Free Questions for HPE6-A79 by ebraindumps

Shared by Reyes on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization owns a fully functional multi-controller Aruba network with a Virtual Mobility Master (VMM) in VLAN20. They have asked a network consultant to deploy a redundant MM on a different server. The solution must offer the lowest convergence time and require no human interaction in case of failure.

The servers host other virtual machines and are connected to different switches that implement ACLs to protect them. The organization grants the network consultant access to the servers only, and appoints a network administrator to assist with the deployment.

What must the network administrator do so the network consultant can successfully deploy the solution? (Choose two.)

Options:

A- Allocate VLAN20 to the second server, and extend it throughout the switches, then reserve one IP address for the second MM and another IP address for its gateway.

B- Allocate VLAN20 to the second server, and permit routing between them, then reserve one IP address for the second MM and another IP address for its gateway.

C- Configure an ACL entry that permits IP protocol 50, UDP port 500, and multicast IP 224.0.0.18.

D- Allocate VLAN20 to the second server, and extend it throughout the switches, then reserve one IP address for the second MM and another for the VIP.

E- Configure an ACL entry that permits UDP 500, TCP 4500, and multicast IP 224.0.0.5.

Answer:

A, E

Question 2

Question Type: **MultipleChoice**

Refer to the exhibits.

Exhibit 1

```
(MC2) [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/Phy
      Profile  Forward mode Type     Host Name   User Type
---------    ----------             -----   ----                  ---------  ----    -------  --------  -------  --------------
     -------      ------------      ----- --------   -------
192.168.14.101  xx:xx:xx:xx:xx:xx            guest-guest-logon     00:00:32                  AP1       Wireless  Guest/yy:yy:yy:yy:yy:yy/a-
VHT  Guest    tunnel         Win 10              WIRELESS

User Entries: 1/1
  Curr/Cum Alloc:2/5 Free:0/3 DVN:2 AllocErr:0 FreeErr:0
```

Exhibit 2

```
(MC2) [MDC] #show rights guest-guest-logon

Valid = 'Yes'
CleanedUp = 'No'
Derived Role = 'guest-guest-logon'
  Up BW:No Limit   Down BW:No Limit
  L2TP Pool = default-l2tp-pool
  PPTP Pool = default-pptp-pool
  Number of users referencing it = 2
  Periodic reauthentication: Disabled
  DPI Classification: Enabled
  Youtube education: Disabled
  Web Content Classification: Enabled
  IP-Classification Enforcement: Enabled
  ACL Number = 98/0
  Openflow: Enabled
  MaxSessions = 65535

  Check CP Profile for Accounting = TRUE
  Captive Portal profile = default
```

Exhibit 3

```
(MC2) [MDC] #show aaa authentication captive-portal Guest

Captive Portal Authentication Profile “Guest”
---------------------------------------------
Parameter                                   Value
---------                                   -----
Default Role                                guest
Default Guest Role                          guest
Server Group                                Guest
Redirect Pause                              10 sec
User Login                                  Enabled
Guest Login                                 Disabled
Logout popup window                         Enabled
Use HTTP for authentication                 Disabled
Logon wait minimum wait                     5 sec
Logon wait maximum wait                     10 sec
Logon wait CPU utilization threshold        60%
Max Authentication failures                 0
Show FQDN                                   Disabled
Authentication Protocol                     PAP
Login page                                  https://cp.mycompany.com/guest/web_login.php
Welcome page                                /auth/welcome.html
Show Welcome Page                           Yes
```

Exhibit 4

```
(MC2) [MDC] #show aaa authentication captive-portal default

Captive Portal Authentication Profile "default"
-----------------------------------------------
Parameter                                       Value
---------                                       -----
Default Role                                    guest
Default Guest Role                              guest
Server Group                                    Guest
Redirect Pause                                  10 sec
User Login                                      Enabled
Guest Login                                     Disabled
Logout popup window                             Enabled
Use HTTP for authentication                     Disabled
Logon wait minimum wait                         5 sec
Logon wait maximum wait                         10 sec
Logon wait CPU utilization threshold            60%
Max Authentication failures                     0
Show FQDN                                       Disabled
Authentication Protocol                         PAP
Login page                                      /auth/index.html
Welcome page                                    /auth/welcome.html
Show Welcome Page                               Yes
Add switch IP addresses in the redirection URL  Disabled

(MC2) [MDC] #show aaa server-group default

Fail Through: No
Load Balance: No

Auth Servers
------------
Name        Server-Type    trim-FQDN   Match-Type  Match-Op  Match-Str
----        -----------    ---------   ----------  --------  ---------
Internal    Internal       No

Role/VLAN derivation rules
--------------------------
Priority   Attribute   Operation   Operand   Type    Action    Value   Validated
--------   ---------   ---------   -------   ----    ------    -----   ---------
```

A captive portal-based solution is deployed in a Mobility Master (MM) - Mobility Controller (MC) network. A wireless station connects to the network and attempts the authentication process. The outputs are shown in the exhibits.

Which names correlate with the authentication and captive portal servers?

Options:

A- ClearPass.23 is the authentication server, and cp.mycompany.com is the captive portal server.

B- ClearPass.23 is the authentication server, and MC2 is the captive portal server.

C- Internal database in MC2 is the authentication server, and cp.mycompany.com is the captive portal server.

D- cp.mycompany.com is the authentication server, and ClearPass.23 is the captive portal server.

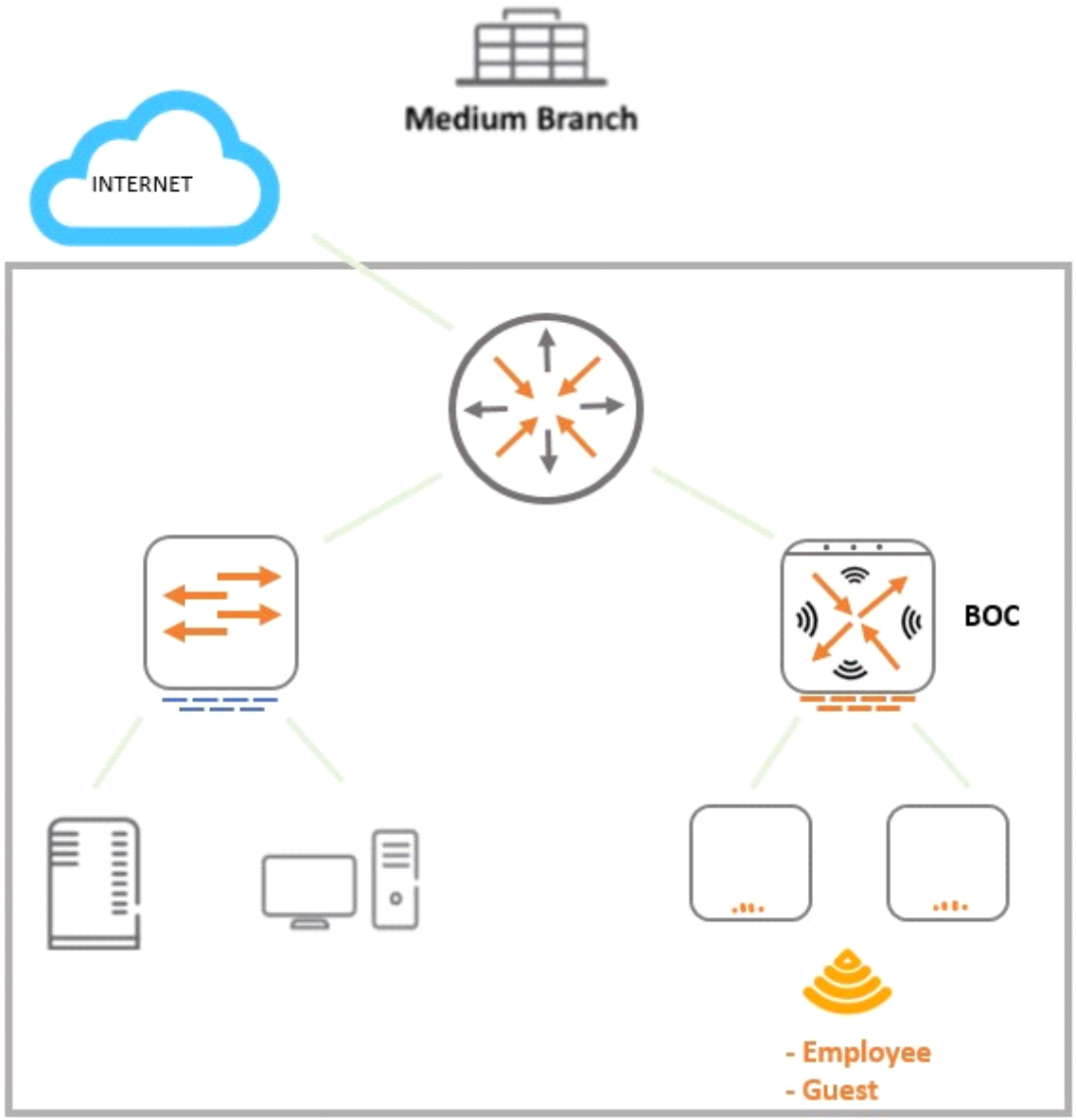
Answer:

A

Question 3

Question Type: MultipleChoice

Refer to the exhibit.


Medium Branch
INTERNET
BOC
- Employee
- Guest

A 7008 Branch Office Controller (BOC) is deployed in a remote office behind a core router. This core does not support 802.1q encapsulation. The Mobility Controller (MC) is the gateway for two tunneling mode SSIDs, as shown in the exhibit.

Which two different configuration options ensure that wireless users are able to reach the branch network through the router? (Choose two.)

Options:

A- Configure all ports of the BOC as access ports on the controller VLAN, and change the gateway of clients to the core router IP.

B- Configure the uplink of the BOC as an access port on the controller VLAN, and add static routes in the router for the SSID VLAN subnets.

C- Configure the uplink of the BOC as a trunk port that permits the controller and the SSID VLANs. The controller VLAN must be native.

D- Configure the uplink of the BOC as an access port on the controller VLAN, and enable NAT for the SSID VLANs.

E- Configure the uplink of the BOC as a trunk port, tagging the controller and the SSOD VLANs, and enable NAT for the SSID VLANs.

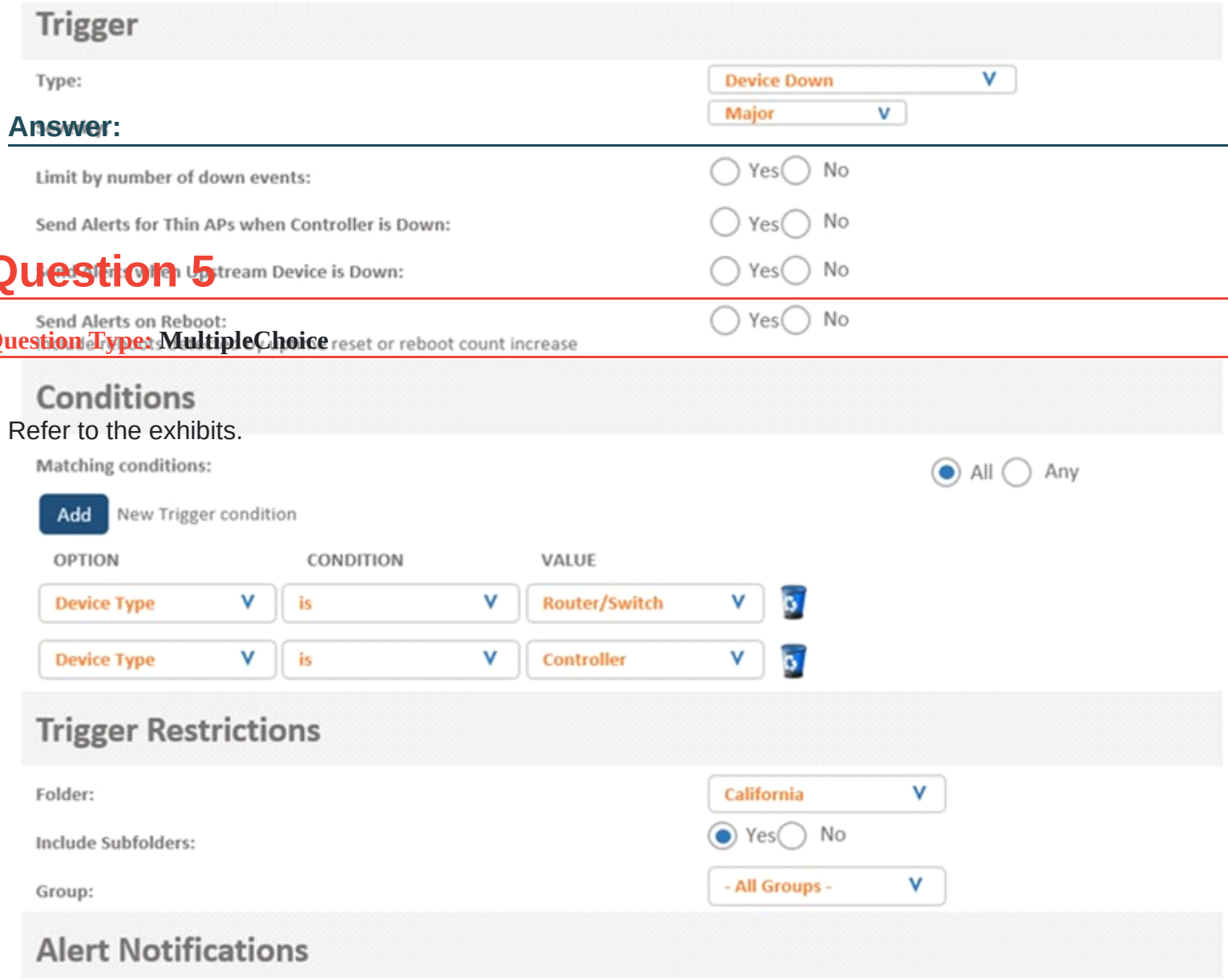
Answer:

B, E

Question 4

Question Type: **Hotspot**

A network administrator wants to receive a major alarm every time a controller or an Aruba switch goes down for either a local or an upstream device failure. Which alarm definition must the network administrator create to accomplish this?

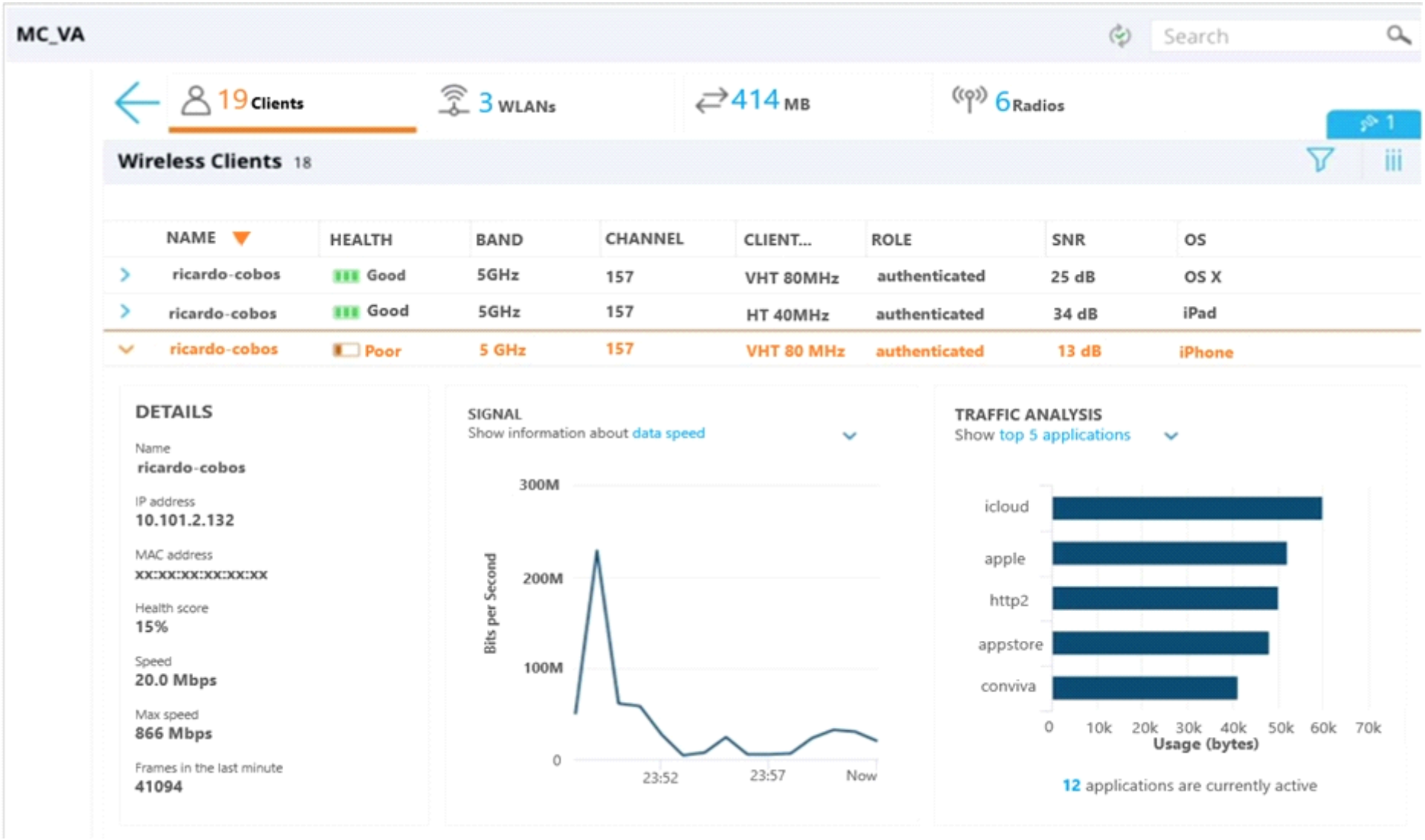


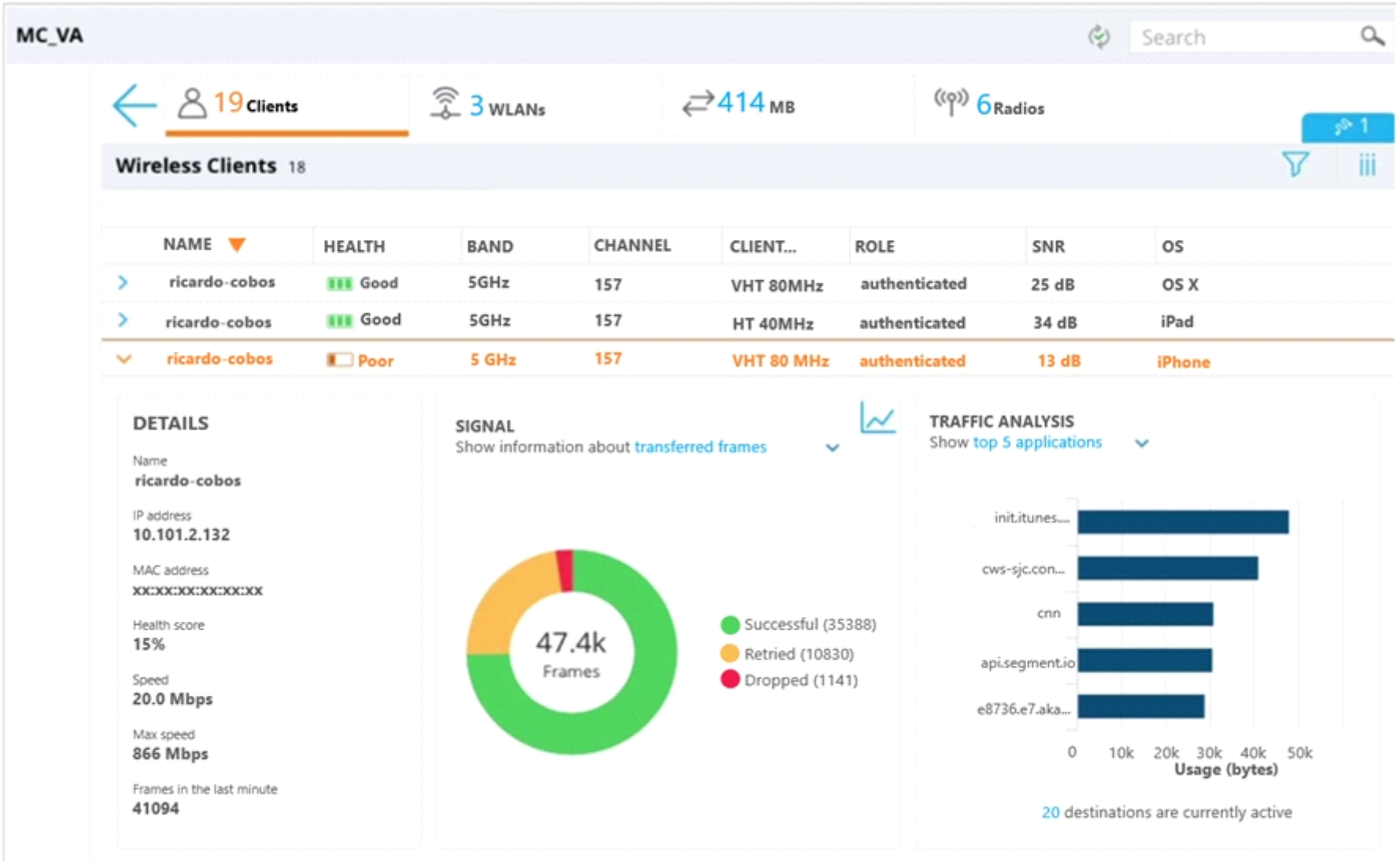
Answer:

Question 5

Question Type: MultipleChoice

Refer to the exhibits.


MC_VA
Search
19 Clients
3 WLANs
414 MB
6 Radios
1
Wireless Clients 18
NAME
HEALTH
BAND
CHANNEL
CLIENT...
ROLE
SNR
OS
ricardo-cobos Good 5GHz 157 VHT 80MHz authenticated 25 dB OS X
ricardo-cobos Good 5GHz 157 HT 40MHz authenticated 34 dB iPad
ricardo-cobos Poor 5 GHz 157 VHT 80 MHz authenticated 13 dB iPhone
DETAILS
Name
ricardo-cobos
IP address
10.101.2.132
MAC address
xx:xx:xx:xx:xx:xx
Health score
15%
Speed
20.0 Mbps
Max speed
866 Mbps
Frames in the last minute
41094
SIGNAL
Show information about data speed
300M
200M
100M
0
Bits per Second
23:52
23:57
Now
TRAFFIC ANALYSIS
Show top 5 applications
icloud
apple
http2
appstore
conviva
0
10k
20k
30k
40k
50k
60k
70k
Usage (bytes)
12 applications are currently active



A user reports slow response time to a network administrator and suggests that there might be a problem with the WLAN. The user's phone supports 802.11ac in the 5 GHz band. The network administrator finds the user in the Mobility Master (MM) and reviews the

output shown in the exhibit.

What can the network administrator conclude after analyzing the data?

Options:

A- The low SNR forces the client to back off to low MCs. therefore speed is low and retransmits are high.

B- Client health is poor, but SNR is fair. TX power must be increased in both the client and the AP.

C- Since SNR is good, then the high retransmit rate must be due a hidden node scenario or high interference.

D- High Successful frame count and high Max Speed is an indication of a healthy client. Connection will improve at anytime.

Answer:

D

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit.

```
(MC1) [MDC] #show aaa profile corp_aaa_prof

AAA Profile "corp_aaa_prof"
-----------------------
```

Parameter	Value
Initial role	logon
MAC Authentication Profile	N/A
MAC Authentication Default Role	guest
MAC Authentication Server Group	default
802.1X Authentication Profile	corp-employee_dot1_aut
802.1X Authentication Default Role	guest
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
XML API server	N/A
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 created AAA profile for the corporate VAP. In addition to the regular Radius based authentication, the administrator needs to be able to disconnect the users from either of the two servers that are part of the "Radius" server group.

What must the administrator do next in order to achieve this goal?

Options:

A- Use the 'Radius' server group as the RADIUS Accounting Server Group in the AAA profile.

B- Create two new RFC 3576 servers and assign them as the RFC 3576 servers in the AAA profile.

C- Use the 'Radius' server group as both the Accounting Server Group and the RFC 3576 server in the AAA profile.

D- Use the 'Radius' server group as the RFC 3576 server in the AAA profile.

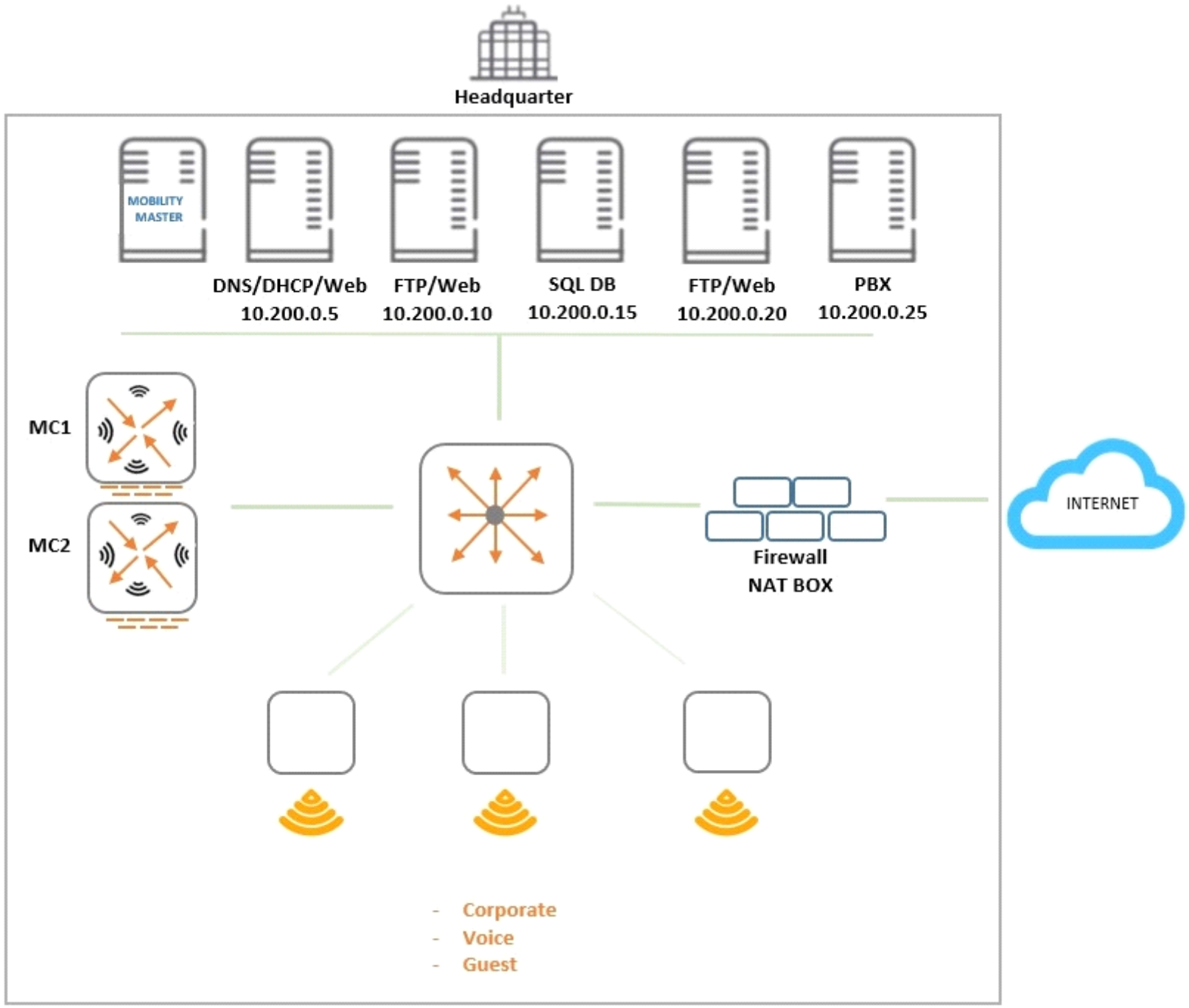
Answer:

C

Question 7

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 8

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

Question 9

Question Type: MultipleChoice

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	xx:xx:xx:xx:xx:xx	2018-07-25_07:50:05	100	80MHz	149	80MHz	AP2
5GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-24_07:48:42	124	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	xx:xx:xx:xx:xx:xx	2018-07-23_16:44:36	100	80MHz	124	80MHz	AP2
5GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_19:12:34	157	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_10:02:30	100	80MHz	157	80MHz	AP2
5GHz	RADAR_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_08:34:31	56	80MHz	100	80MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-25_08:31:31	11	20MHz	6	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-25_08:31:31	6	20MHz	1	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-24_07:46:34	1	20MHz	11	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-24_07:46:33	6	20MHz	1	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-23_15:13:15	11	20MHz	6	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-23_15:12:12	1	20MHz	11	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_08:07:27	11	20MHz	1	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-20_08:07:26	6	20MHz	11	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-19_19:22:45	1	20MHz	6	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	2018-07-19_19:22:44	11	20MHz	1	20MHz	AP2
2GHz	NOISE_DETECT	xx:xx:xx:xx:xx:xx	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, and then they are suddenly disconnected. This 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, what is the most likely reason users get disconnected?

Options:

A- Adaptive Radio Management is reacting to RF events.

B- AirMatch is applying a scheduled optimization solution.

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

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

Answer:

C