HP2-Z33 Q&As

HP Unified Wired-Wireless Networks and BYOD

Pass HP HP2-Z33 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/hp2-z33.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

The Wireless Intrusion Prevention System (WIPS) determines that a client has exceeded the maximum number of authentication requests that a client should make in the allowed period. What does the WIPS system do?

A. adds the client\\'s MAC address to the static blacklist on the access controller

B. adds the client\\'s MAC address to the static blacklist on the access point

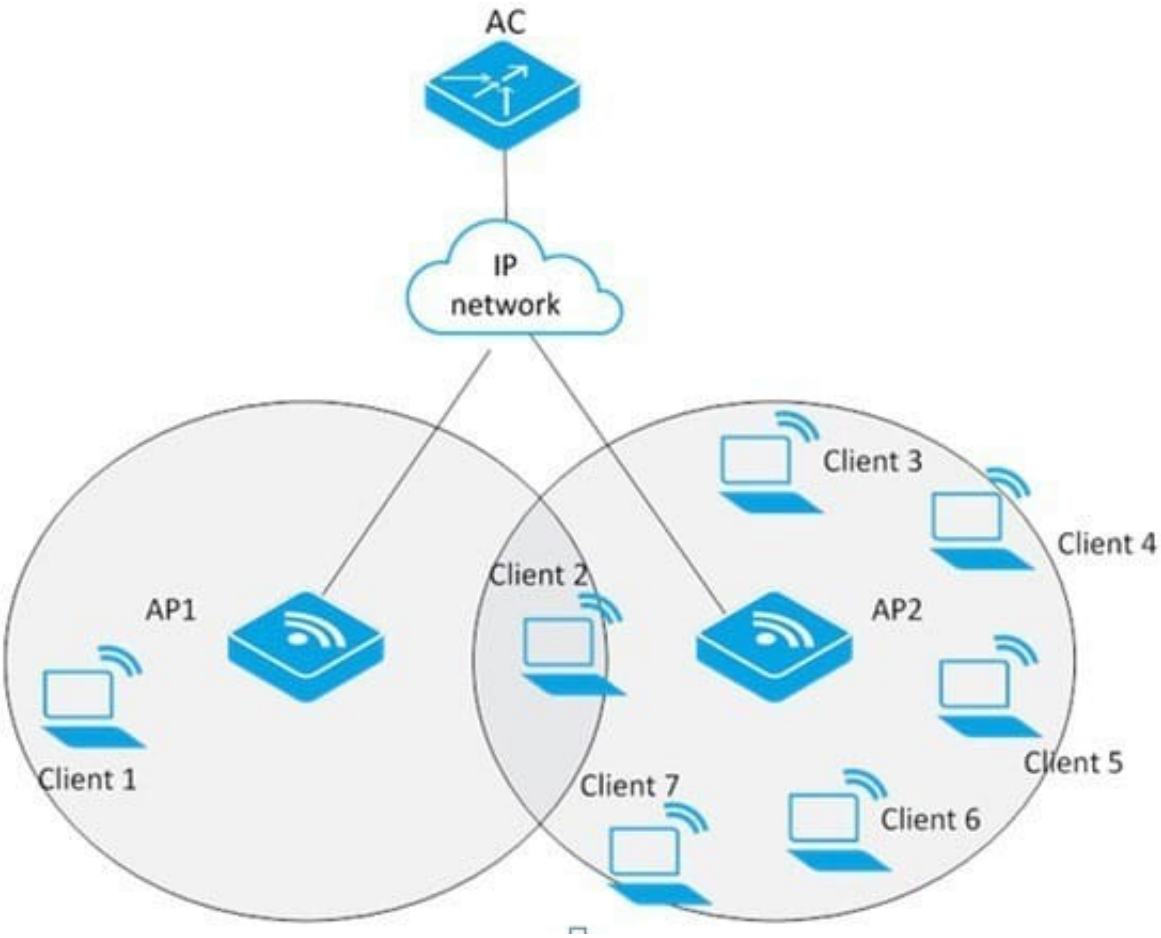
C. adds the client\\'s MAC address to the dynamic blacklist for the access point

D. removes the client\\'s MAC address from the whitelist on the access controller

Correct Answer: C

QUESTION 2

Refer to the exhibit.



The access controller (AC) has configured session-mode load balancing. The maximum number of sessions is configured as 5. The maximum session gap is configured as 4. Client 1 is associated with API Clients 2 to 6 are associated with AP2. Client 7 can only hear AP2. Client 7 attempts to associate to AP2.

What happens?

A. AP2 allows client 7 to associate with it, after client 7 sends multiple association attempts to AP2.

B. AP2 accepts client 7 association requests and forces client 2 to connect to AP1 by sending client 2 a disassociation request

C. AP2 accepts client 7 association requests, as the load balancing threshold values have not been met.

D. AP2 rejects all client 7 association requests.

Correct Answer: D

QUESTION 3

An organization implements an N+1 redundancy for its access controllers (ACs). When the primary AC fails, the access points (APs) successfully fail over to the standby AC. However, when the failed AC comes back in to service, the APs do not switch back to the original AC.

What could cause this to happen?

A. AP Connection priority on the primary AC is not set to 1.

B. APs determine which AC to connect to based on load.

C. APs do not fail back to the original AC.

D. AP Connection priority on the primary AC is not set to 7.

Correct Answer: D

QUESTION 4

HP has released a new version of an access controller software package file. How does the network administrator activate the new software version?

A. by interrupting the boot sequence and selecting the Update Bootware option

B. by interrupting the boot sequence and selecting the Boot Extend Bootware option

C. by interrupting the boot sequence and selecting the Boot Backup Bootware option

D. by interrupting the boot sequence and selecting the Update Full Bootware option

Correct Answer: B

QUESTION 5

To allow user access for corporate employees, a network administrator sets an SSID named CORPORATE using an HP Unified Wireless solution. The administrator wants these security enhancements: Enable 802.1x authentication in PEAP MS-CHAP V2 mode on this SSID along with AES and WPA2.

Set the User Access Manager server at 10.0.1.100 to authenticate 802.1x supplicants.

The network administrator enters these commands:

▪

```
radius scheme radius-uam
 server-type extended
 primary authentication 10.0.1.100
 primary accounting 10.0.1.100
 key authentication simple password1.
 key accounting simple password1.
 user-name-format without-domain
 quit
domain uam
 authentication lan-access radius-scheme radius-uam
 authorization lan-access radius-scheme radius-uam
 accounting lan-access radius-scheme radius-uam quit
```

What is another set of commands that must be entered onto the Unified Wireless Controller in system-view mode to define the SSID CORPORATE with 802.1X Authentication in PEAP MSCHAPV2, using the defined RADIUS server?

A
```
dot1x authentication-method chap

interface WLAN-ESS11
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain uam
 undo dot1x multicast-trigger

wlan service-template 11 crypto
 ssid CORPORATE
 bind WLAN-ESS 11
 cipher-suite tkip
 security-ie rsn
 service-template enable
```

B
```
dot1x authentication-method eap

interface WLAN-ESS11
  port-security port-mode userlogin-secure-ext
  port-security tx-key-type 11key
  undo dot1x handshake
  dot1x mandatory-domain radius-uam
  undo dot1x multicast-trigger

wlan service-template 11 crypto
 ssid CORPORATE
 bind WLAN-ESS 11
 cipher-suite ccmp
 security-ie rsn
 service-template enable
```

C
```
dot1x authentication-method eap

interface WLAN-ESS11
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain radius-uam
 undo dot1x multicast-trigger

wlan service-template 11 crypto
 ssid CORPORATE
 bind WLAN-ESS 12
 cipher-suite tkip
 security-ie rsn
 service-template enable
```

D
```
dot1x authentication-method eap

interface WLAN-ESS11
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain radius-uam
 undo dot1x multicast-trigger

wlan service-template 11 open
 ssid CORPORATE
 bind WLAN-ESS 11
 cipher-suite tkip
 security-ie rsn
 service-template enable
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D