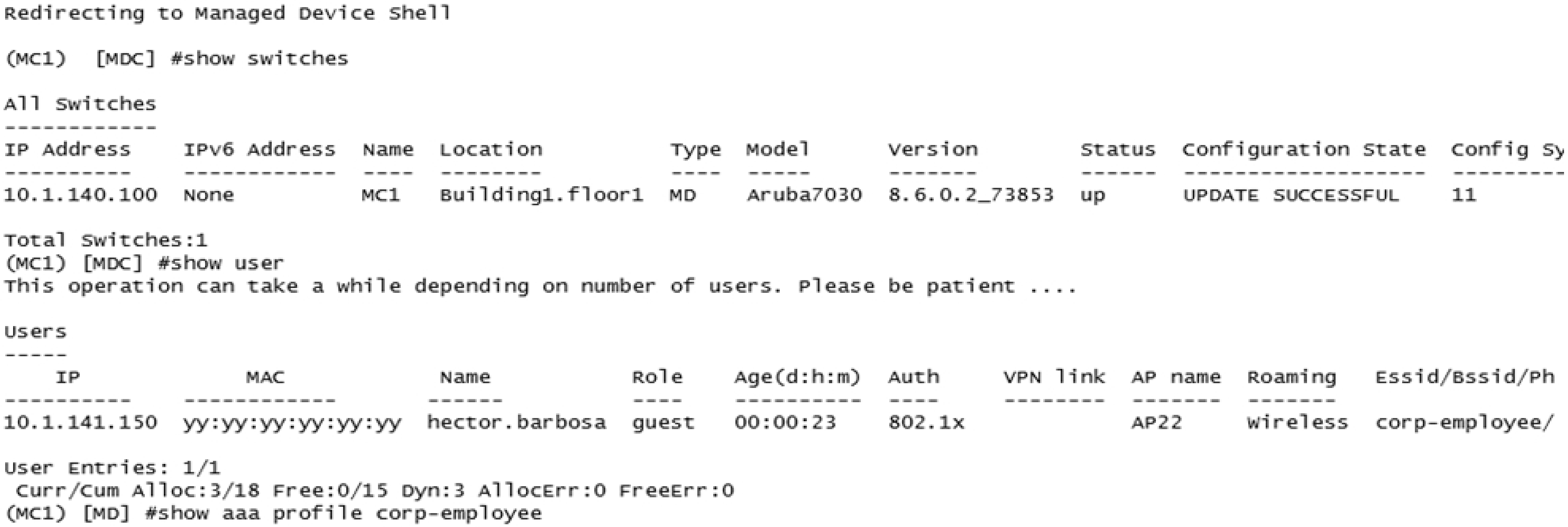
Question Type: MultipleChoice

Refer to the exhibits.

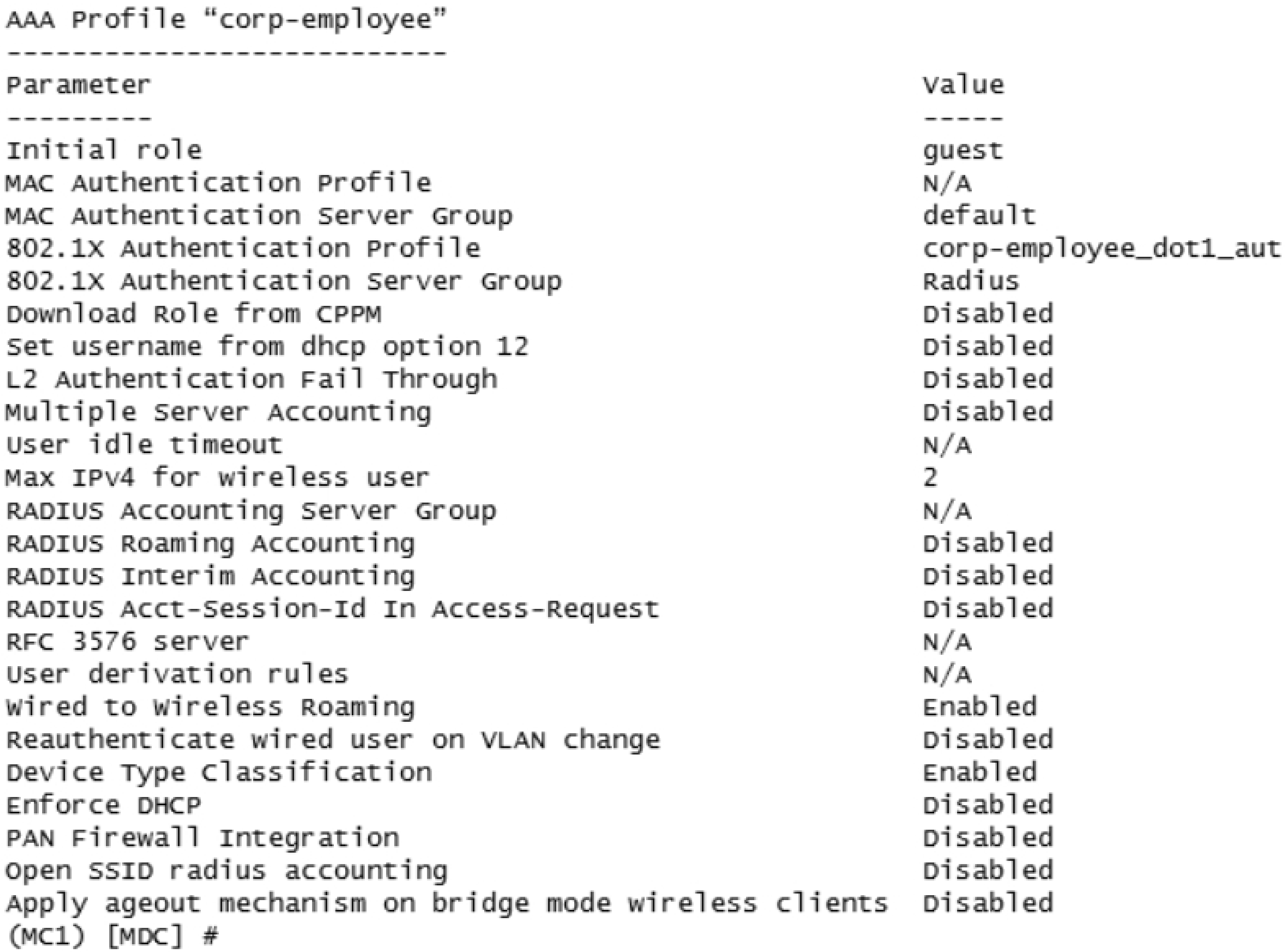


```
(MM1) [md] #configure t
Enter Configuration commands, one per line. End with CNNL/Z

(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_dot1_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?

Options:

A) The administrator forgot to map a dotlx 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.

Answer:

C

Question 3

Question Type: MultipleChoice

A network administrator has deployed an Airwave Management Platform (AMP) server and integrated it with a Mobility Master (MM) -- Mobility Controller (MC) based WLAN. The AMP server already has all Aruba Mobility devices including Access Points (APs) in the "UP" devices list.

What are two actions the administrator can execute upon the APs under "Airwave>Devices>Monitor"? (Choose two.)

Options:

A) Open the WebUI of the MC where the AP terminates.

B) Re-provision the Access Point.

C) Disable and change the mode of the AP's radios.

D) Invoke MC's show commands for that Access Point.

E) Run Spectrum Analysis locally.

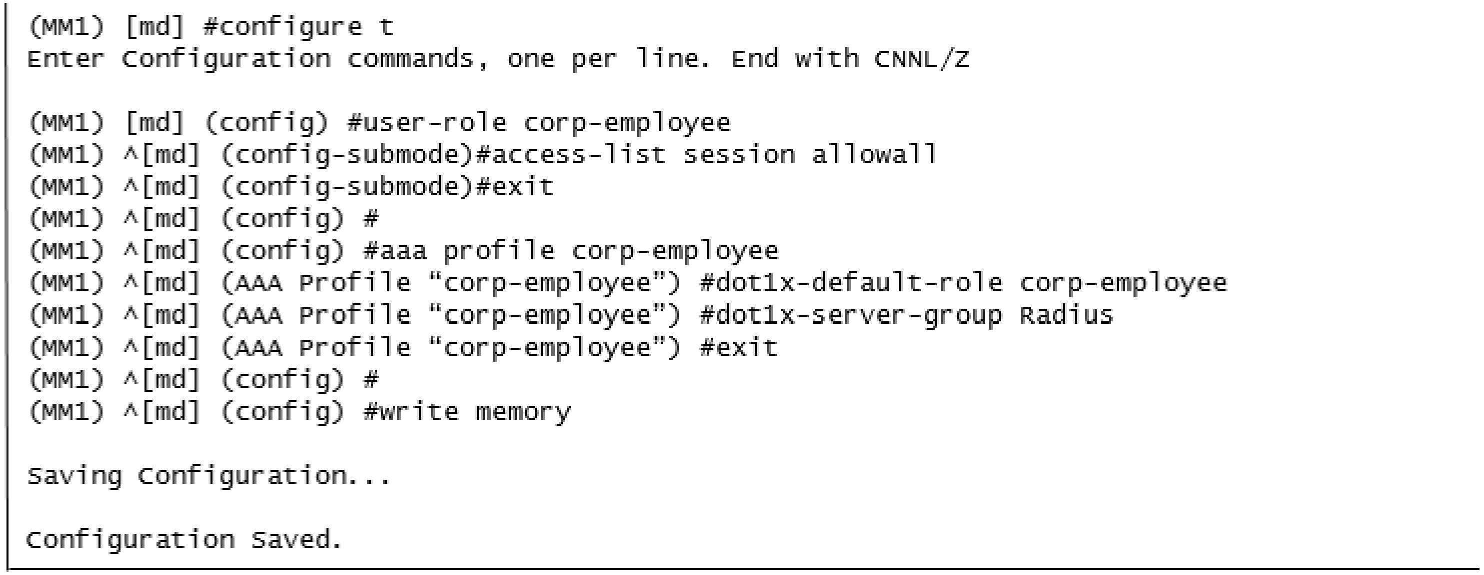
Answer:

D, E

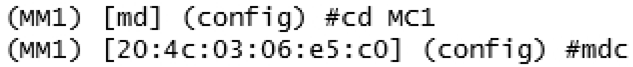
Question 4

Question Type: **MultipleChoice**

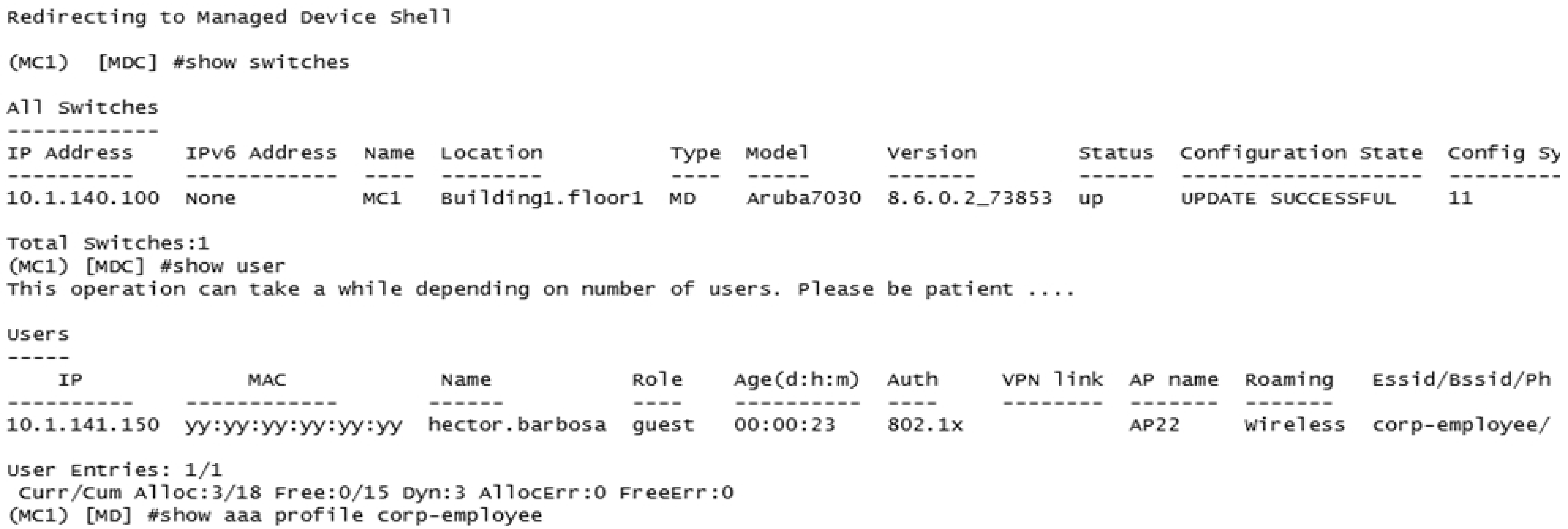
Refer to the exhibits.



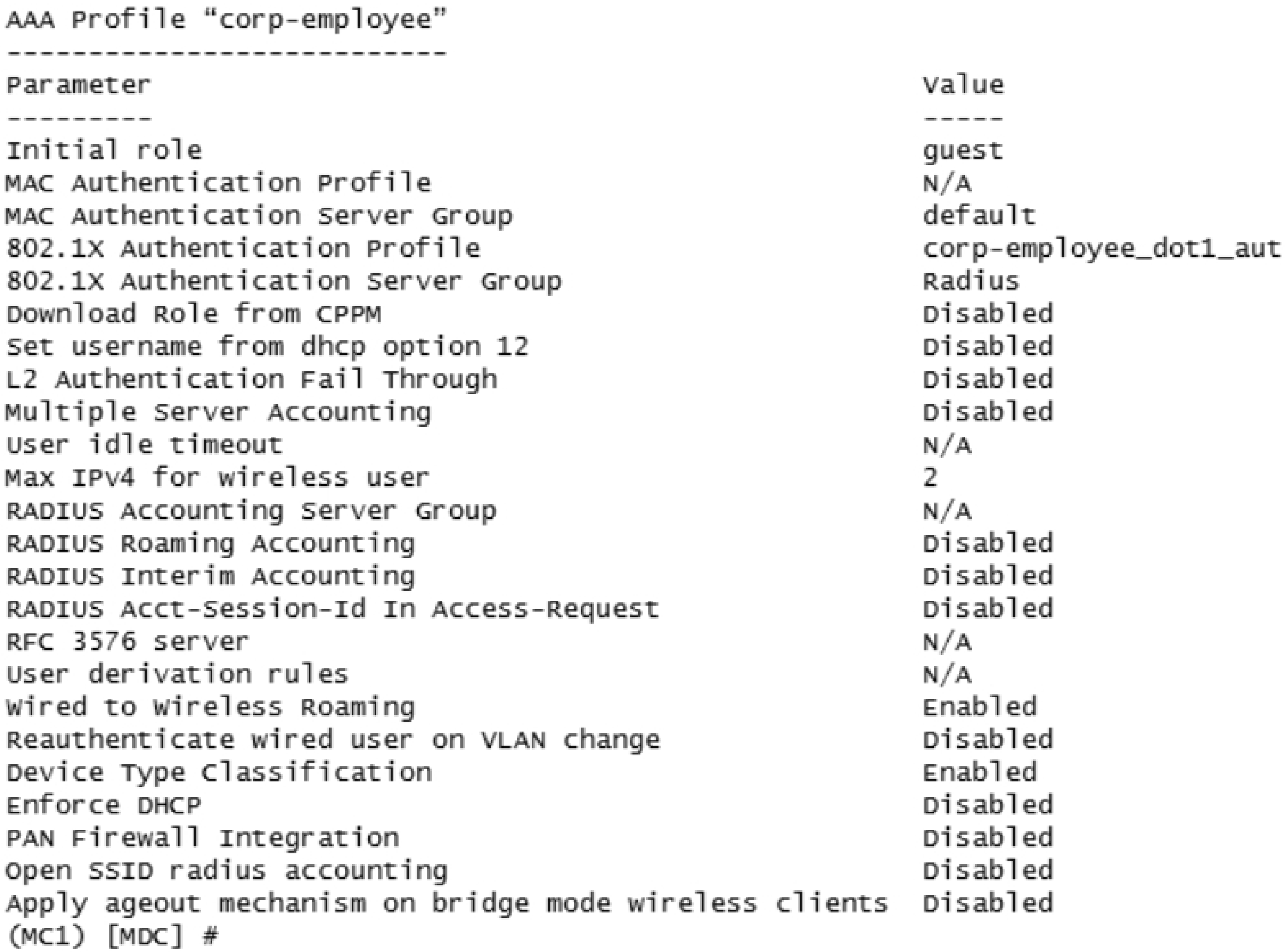
```
(MM1) [md] #configure t
Enter Configuration commands, one per line. End with CNNL/Z

(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_dot1_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?

Options:

A) The administrator forgot to map a dotlx 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.

Answer:

C

Question 5

Question Type: **MultipleChoice**

A network administrator has deployed an Airwave Management Platform (AMP) server and integrated it with a Mobility Master (MM) -- Mobility Controller (MC) based WLAN. The AMP server already has all Aruba Mobility devices including Access Points (APs) in the ''UP'' devices list.

What are two actions the administrator can execute upon the APs under ''Airwave>Devices>Monitor''? (Choose two.)

Options:

A) Open the WebUI of the MC where the AP terminates.

B) Re-provision the Access Point.

C) Disable and change the mode of the AP's radios.

D) Invoke MC's show commands for that Access Point.

E) Run Spectrum Analysis locally.

Answer:

D, E

Question 6

Question Type: **MultipleChoice**

A network administrator is in charge of a Mobility Master (MM) -- Mobility Controller (MC) based network security. Recently the Air Monitors detected a Rogue AP in the network and the administrator wants to enable ''Tarpit'' based wireless containment.

What profile must the administrator enable ''tarpit'' wireless containment on?

Options:

A) IDS Unauthorized device profile

B) IDS profile

C) IDS General profile

D) IDS DOS profile

Answer:

A