Free Questions for HPE6-A79 by dumpssheet

Shared by Meadows on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A customer wants a WLAN solution that permits Aps to terminate WPA-2 encrypted traffic from different SSIDs to different geographic locations where non-related IT departments will take care of enforcing security policies. A key requirement is to minimize network congestion, overhead, and delay while providing data privacy from the client to the security policy enforcement point. Therefore, the solution must use the shortest path from source to destination.

Which Aruba feature best accommodates this scenario?

Options:

A- Inter MC S2S IPsec tunnels

B- RAPs

C- Multizone Aps

D- VIA

E- Inter MC GRE tunnels

Answer:

B

Question 2

Question Type: **MultipleChoice**

A network administrator is in charge of a Mobility Master (MM) -- Mobility Controller (MC) based WLAN. The administrator has deployed an Airwave Management Platform (AMP) server in order to improve the monitoring capabilities and generate reports and alerts.

The administrator has configured SNMPv3 and Admin credentials on both the MMs and MCs and has created Groups and Folders in the AMP server.

What two additional steps must the administrator do in order to let Airwave monitor the network devices? (Choose two.)

Options:

A- Manually add the Active MM and wait for automatic Discovery.

B- Map the AMP's IP address with a mgmt-config profile in the MM.

C- Set the AMP's IP address and Org string as DHCP option 43.

D- Manually add each MM. MC and Access Point in the AMP server.

E- Move 'New' devices into a group and folder in Airwave.

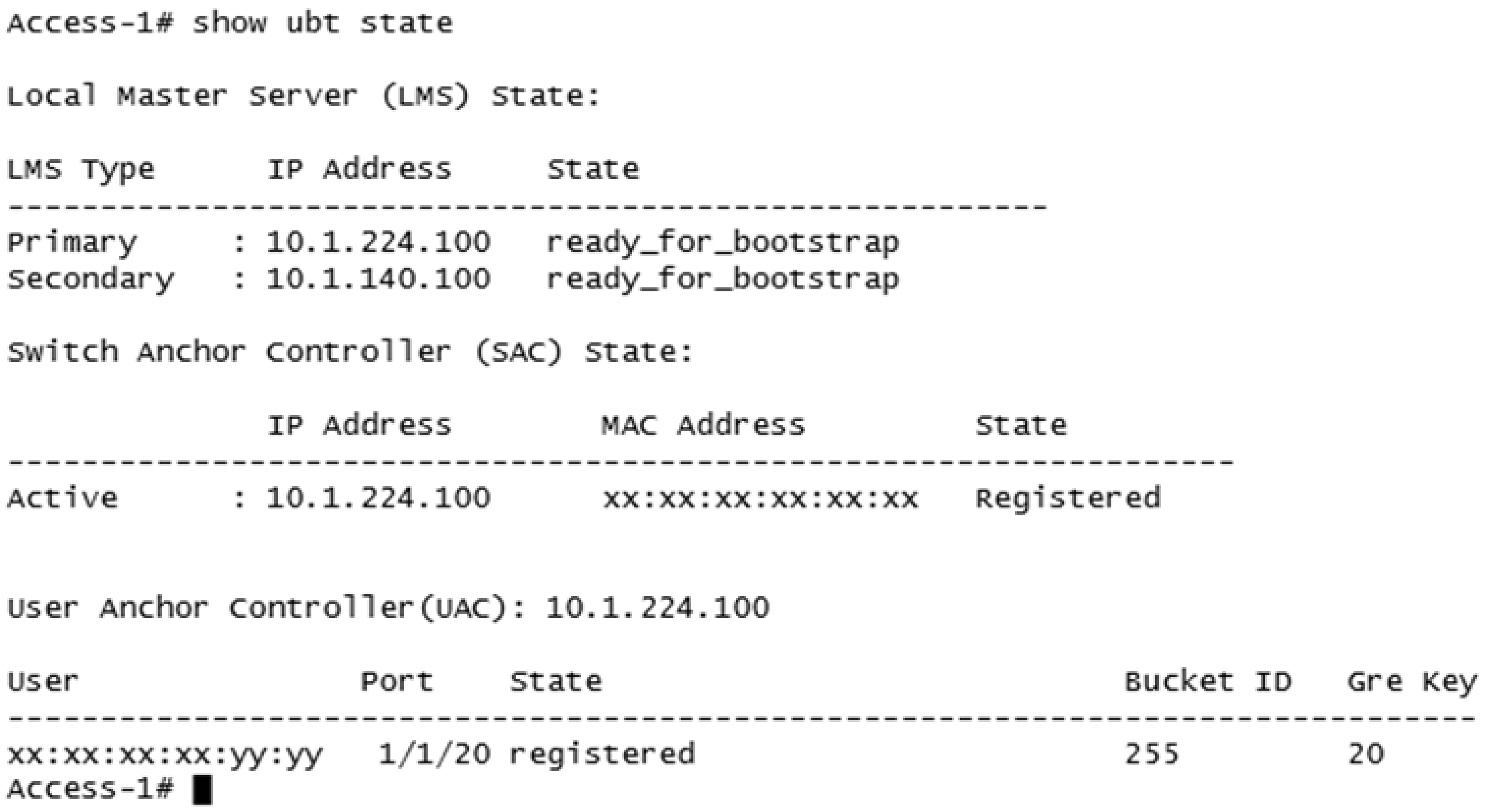
Answer:

A, B

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.



```
Access-1# show ubt state

Local Master Server (LMS) State:

LMS Type      IP Address     State
--------------------------------------------------------
Primary     : 10.1.224.100   ready_for_bootstrap
Secondary   : 10.1.140.100   ready_for_bootstrap

Switch Anchor Controller (SAC) State:

              IP Address        MAC Address         State
------------------------------------------------------------------
Active      : 10.1.224.100      xx:xx:xx:xx:xx:xx   Registered


User Anchor Controller(UAC): 10.1.224.100

User               Port    State                            Bucket ID   Gre Key
-------------------------------------------------------------------------------
xx:xx:xx:xx:yy:yy   1/1/20 registered                       255         20
Access-1# █
```

Based on the output shown in the exhibit, with which Aruba devices has Access-1 established tunnels?

Options:

A- a pair of standalone MCs

B- a pair of switches running VXLAN

C- a pair of MCs within a L3 cluster

D- a single standalone MC

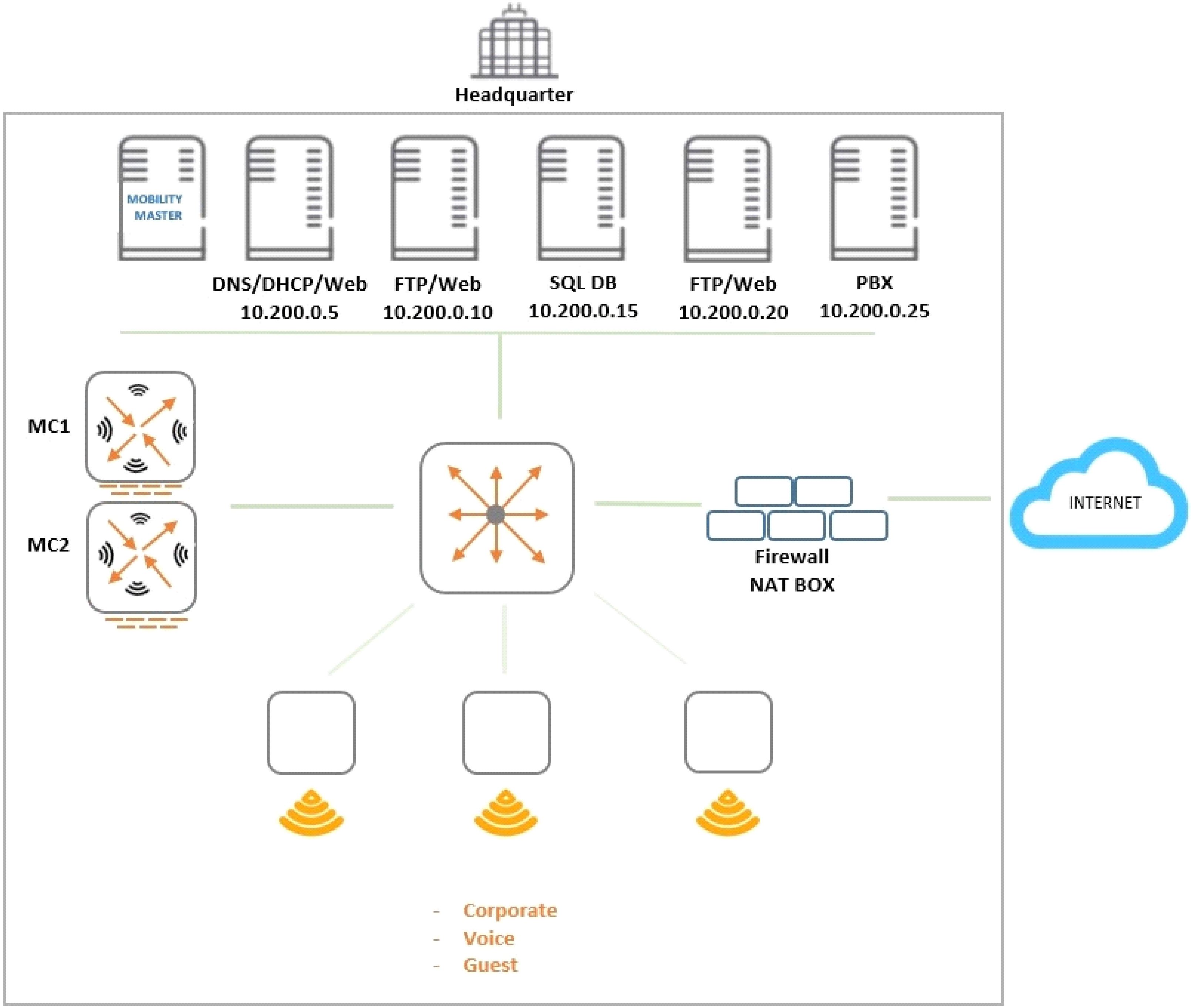
Answer:

C

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit.

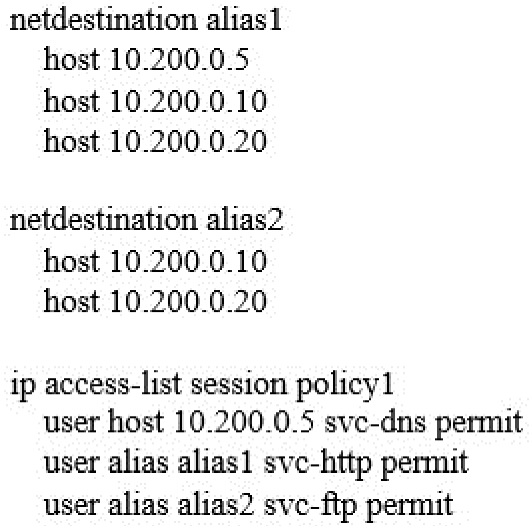

Headquarter
MOBILITY MASTER
DNS/DHCP/Web
10.200.0.5
FTP/Web
10.200.0.10
SQL DB
10.200.0.15
FTP/Web
10.200.0.20
PBX
10.200.0.25
MC1
MC2
Firewall
NAT BOX
INTERNET
- Corporate
- Voice
- Guest

An organization provides WiFi access through a corporate SSID with an Aruba Mobility Master (MM) - Mobility Controller (MC) network that includes PEF functions. The organization wants to have a single firewall policy configured and applied to the employee role.

This policy must allow users to reach Web, FTP, and DNS services, as shown in the exhibit. Other services should be exclusive to other roles. The client NICs should receive IP settings dynamically.

Which policy design meets the organization's requirements while minimizing the number of policy rules?

A.

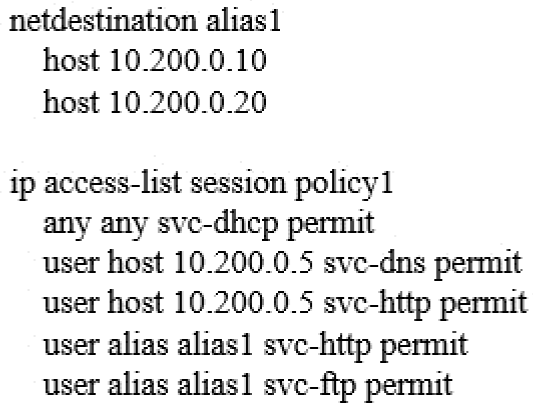


```
netdestination alias1
   host 10.200.0.5
   host 10.200.0.10
   host 10.200.0.20

netdestination alias2
   host 10.200.0.10
   host 10.200.0.20

ip access-list session policy1
   user host 10.200.0.5 svc-dns permit
   user alias alias1 svc-http permit
   user alias alias2 svc-ftp permit
```

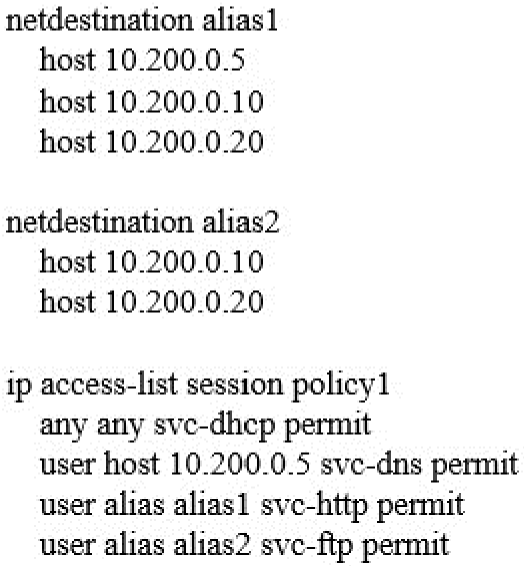
B.



```
netdestination alias1
   host 10.200.0.10
   host 10.200.0.20

ip access-list session policy1
   any any svc-dhcp permit
   user host 10.200.0.5 svc-dns permit
   user host 10.200.0.5 svc-http permit
   user alias alias1 svc-http permit
   user alias alias1 svc-ftp permit
```

C.

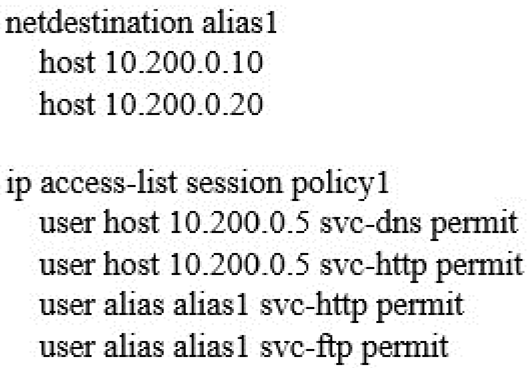


```
netdestination alias1
   host 10.200.0.5
   host 10.200.0.10
   host 10.200.0.20

netdestination alias2
   host 10.200.0.10
   host 10.200.0.20

ip access-list session policy1
   any any svc-dhcp permit
   user host 10.200.0.5 svc-dns permit
   user alias alias1 svc-http permit
   user alias alias2 svc-ftp permit
```

D.



```
netdestination alias1
   host 10.200.0.10
   host 10.200.0.20

ip access-list session policy1
   user host 10.200.0.5 svc-dns permit
   user host 10.200.0.5 svc-http permit
   user alias alias1 svc-http permit
   user alias alias1 svc-ftp permit
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

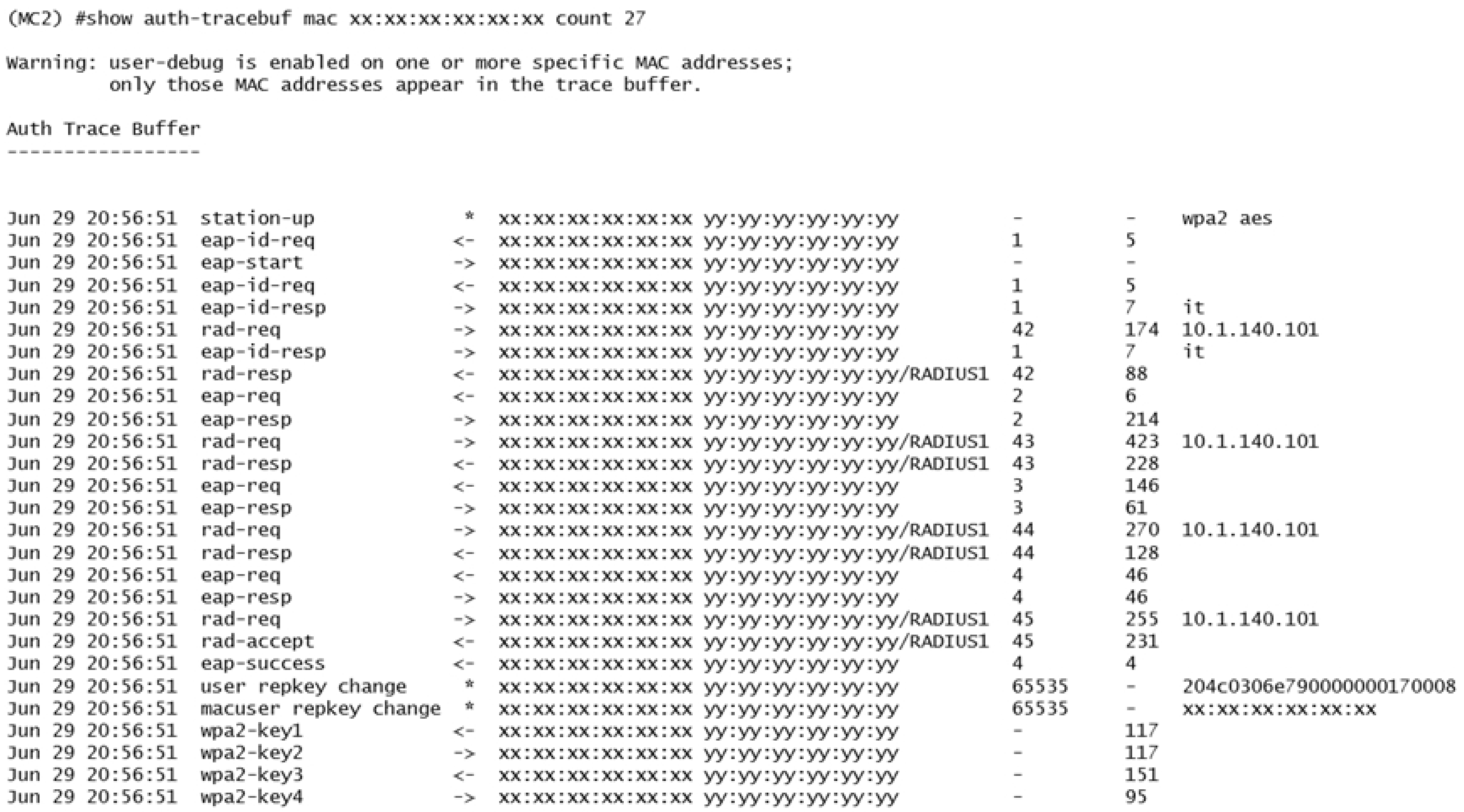
Answer:

C

Question 5

Question Type: **MultipleChoice**

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?

Options:

A- EAP authentication

B- 802.1X machine authentication

C- MAC authentication

D- 802.1X user authentication

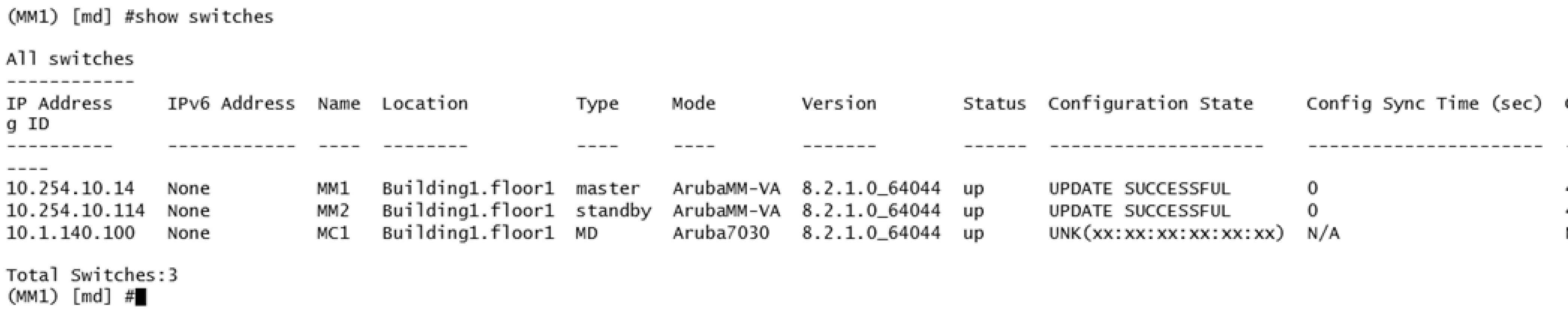
Answer:

D

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit.



```
(MM1) [md] #show switches

All switches
------------
IP Address     IPv6 Address  Name  Location          Type     Mode         Version         Status  Configuration State      Config Sync Time (sec)
g ID
----------     ------------  ----  --------          ----     ----         -------         ------  -------------------      ----------------------
----
10.254.10.14   None          MM1   Building1.floor1  master   ArubaMM-VA   8.2.1.0_64044   up      UPDATE SUCCESSFUL        0
10.254.10.114  None          MM2   Building1.floor1  standby  ArubaMM-VA   8.2.1.0_64044   up      UPDATE SUCCESSFUL        0
10.1.140.100   None          MC1   Building1.floor1  MD       Aruba7030    8.2.1.0_64044   up      UNK(xx:xx:xx:xx:xx:xx)   N/A

Total Switches:3
(MM1) [md] #█
```

A network administrator adds a Mobility Controller (MC) in the /mm level and notices that the device does not show up in the managed networks hierarchy. The network administrator accesses the CLI. executes the show switches command, and obtains the output shown in the exhibit.

What is the reason that the MC does not appear as a managed device in the hierarchy?

Options:

A- The network administrator added the device using the wrong Pre-Shared Key (PSK).

B- The network administrator has not moved the device into a group yet.

C- The digital certificate of the MC is not trusted by the MM.

D- The IP address of the MC does not match the one that was defined in the MM.

Answer:

D

Question 7

Question Type: Hotspot

A network administrator wants to receive a warning level alarm every time the noise floor rises above -82 dBm on any of the AP radios.

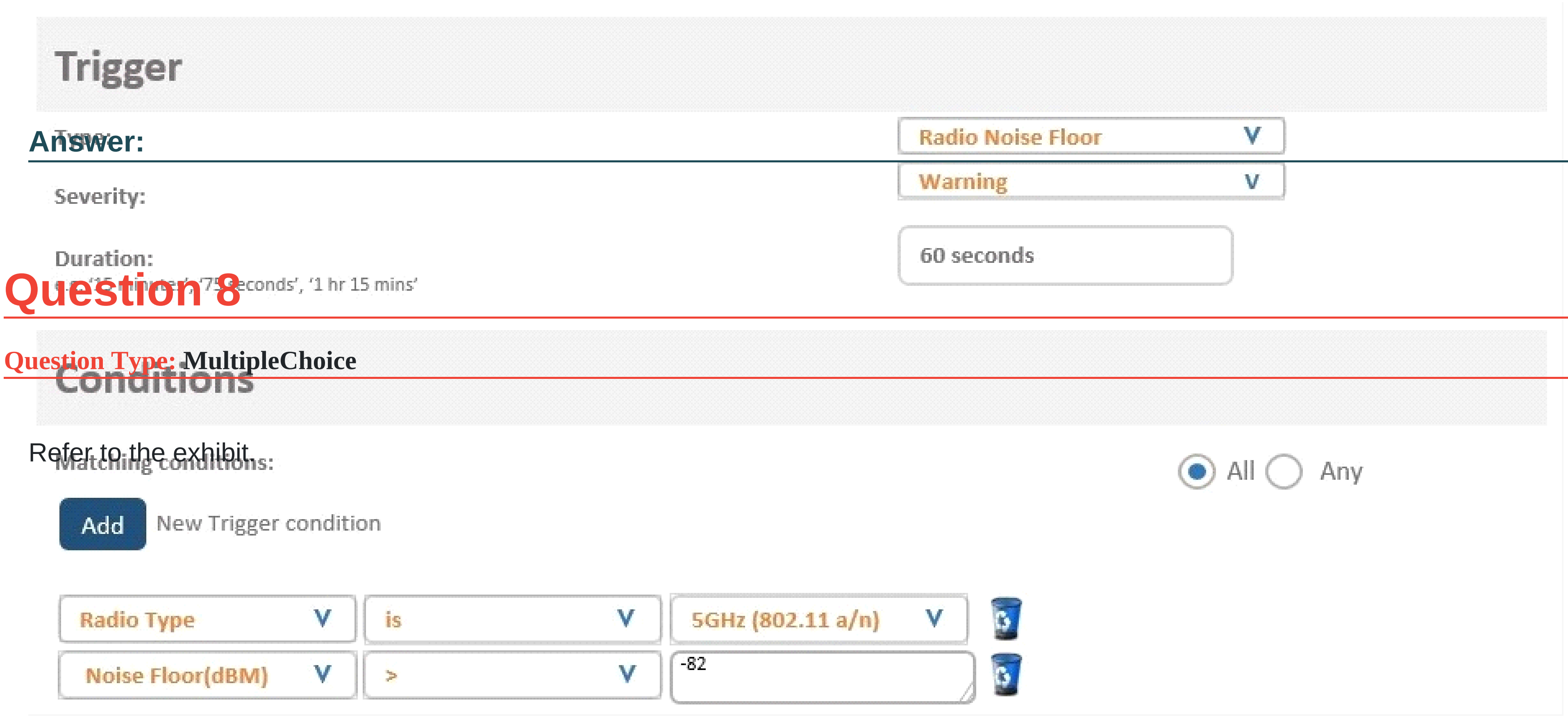
Which alarm definition must the network administrator create to accomplish this?

Answer:

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



Trigger

Type: Radio Noise Floor

Severity: Warning

Duration: 60 seconds

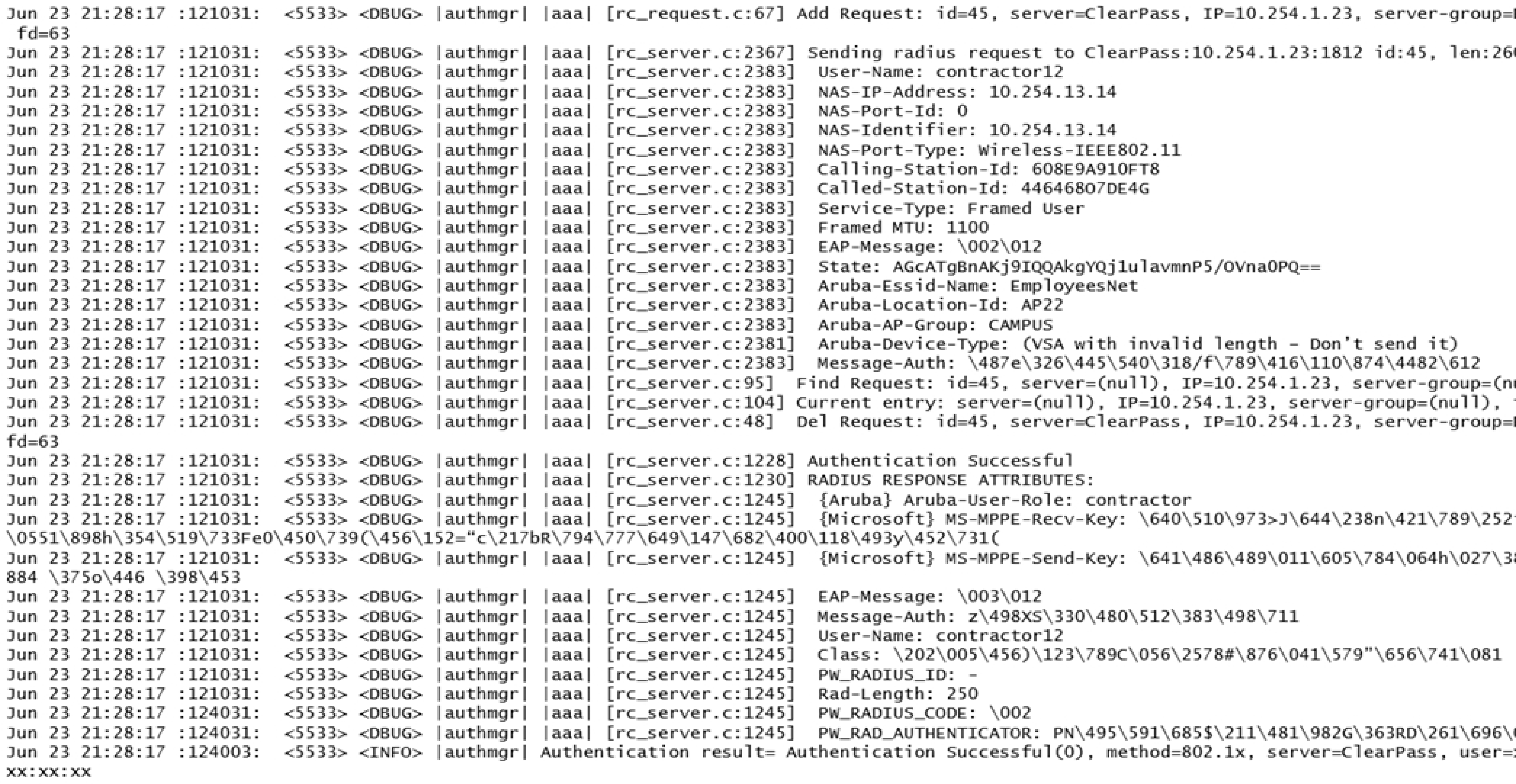
e.g. '15 minutes', '75 seconds', '1 hr 15 mins'

Conditions

Matching conditions: ● All ○ Any

Add New Trigger condition

Radio Type	is	5GHz (802.11 a/n)
Noise Floor(dBM)	>	-82



```
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=
 fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass:10.254.1.23:1812 id:45, len:26
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  User-Name: contractor12
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-IP-Address: 10.254.13.14
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Id: 0
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Identifier: 10.254.13.14
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Type: Wireless-IEEE802.11
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Calling-Station-Id: 608E9A910FT8
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Called-Station-Id: 446468O7DE4G
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Service-Type: Framed User
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Framed MTU: 1100
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  EAP-Message: \002\012
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  State: AGcATgBnAKj9IQQAkgYQj1ulavmnP5/OVnaOPQ==
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Essid-Name: EmployeesNet
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Location-Id: AP22
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-AP-Group: CAMPUS
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2381]  Aruba-Device-Type: (VSA with invalid length - Don't send it)
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Message-Auth: \487e\326\445\540\318/f\789\416\110\874\4482\612
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:95]  Find Request: id=45, server=(null), IP=10.254.1.23, server-group=(n
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:104] Current entry: server=(null), IP=10.254.1.23, server-group=(null), 
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:48]  Del Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=
fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1228] Authentication Successful
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Aruba} Aruba-User-Role: contractor
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Microsoft} MS-MPPE-Recv-Key: \640\510\973>J\644\238n\421\789\252
\0551\898h\354\519\733FeO\450\739(\456\152="c\217bR\794\777\649\147\682\400\118\493y\452\731(
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Microsoft} MS-MPPE-Send-Key: \641\486\489\011\605\784\064h\027\3
884 \375o\446 \398\453
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  EAP-Message: \003\012
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Message-Auth: z\498XS\330\480\512\383\498\711
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  User-Name: contractor12
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Class: \202\005\456)\123\789C\056\2578#\876\041\579"\656\741\081
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RADIUS_ID: -
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Rad-Length: 250
Jun 23 21:28:17 :124031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RADIUS_CODE: \002
Jun 23 21:28:17 :124031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RAD_AUTHENTICATOR: PN\495\591\685$\211\481\982G\363RD\261\696\
Jun 23 21:28:17 :124003:  <5533> <INFO> |authmgr| Authentication result= Authentication Successful(0), method=802.1x, server=ClearPass, user=
xx:xx:xx
```

A network administrator wants to allow contractors to access the WLAN named EmployeesNet. In order to restrict network access, the network administrator wants to assign this category of users to the contractor user role. To do this, the network administrator configures

ClearPass in a way that it returns the Aruba-User-Role with the contractor value.

When testing the solution, the network administrator receives the wrong role.

What should the network administrator do to assign the contractor role to contractor users without affecting any other role assignment?

Options:

A- Check the Download role from the CPPM option in the AAA profile.

B- Set contractor as the default role in the AAA profile.

C- Create Contractor firewall role in the M.

D- Create server deviation rules in the server group.

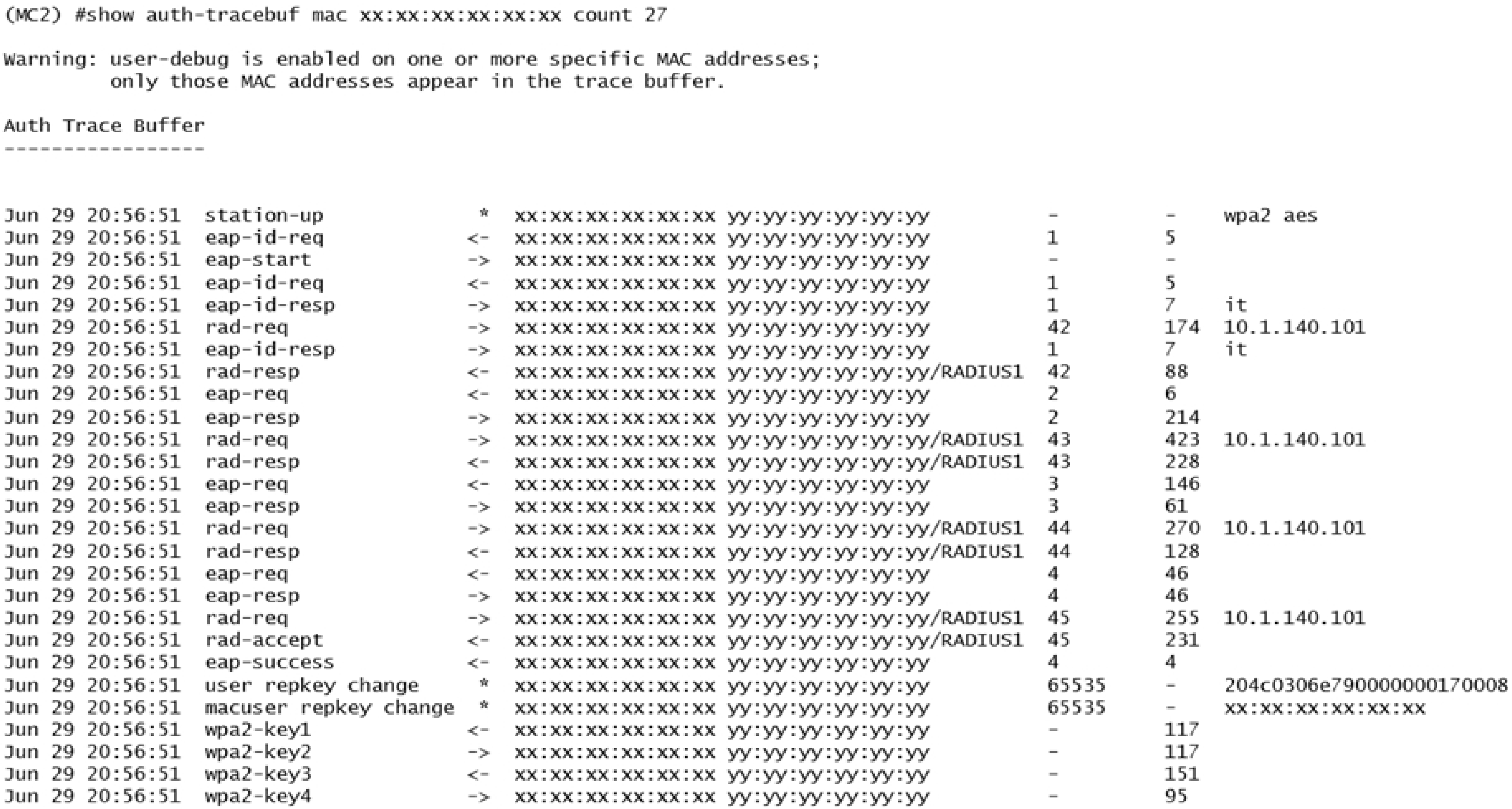
Answer:

A

Question 9

Question Type: **MultipleChoice**

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
```

Based on the output shown in the exhibit, which wireless connection phase has just completed?

Options:

A- L3 authentication and encryption

B- MAC Authentication and 4-way handshake

C- 802.11 enhanced open association

D- L2 authentication and encryption

Answer:

A