DUMPSARENA

Aruba Certified Mobility Expert Written Exam

HP HPE6-A79

Version Demo

Total Demo Questions: 10

Total Premium Questions: 55

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A network administrator has updated the ArubaOS code of a standalone Mobility Controller (MC) that is used for User-Based Tunneling (UBT) to a newer early release. Ever since the MC seems to reject PAPI sessions from the switch with the 10.1.10.10 IP address. Also the controller's prompt is now followed by a star mark: "(MC_VA) [mynode] *#"

When opening a support ticket, an Aruba TAC engineer asks the administrator to gather the crash logs and if possible replicate UBT connection attempts from the switch while running packet captures of PAPI traffic on the controller and obtain the PCAP files. The administrator has a PC with Wireshark and TFTP server using the 10.0.20.20 IP address.

What commands must the administrator issue to accomplish these requests? (Choose two.)

A.
```
packet-capture destination ip-address 10.0.20.20
packet-capture datapath ipsec 10.1.10.10
```

B.
```
show tech-support logs.tar
copy flash: logs.tar tffp: 10.0.20.20 logs.tar
copy flash: logs.tar_md5sum.txt tffp: 10.0.20.20 logs.tar_md5sum.txt
```

C.
```
tar logs
copy flash: logs.tar tffp: 10.0.20.20 logs.tar
copy flash: logs.tar_md5sum.txt tffp: 10.0.20.20 logs.tar_md5sum.txt
```

D.
```
tar crash
copy flash: logs.tar tffp: 10.0.20.20 crash.tar
copy flash: logstarmd5sum.txt tffp: 10.0.20.20 crash.tarmd5sum.txt
```

E.
```
packet-capture destination ip-address 10.0.20.20
packet-capture controlpath udp all
```

A. Option A

B. Option B

C. Option C

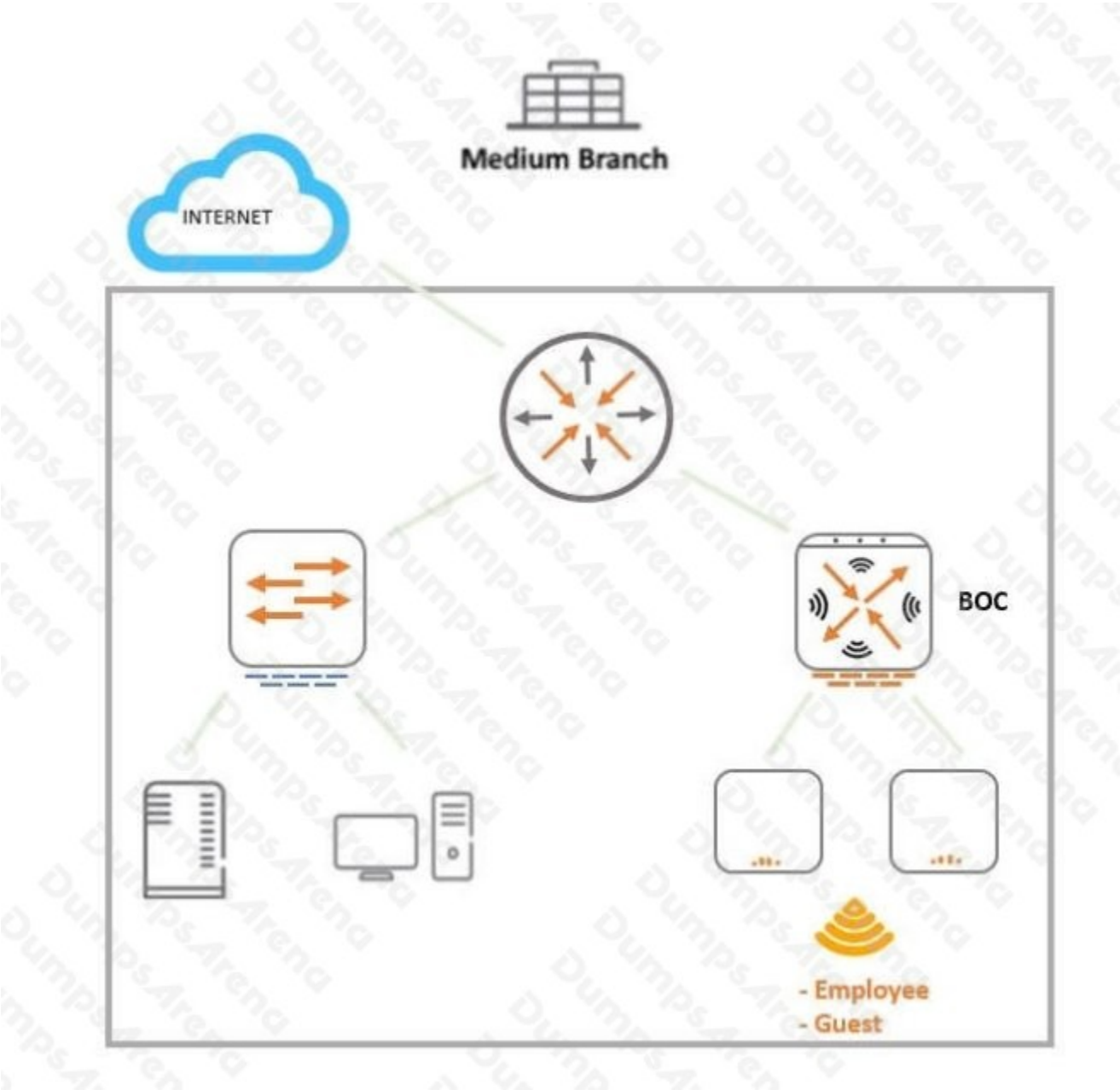
D. Option D

E. Option E

ANSWER: B E

QUESTION NO: 2

Refer to the exhibit.



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.)

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 NO: 3

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.)

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 NO: 4

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.

ANSWER: D

QUESTION NO: 5

A network administrator has racked up a 7210 Mobility Controller (MC) that will be terminating 200+ Aps on a medium-size branch office. Next, the technician cabled the appliance with 4SPF+ Direct Attached Cables (DACs) distributed between two-member switching stack and powered it up.

What must the administrator do next in the MCs to assure maximum wired bandwidth utilization?

A. Map the four physical ports to port channel 0.

B. Disable spanning tree and allocate unique VLANs to each port.

C. Manually set 10Gbps speeds on all ports.

D. Configure the same MSTP region that the switches have.

E. Make all ports trunk interfaces and permit data VLANs.

ANSWER: C

QUESTION NO: 6

A company with 535 users deploys an Aruba solution with more than 1000 Aruba APs, two 7220 Mobility Controllers, and a single Mobility Master (MM) virtual appliance at the campus server farm. The MCs run a HA Fast failover group in dual mode and operate at 50% AP capacity.

If there is an MM or MC failure, the network administrator must ensure that the network is fully manageable and the MC load does not exceed 80%.

What can the network administrator do to meet these requirements?

A. Place the APs in the same hierarchy level.

B. Create a cluster with AP load balancing.

C. Enable oversubscription in the HA group.

D. Add an MC and an MM in the server farm.

E. Add an MM and enable DC redundancy.

F. Place the APs in two different AP-Groups.

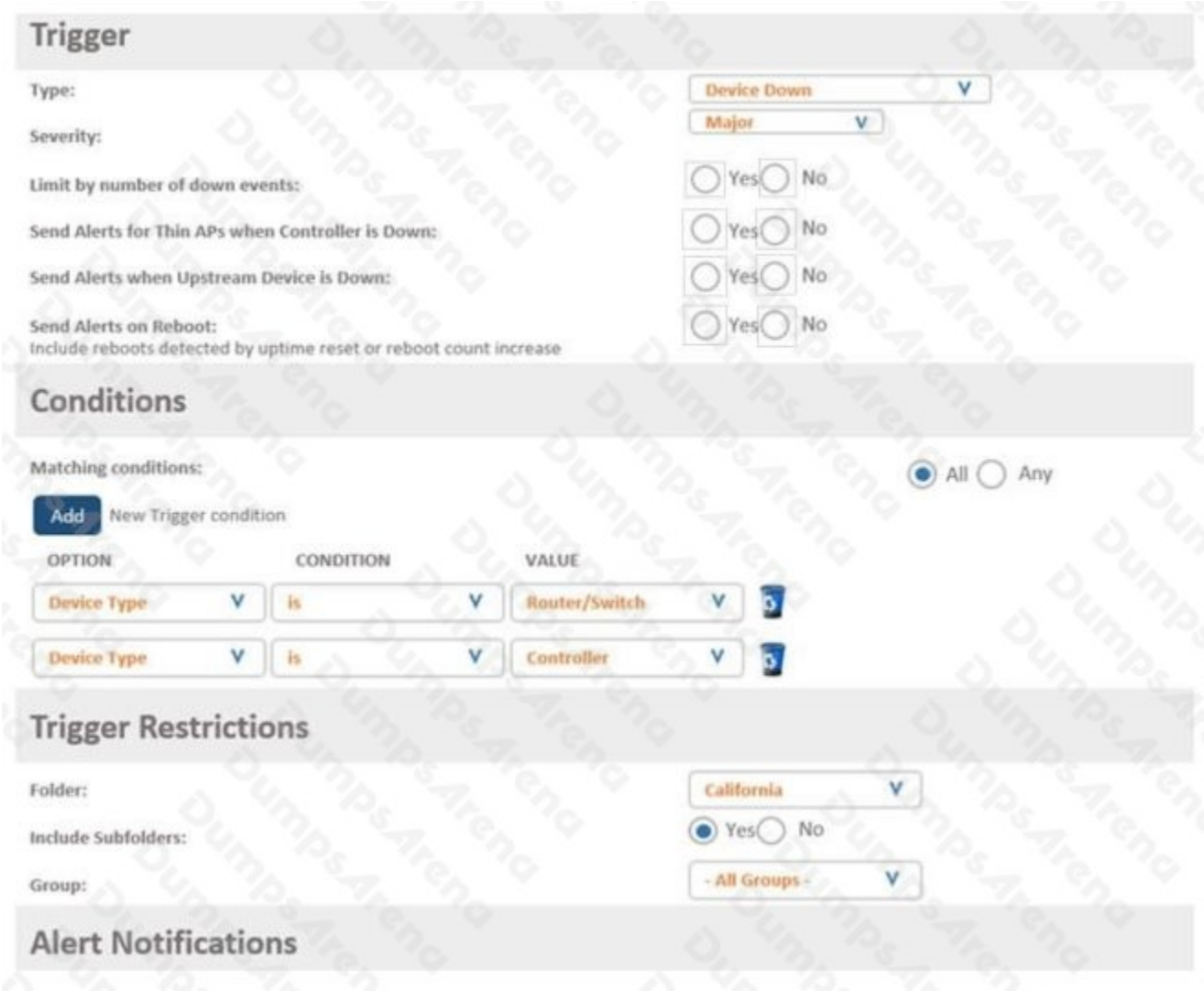
ANSWER: E

QUESTION NO: 7 - (HOTSPOT)

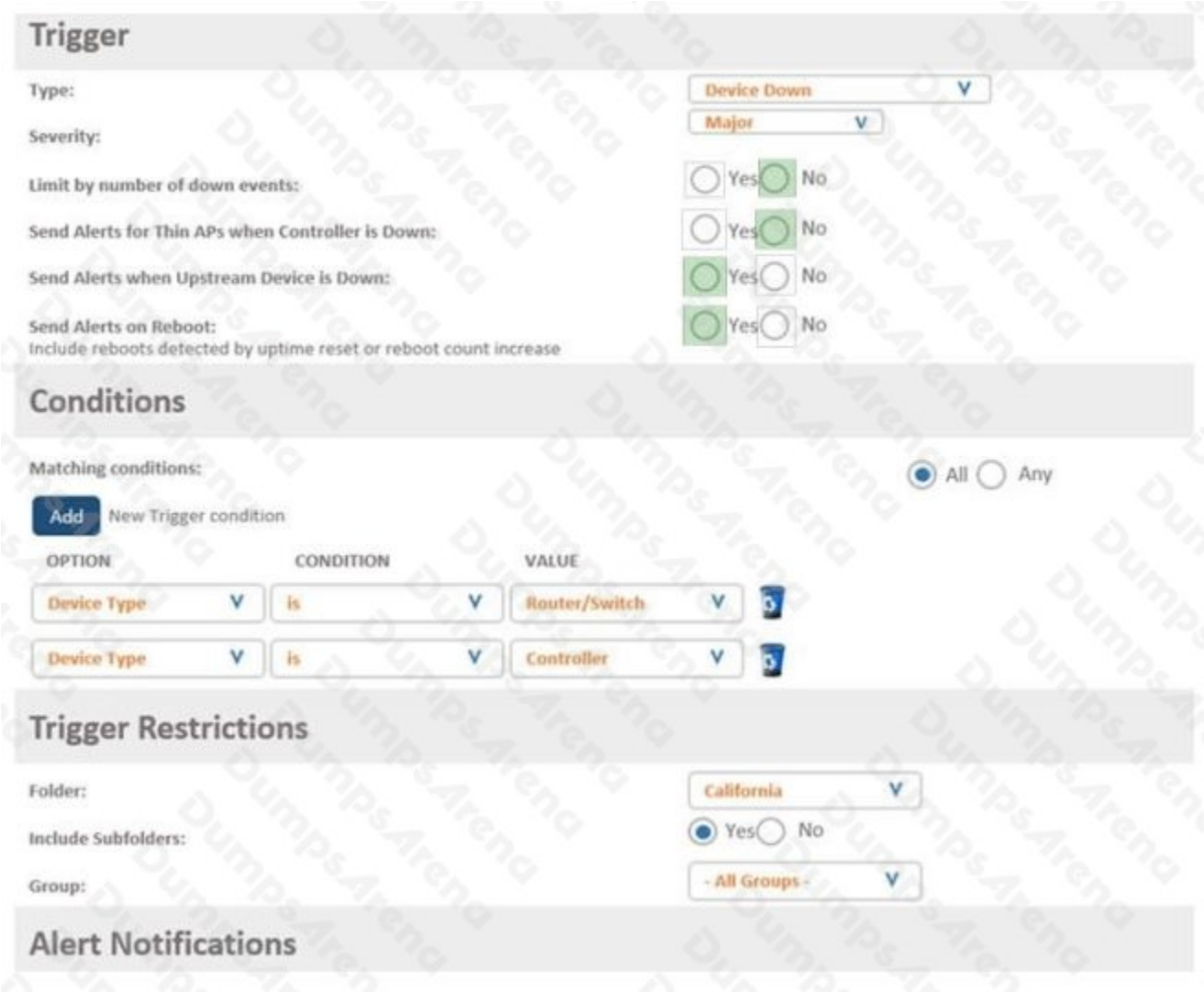
HOTSPOT

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?

Hot Area:


Trigger
Type:
Device Down
Severity:
Major
Limit by number of down events:
Yes No
Send Alerts for Thin APs when Controller is Down:
Yes No
Send Alerts when Upstream Device is Down:
Yes No
Send Alerts on Reboot:
Include reboots detected by uptime reset or reboot count increase
Yes No
Conditions
Matching conditions:
All Any
Add
New Trigger condition
OPTION
CONDITION
VALUE
Device Type
is
Router/Switch
Device Type
is
Controller
Trigger Restrictions
Folder:
California
Include Subfolders:
Yes No
Group:
- All Groups -
Alert Notifications

ANSWER:



Explanation:

QUESTION NO: 8

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.)

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 NO: 9

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.

ANSWER: A

QUESTION NO: 10

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.

ANSWER: D