HP.HPE7-A07.v2024-07-01.q22

試験コード:	HPE7-A07
試験名称:	Aruba Certified Campus Access Mobility Expert Written Exam
認定資格:	HP
無料問題数:	22
バージョン:	v2024-07-01
アクセス数:	215
ページビュー数:	220
https://www.jpnpdf.com/HP.HPE7-A07.v2024-07-01.q22-mondaishu.html	

最新問題: **1**
顧客は CX 6300 スイッチのデバイス プロファイルを評価しています。テスト デバイスには次の属性があります。

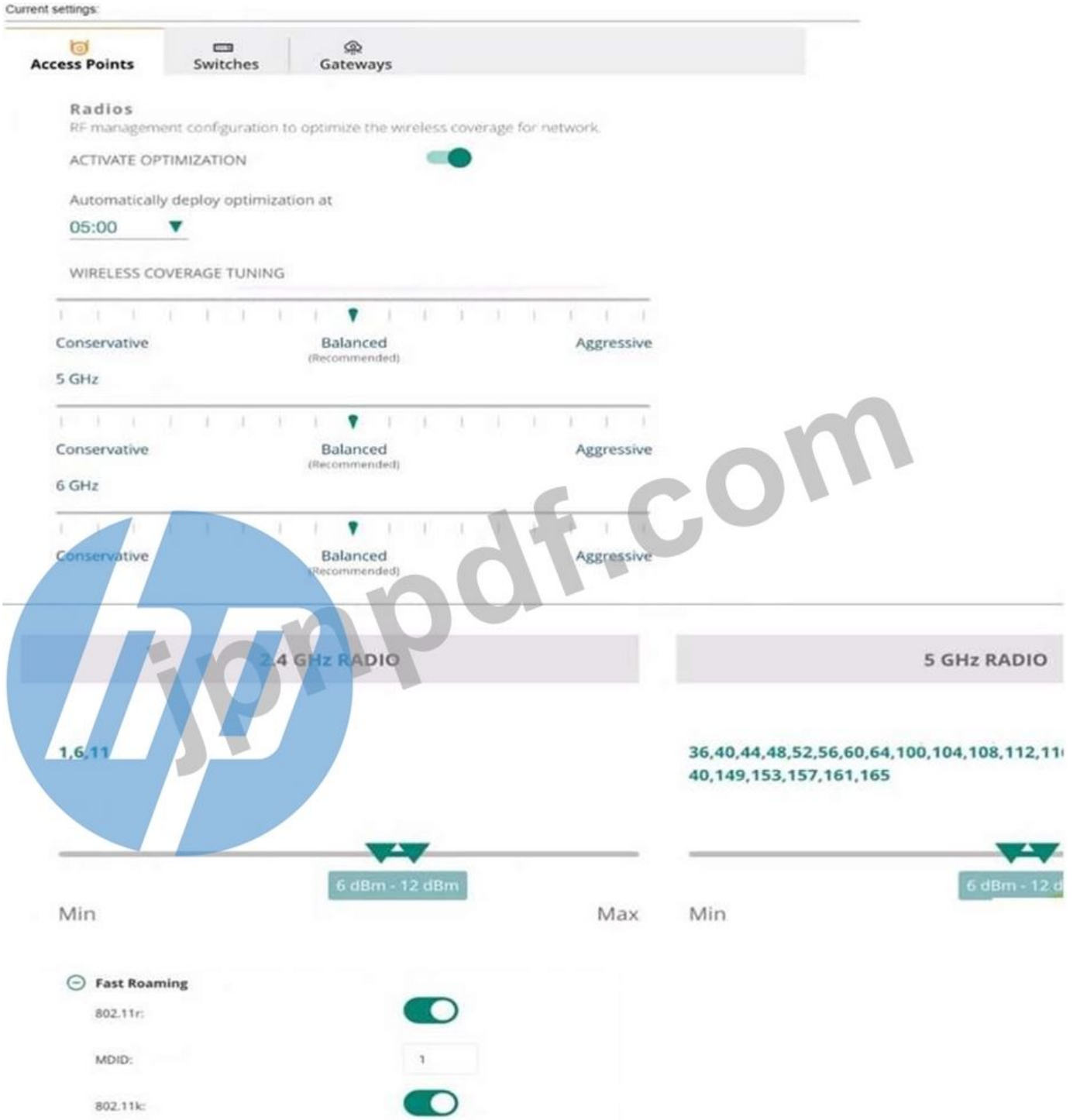
```
mac-group iot
     seq 10 match mac-oui 81:cd:93

port-access device-profile iot-prod
    enable
    associate role iot-prod
    associate mac-group it
```

* MAC アドレス=81:cd:93:13:ab:31
テスト デバイスには「Iot-prod」ロールを割り当てる必要があり、さらにインターフェイス 1/1/1 に接続されている他のデバイスには「Iot-default」ロールを適用する必要があります。これは、テスト用の外部認証サーバー。
構成例を考えると、このテスト要件を満たすには何が必要でしょうか?
A. インターフェイス 1/1/1 に対してコマンド「Iot-access device-profile mode block-until-profile-applied」を入力します。
B. コマンド「port-access fallback-role Lot-default global」を入力します。
C. コマンド「port-access onboarding-method precedence」を入力して、デバイス プロファイルの優先順位を低く設定します。
D. コマンド「port-access device-profile mode block-until-profile-applied」をグローバルに入力します。
Answer: B (メーッセージを残す)
フォールバック ロールは、指定されたロールがない場合、または認証サーバーが使用できない場合に、デフォルトのロールとして使用されます。MAC アドレス 81:cd:93:13:ab:31 のテスト デバイスを「Iot-prod」に割り当て、その他のデバイスを「Iot-default」に割り当てる必要があるシナリオで、外部認証サーバーが存在しないことを考慮すると、テスト用に構成されている場合、適切なアクションは、ネットワークに接続しているすべてのデバイスに適用されるグローバル フォールバック ロールを設定することです。これにより、特定のデバイス プロファイルに一致しないデバ

イスは必ず「iot-default」ロールを継承します。「iot-prod」ロールに関連付ける特定の MAC アドレス (81:cd:93:xx:xx:xx) の構成がすでに設定されているため、フォールバック ロールをグローバルに設定すると、他のデバイスの要件に対応できます。

最新問題: **2**
大学キャンパスの無線管理者は、学生が屋外で作業しているときに接続の問題が発生するという報告をまとめています。



上記の設定を確認すると、ベスト プラクティスに合わせるために変更を監視する必要がありますか?

A. 802 11r を無効にします。

B. 802 11k を無効にします。
C. 5Gnz TX 電力範囲の最小/最大を増加します。
D. 5 GHz のワイヤレス カバレッジをアグレッシブに調整します。
Answer: C (メーッセージを残す)
学生が屋外で作業している場合の接続の問題に対処するには、5GHz 無線の送信 (TX) 出力範囲を拡大すると、信号強度とカバレッジが向上します。示されている設定は、電力設定に対する保守的なアプローチを示しているため、屋外エリアに十分なカバレッジを提供できない可能性があります。出力範囲を増やすことで、ワイヤレス信号の到達範囲を拡張でき、屋外のワイヤレス カバレッジのベスト プラクティスと一致します。

最新問題**: 3**
ACME 企業の従業員が、オフィス環境内を移動中に最近品質の悪い VoIP 通話について苦情を言いました。HPE Aruba Networking Central はこの通話について妥当な UCC スコアを報告しましたが、VoIP エンジニアはシステムの MOS が 2,3 であると報告しました。VoIP デバイスは 5GHz 周波数帯域で動作しています。
考えられる要因は何ですか? (2つ選択してください。)
A. カバレッジ AP 導入計画は通常、VoIP の十分なセル オーバーラップをサポートしていません。
B. 802.tr は WLAN セキュリティ設定で有効になっています。
C. 発信者の場所で局所的な干渉が発生しました
D. 802.1K は WLAN セキュリティ設定で無効になっています
E. クライアントは Zigbee を継続的に動作させるエリアにローミングしました。
Answer: A,E (メーッセージを残す)
AP 導入計画におけるセルの重複が不十分であると、VoIP の品質が悪影響を受ける可能性があります。これにより、ユーザーが移動するときに AP 間のハンドオフが低下する可能性があります。これにより、VoIP エクスペリエンスが低下します。さらに、継続的に Zigbee 動作が行われているエリアにローミングすると、5GHz 周波数帯域との干渉が発生し、VoIP 通話品質がさらに低下する可能性があります。VoIP エンジニアの報告によれば、Zigbee 通信プロトコルは Wi-Fi と同じ周波数帯域で動作するため、ノイズや干渉が発生し、MOS スコアの低下につながる可能性があります。

最新問題**: 4**
展示する。

```
Central-3-Edge# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 172.21.10.3

     Network                                                Nexthop          Metric     LocPrf     Weight   Path
-------------------------------------------------------------------------------------------------------------------
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]           172.21.11.2      0          100        0        ?
*>i [3]:[0]:[172.21.11.2]                                  172.21.11.2      0          100        0        ?

Route Distinguisher: 172.21.11.2:201      (L2VNI 201)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.201.1.1]           172.21.11.2      0          100        0        ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[10.201.1.102]         172.21.11.2      0          100        0        ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[]                     172.21.11.2      0          100        0        ?

Route Distinguisher: 172.21.10.1:10010      (L3VNI 10010)
*>i [5]:[0]:[0]:[0]:[0.0.0.0]                              172.21.11.1      0          100        0        ?
*>i [5]:[0]:[0]:[24]:[172.21.111.0]                        172.21.11.1      0          100        0        ?

Route Distinguisher: 172.21.10.2:10010      (L3VNI 10010)
*>i [5]:[0]:[0]:[24]:[10.200.1.0]                          172.21.11.2      0          100        0        ?
*>i [5]:[0]:[0]:[24]:[10.201.1.0]                          172.21.11.2      0          100        0        ?

Route Distinguisher: 172.21.10.3:10010      (L3VNI 10010)
*>  [5]:[0]:[0]:[24]:[10.203.1.0]                          172.21.11.3      0          100        0        ?
*>  [5]:[0]:[0]:[32]:[172.21.11.5]                         172.21.11.3      0          100        0        ?

Route Distinguisher: 172.21.11.2:200      (L3VNI 10010)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]           172.21.11.2      0          100        0        ?

Route Distinguisher: 172.21.11.2:201      (L3VNI 10010)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.201.1.1]           172.21.11.2      0          100        0        ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[10.201.1.102]         172.21.11.2      0          100        0        ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[]                     172.21.11.2      0          100        0        ?

Route Distinguisher: 172.21.11.3:203      (L3VNI 10010)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.203.1.1]           172.21.11.3      0          100        0        ?
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[10.203.1.100]         172.21.11.3      0          100        0        ?
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[]                     172.21.11.3      0          100        0        ?
Total number of entries 24
```

```
Central-3-Edge# show ip route all-vrfs

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2

VRF: default

Prefix              Nexthop          Interface      VRF(egress)   Origin/    Distance/     Age
                                                                  Type       Metric
-------------------------------------------------------------------------------------------------
0.0.0.0/0           172.21.1.5       vlan501        -               O/E2       [110/25]      06h:47m:36s
172.21.1.0/30       172.21.1.5       vlan501        -               O          [110/200]     06h:47m:36s
172.21.1.4/30       -                vlan501        -               C          [0/0]         -
172.21.1.6/32       -                vlan501        -               L          [0/0]         -
172.21.10.1/32      172.21.1.5       vlan501        -               O          [110/100]     06h:47m:36s
172.21.10.2/32      172.21.1.5       vlan501        -               O          [110/200]     06h:47m:36s
172.21.10.3/32      -                loopback0      -               L          [0/0]         -
172.21.11.1/32      172.21.1.5       vlan501        -               O          [110/100]     06h:47m:36s
172.21.11.2/32      172.21.1.5       vlan501        -               O          [110/200]     06h:47m:36s
172.21.11.3/32      -                loopback1      -               L          [0/0]         -

VRF: overlay_lab

Prefix              Nexthop          Interface      VRF(egress)   Origin/    Distance/     Age
                                                                  Type       Metric

VRF: default

Prefix              Nexthop          Interface      VRF(egress)   Origin/    Distance/     Age
                                                                  Type       Metric
-------------------------------------------------------------------------------------------------
0.0.0.0/0           172.21.1.5       vlan501        -               O/E2       [110/25]      06h:47m:36s
172.21.1.0/30       172.21.1.5       vlan501        -               O          [110/200]     06h:47m:36s
172.21.1.4/30       -                vlan501        -               C          [0/0]         -
172.21.1.6/32       -                vlan501        -               L          [0/0]         -
10.201.1.1/32       172.21.11.2      -              -               O          [110/100]     06h:47m:36s
10.201.1.102/32     172.21.11.2      -              -               B/EV       [200/0]       05h:14m:09s
10.203.1.0/24       -                vlan203        -               C          [0/0]         -
10.203.1.1/32       -                vlan203        -               L          [0/0]         -
172.21.11.4/32      172.21.11.2      -              -               B/EV       [200/0]       06h:47m:30s
172.21.11.5/32      -                loopback3      -               L          [0/0]         -
172.21.111.0/24     172.21.11.1      -              -               B/EV       [200/0]       06h:47m:30s

Total Route Count : 21
```

CX 6300 からの次の CLI 出力を考慮すると、正しいのはどれですか?

A. RD 172.16.10.1 を備えた CX スイッチにはアクティブなファブリック クライアントがありません
B. IP アドレス 10.203 1.100 の有線クライアントは、ループバック IP アドレス 172.21.11.2 のファブリック内のリモート CX 6300 上にあります。
C. IP アドレス 10 203 1 100 の有線クライアントには、適切にアドバタイズされていないホストルートがあります。
D. オーバーレイ ループバック アドレスは、2 ビット サブネット マスクを使用してフェアリーでアドバタイズされます。
Answer: B (メーッセージを残す**)**
提供される CLI 出力には、CX 6300 スイッチからのルーティング情報が表示されます。「VRF: デフォルト」の下の出力には、ネクスト ホップ 172.21.11.2 の 10.203.1.100/32 のルートを含む、さまざまな IP ルートが表示されます。これは、IP アドレス 10.203.1.100 を持つクライアントへのルートがネットワーク内で既知であり、ループバック IP アドレス 172.21.11.2 を持つファブリック内の別のデバイス経由で到達可能であることを示します。ルートがルーティング テーブルに存在するということは、クライアントが既知であり、ファブリック ネットワーク内でアクティブであることを意味します。

最新問題**: 5**
お客様は、IT ヘルプデスクが、他のデバイスが使用できない固有の PSK を使用して単一の SSID に接続するように LOT デバイスを設定できるようにしたいと考えています。どの解決策をお勧めしますか?
A. MAC 認証を使用した MPSK AES
B. MPSK ローカル
C. クラウド認証を使用した MPSK AES
D. ClearPass を使用した MPSK AES
Answer: (解答を表示する**)**
ClearPass を使用したマルチ事前共有キー (MPSK) は、IT ヘルプデスクが固有の PSK を使用して単一の SSID に接続するように IoT デバイスを構成する必要があるシナリオに推奨されるソリューションです。MPSK を使用すると、同じ SSID 上で異なる PSK を使用でき、ClearPass を使用すると、これらの一意のキーを効率的に管理できます。

最新問題**: 6**
顧客は、単一サイトに 3 つのコントローラで構成される AOS 10 モビリティ ゲートウェイ クラスタを導入しました。WLAN は、ワイヤレス デバイス トラフィックを AOS 10 モビリティ クラスタにトンネリングするように設定されています。クライアントは、WPA3-Enterprise (opmode wpa3-aes-ccm) を使用して ClearPass によって認証されます。-128)。セキュリティ チームは、ClearPass を使用してワイヤレス デバイスに再認証を強制する機能を要求しました。

ゲートウェイ フェールオーバー シナリオ中も含めて、ClearPass が AOS 10 モビリティ クラスタに対する認証の変更を一貫して開始できるようにするには、どの手順が必要ですか? (2つ選択してください)

A. 高可用性 - クラスター構成でクラスター モードを自動サイトに設定します。

B. WLAN - SSID - VLAN - モード設定を変更します

C. 高可用性 - クラスター構成で手動クラスター構成を有効にします。

D. 高可用性 - クラスター構成で動的認証 CoA を有効にします。

E. [セキュリティ] - [詳細] - [RADIUS クライアント] で NAS IPv4 アドレスを変更します。

Answer: D,E (メーッセージを残す**)**

ClearPass が一貫して認可変更 (CoA) を開始できるようにするには、動的認可を有効にして RADIUS CoA メッセージを処理できるようにすることが重要です。通常、この設定は高可用性クラスター構成に該当し、ゲートウェイのフェールオーバー後も確実に維持されます。さらに、RADIUS 通信に正しい IP アドレスが使用されるように、RADIUS クライアント設定で NAS IP アドレスを構成する必要があります。これは CoA が正しく機能するために必要です。

最新問題**: 7**

SSID に対して 1024 kbpsdown と 2048 Kops up の正しい Banawidth Control が表示されるオプションはどれですか?

A.

B.

C.

D.

Answer: D (メーッセージを残す)

SSID のダウン 1024 Kbps とアップ 2048 Kbps の正しい帯域幅制御設定がオプション D に示されています。オプション D では、ダウンストリームは 1024 Kbps、アップストリームは 2048 Kbps に設定され、両方ともユーザーごとに設定され、要求された設定と一致します。。この設定により、SSID に接続したときに各ユーザーに指定されたレートの帯域幅割り当てが保証され、制御された予測可能なユーザー エクスペリエンスが提供されます。

最新問題: **8**

顧客はネットワーク セグメント内の IP アドレスを使い果たしています。同じ VLAN に追加の IP サブネットを追加するとどうなりますか?

A. 2 つのサブネットが勝ったブロードキャストは、同じ VLAN 内のすべてのポートに到着します

B. IGMP は同じ VLAN 内の両方のサブネットでは機能しません

C. これにより、2 つのサブインターフェイスを使用する 1 つの SVI が生成されます。

D. ユーザーは、同じ VLAN 内の L3 ポイントを通過せずに相互に連絡し、PTP トラフィックを確立できます。

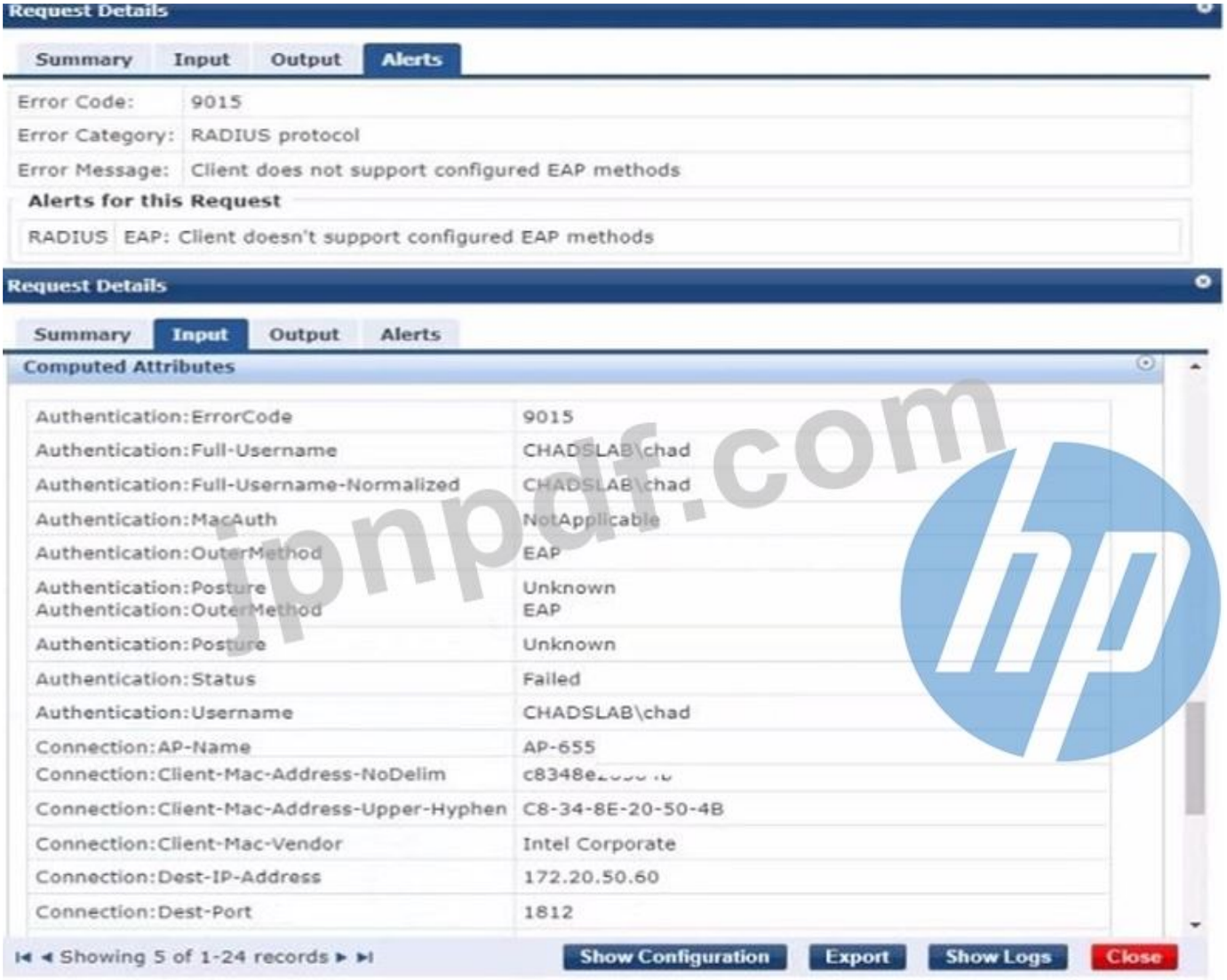
Answer: D (メーッセージを残す)

同じ VLAN に追加の IP サブネットを追加すると、いずれかのサブネットで構成されたデバイスがルーティングを必要とせずにレイヤー 2 で通信できるようになります。これは、それらが同じ VLAN 上にあるため、同じブロードキャスト ドメイン内にあるためです。ただし、サブネット間で通信するには、L3 デバイスまたは VLAN 間ルーティングが必要になります。

最新問題: **9**

Windows デバイスが 802.1X ネットワークに接続しようとしましたが、正しい役割を受け取りません。TEAP は ClearPass の唯一の認証方法として設定されています。ワイヤレス設定は正しいです。

展示する。



私はおそらく何が原因でしょうか？

A. Windows デバイスには 10 個の TEAP が構成されている必要があります。

B. ClearPass には 2 番目の認証方法が必要です。

C. 802.1X は Windows デバイスの TEAP と互換性がありません

D. Windows デバイスではマシン認証のみを構成する必要があります

Answer: A (メーッセージを残す**)**

この問題は、Windows デバイスが ClearPass 構成で指定されている TEAP (Tunneled Extensible Authentication Protocol) を使用するように構成されていないことが原因である可能性があります。TEAP は、安全な認証のための内部 EAP メソッドをカプセル化する EAP メソッドです。ClearPass を使用してネットワーク上で正常に認証するには、Windows デバイスのネットワーク設定で TEAP が有効になっており、正しく構成されている必要があります。

最新問題: **10**

フルセットアップ方法を使用して 3 つの新しい AOS 10 ゲートウェイを同じセントラル グループにオンボードした後、顧客はパスワードが間違っているため、HPE Aruba Networking Central リモート コンソールを使用してゲートウェイの 1 つにログインできません。

A. フルセットアップを使用して作成された管理者パスワードが、グローバル Central 管理者パスワードと一致しません。
B. セットアップの実行プロセス中に作成された管理者パスワードは、リモート コンソール アクセスを許可するように構成されていません
C. 完全セットアップ プロセス中に作成された管理者パスワードが、Central グループの管理者パスワードと一致しません。
D. Central グループ レベルで作成された管理者パスワードの有効期限が切れています
Answer: C (メーッセージを残す)
集中管理システムにデバイスをオンボードする場合、オンボード プロセス中に各デバイスに個別の管理者パスワードを設定できます。このパスワードが中央管理プラットフォームのグループ レベルで期待されるものと一致しない場合、前述のようなログインの問題が発生する可能性があります。

最新問題: **11**
顧客は CX 6300 スイッチのデバイス プロファイルを評価しています。テスト デバイスには次の属性があります。
* MAC アドレス = 81:cd:93:13:ab:31
* LLDP sys-desc = iotcontroller
テスト デバイスは「iot-dev」ロールに割り当てられていますが、顧客は「iot-prod」ロールを適用することを要求しています。

```
mac-group iot
     seq 10 match mac-oui 81:cd:93
port-access lldp-group iot-lldp
     seq 10 match sys-desc iot
port-access cdp-group iot-cdp
     seq 10 match platform accesspoint

port-access device-profile iot-dev
    associate role iot-dev
    associate lldp-group iot-lldp
port-access device-profile iot-prod
    associate role iot-prod
    associate mac-group iot
port-access device-profile iot-test
    associate role iot-test
    associate cdp-group iot-cdp
```

構成を考えると、「iot-dev」ロールがデバイスに適用される原因は何ですか?
A. テスト デバイスは CDP をサポートしていません。
B. デバイス プロファイルの優先順位が設定されていません。
C. 外部 RADIUS サーバーに到達できません。
D. LLDP システムの説明は、lldp グループ構成と一致します。
Answer: D (メーッセージを残す)
デバイス プロファイル設定では、デバイスの役割は、MAC アドレス、LLDP システムの説明、CDP 情報などの属性を定義された条件と照合することによって決定されることがよくあります。テスト デバイスには、LLDP システムの説明が「iot-dev」ロールに関連付けられている「iot-lldp」グループ構成と一致するため、「iot-dev」ロールが割り当てられています。

最新問題: **12**

ネットワーク管理者は HPE Aruba Networking Central にアクセスし、訪問者が外部サービスにアクセスするときにインターネット帯域幅を消費しすぎて従業員のトラフィックが枯渇していることに気付きました。そのため、管理者は、無線帯域幅を音声担当のすべてのユーザー間で両方向で 60 Mops に制限し、10 Mops 以下に制限したいと考えています。YouTube トラフィックを両方向にモップします。ディープ パケット インスペクション、Web コンテンツ分類、およびファイアウォールの可視化が有効になります。
このタスクを実行するにはどの構成が必要ですか? (2つ選択してください。)

A.

B.

C.

D.

Answer: (解答を表示する)

ネットワーク管理者が設定した帯域幅制限を達成するには、アプリケーションごとの制限と合計制限の両方を構成する必要があります。オプション B は、アプリケーションごとの帯域幅制限を設定するための構成を示しています。これにより、YouTube トラフィックを両方向で 10 Mbps に制限できます。オプション D は、音声ロール内のすべてのユーザーの合計帯域幅制限を 50000 Kbps (または 50 Mbps) に設定し、合計ワイヤレス帯域幅を制限する要件を満たす構成を示しています。これらの構成を HPE Aruba Networking Central に適用することで、管理者は必要な制御を適切に実装して、訪問者のトラフィックが従業員のトラフィックのネットワーク パフォーマンスを妨げないようにするとともに、Aruba ソリューションの機能に合わせてネットワーク リソースを効果的に管理および優先順位付けすることができます。

最新問題: **13**
最近、ClearPass を認証サーバーとして HPE Aruba Networking Central グループに追加しました。
ローカル ユーザー ロール (LUR) を使用した RADIUS 認証は正常に機能しますが、同じアクセス ポイントではダウンロード可能なユーザー ロール (DUR) を使用できません。
DUR の問題を解決するには、この構成の何を修正する必要がありますか?
A. ClearPass に 「WEBAUTH」タイプの新しい施行ポリシーを追加し、それを ClearPass 上のマッチング サービスに関連付けます。
B. ClearPass の [デバイス] タブにネットワーク アクセス デバイス (NAD) の正しい IP アドレスまたは IP サブネットを追加します。
C. 「crypto pki-import pem serverCert」コマンドを使用して、AP の期限切れのデジタル証明書を置き換えます。
D. HPEAruba Networking Central の認証サーバー設定に 「CPPM ユーザー名」と 「CPPM パスワード」の正しい値を追加します。
Answer: B (メーッセージを残す**)**
ダウンロード可能なユーザー ロール (DUR) が ClearPass で正しく機能するには、ネットワーク アクセス デバイス (NAD) が ClearPass の [デバイス] タブで正しく定義されている必要があります。これにより、ClearPass が NAD を識別して通信し、適切なユーザー ロールを提供できるようになります。NAD が正しく定義されていない場合、ClearPass は適用のためにアクセス ポイントに DUR を提供できません。これは、高度な役割ベースのアクセス制御のために ClearPass をネットワーク デバイスと統合するために必要な一般的な構成手順です。

最新問題: **14**
有線ネットワークに接続している顧客の従業員は、ユーザー エクスペリエンスが劣悪であると不満を抱いています。顧客は社内に UXI センサーを導入しています。これらのセンサーは数か月間稼働し続けています。
彼らは、有線ネットワーク (各センサーの有線インターフェイスを使用) と無線ネットワークの両方をテストしています。
顧客は、UXI ダッシュボードを使用して、ユーザー エクスペリエンスが悪い理由を調べて詳細を調べました。顧客は、UXI ダッシュボードを使用してセンサーからダウンロードされたパケット キャプチャを確認するように依頼しました。
UXI センサーからダウンロードした zip ファイルから 「datagrams」.pcap ファイルをチェックしましたが、問題は見つかりませんでした。これはどのように説明できますか?
A. 「datagrams-pcap ファイルには、成功したテストのみが含まれています。失敗したテストは、「データグラム失敗」.pcap ファイル
B. UXI センサーは最新のテスト結果をクラウドにアップロードできなかったため、パケット キャプチャが古くなっています
C. 物理イーサネット インターフェイスでキャプチャされたデータグラムは、別の .pcap ファイル内にあります。

D. パケット キャプチャのデフォルトのファイラーでは、センサーによる追跡テストのキャプチャが許可されていません

Answer: A (メーッセージを残す)

トラブルシューティングを容易にするために、成功したテスト結果と失敗したテスト結果を異なるファイルに分割するのが一般的です。「datagrams.pcap」ファイルに問題がない場合、そのファイルには成功したテスト データのみが含まれており、ユーザー エクスペリエンスの低下を説明する失敗したテストは別のファイルにある可能性があります。

「データグラム失敗.pcap」

最新問題: **15**

各グループ ベース ポリシー (GBP) の役割の説明をそれぞれの役割 ID と照合します。

Answer:

Explanation:

デフォルト GBP ロール =GBP ロール ID = 0インフラストラクチャ GBP ロール =GBP ロール ID = 2ユーザー定義 GBP ロール =GBP ロール ID = <100-8191>

最新問題: **16**

顧客のインフラストラクチャは、ベスト プラクティスに基づいて SSID プロファイルでプライマリ ゲートウェイ クラスタとセカンダリ ゲートウェイ クラスタの両方を使用するように設定されています。120 個の AP をプライマリ ゲートウェイ クラスタとセカンダリ ゲートウェイ クラスタに均等に分割しているのはなぜですか?

A. プライマリ ゲートウェイ クラスターは、6 つのノードを持つ異種クラスターです。

B. プライマリ ゲートウェイ クラスタとセカンダリ ゲートウェイ クラスタが起動しています。クラスターのプリエンプションが有効になっている

C. セカンダリ ゲートウェイ クラスターは、6 つのノードを持つ同種クラスターです。

D. プライマリ ゲートウェイ クラスタとセカンダリ ゲートウェイ クラスタが起動しています。ただし、クラスターのプリエンプションは有効になっていません

Answer: D (メーッセージを残す)

クラスターのプリエンプションが有効になっていない場合、アクセス ポイント (AP) は、セカンダリにフェイルオーバーした後にプライマリ ゲートウェイ クラスターが再び起動しても、自動的に

プライマリ ゲートウェイ クラスターにフェイルバックしません。これにより、両方のクラスターが動作している場合、プライマリ クラスターとセカンダリ クラスター間で AP が均等に分割されます。プリエンプションがないと、AP がプライマリ クラスターに自動的に再バランスされず、現在の分散が行われます。

最新問題: **17**
展示する。

音声クライアントが初めて接続を試行したが、RADIUS サーバーが利用できない場合、どのユーザー ロールが割り当てられますか?

A. CRITICAL_AUTH
B. DEFAULT_AUTH
C. CRIT1CAL_V0ICE
D. PRE_AUTH

Answer: C (メーッセージを残す**)**

インターフェイス 1/1/7 に提供されている設定には、認証に関するさまざまなシナリオに対して指定されたロールがあります。音声クライアントが接続を試行し、RADIUS サーバーに到達できない場合、割り当てられる役割は「critical-voice-role」として指定された役割です。この場合、「CRITICAL_VOICE」ロールは、そのような状況で割り当てられるように構成されており、RADIUS サーバーが音声クライアントを認証できない場合でも、音声クライアントが適切なネットワーク アクセス許可を確実に受け取ります。

最新問題: **18**

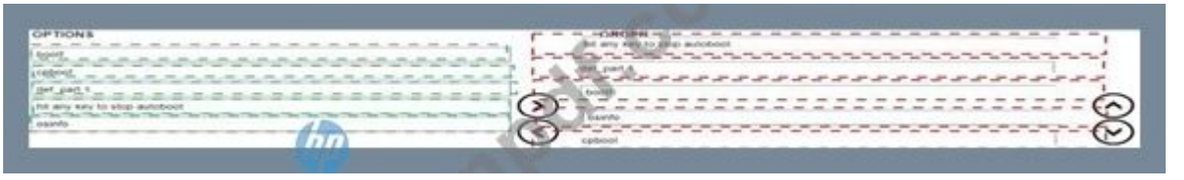
展示する。

ゲートウェイを最新のファームウェアに更新しましたが、ファームウェアを更新した後、ゲートウェイは HPE Aruba Networking Central に接続できなくなりました。企業の ITIL 手順では、バックアウト計画を実行する必要があります。コンソール ケーブルをゲートウェイに接続すると、次のプロンプトが表示されます。

Cpxload#

以前のファームウェア バージョンに戻すには、次のコマンドをどの順序で実行する必要がありますか?

Answer:

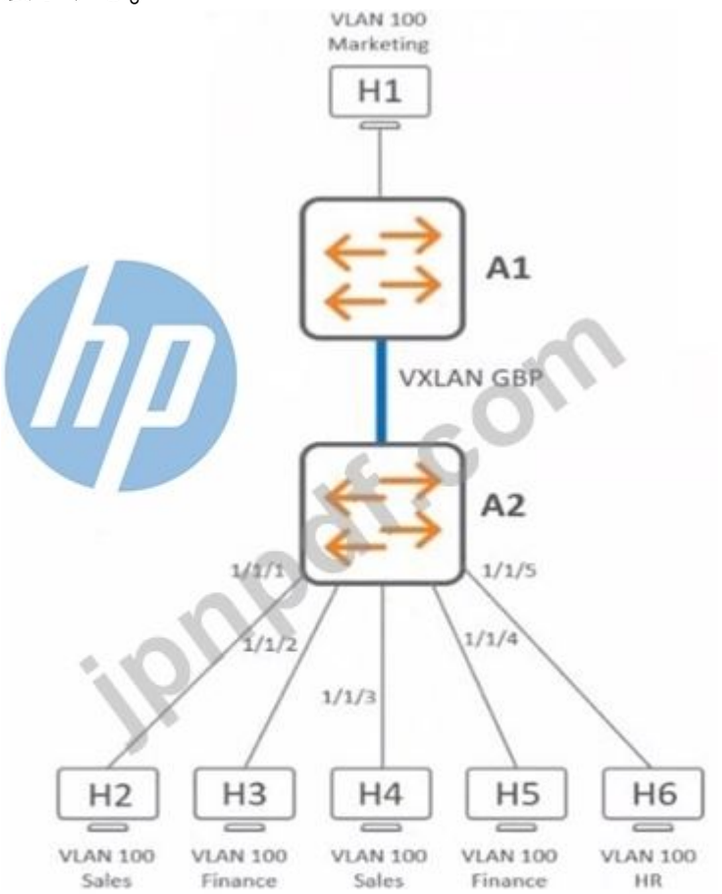


Explanation:

アップデートが失敗した後に以前のファームウェア バージョンに戻る手順は、通常次のとおりです。

任意のキーを押して自動ブートを停止します (これにより、システムが現在の問題のあるファームウェアで自動的に起動することがなくなります。) def_part 1 (このコマンドは、デフォルトのブート パーティションを設定します。これは、以前の動作していたファームウェアが配置されている可能性があります。) bootf(このコマンドは、指定されたフラッシュ パーティションから起動します。2 番目のステップの後は、以前のファームウェアになります。) osinfo(システムの起動後、このコマンドを使用して、ゲートウェイで現在実行されているファームウェアのバージョンを確認できます。)

最新問題: **19**
展示する。



Source	Destination	Action
Marketing	HR	Deny
Marketing	Sales	Permit
Marketing	Finance	Deny

H1 から送信された ARP トラフィックに対して期待される動作は何ですか?

A. A2 は ARP トラフィックをドロップします。

B. A2 はポート 1/1/1 ～ 1/1/4 から ARP トラフィックを送信します。

C. A2 は、ARP トラフィックをすべてのインターフェイスからフラッディングします。

D. A2 はポート 1/1/1 および 1/1/3 から ARP トラフィックを送信します。

Answer: C (メーッセージを残す**)**

VXLAN 環境では、スイッチ A2 によって学習された特定の宛先 MAC アドレスを持たない H1 からの ARP リクエストなどの未知のユニキャスト トラフィックが、すべてのインターフェイスからフラッディングされます。このフラッディング動作が必要なのは、A2 が ARP 要求が目的の宛先 (いずれかのインターフェイス上にある可能性がある) に確実に到達する必要があるためです。これは、宛先ハードウェア アドレスが不明な場合に ARP トラフィックを処理するスイッチの標準動作の一部です。

最新問題: **20**

キャンパス トポロジでは、コア トポロジが折りたたまれた VSX を使用します。顧客は冗長 SFP + トランシーバを追加し、モビリティ ゲートウェイを単一リンクから集約リンクに再構成しまし

た。モビリティ ゲートウェイ クラスタの 1 つのリンク アグリゲーション設定の CLI 出力を確認するように求められます。以下メンバー。

```
interface lag 100 multi-chassis
    no shutdown
    description ArubaGW_01
    no routing
    vlan trunk native 100
    vlan trunk allowed all
    lacp mode active
    lacp rate fast
```

有効な構成とは何ですか?

A.
```
interface port-channel 0
    description Connected_to_Core
    switchport mode trunk
    switchport trunk native vlan 100
    trusted
    trusted vlan 1-4094
!
interface gigabitethernet 0/0/2
    description Core01
    switchport mode trunk
    switchport trunk native vlan 100
    trusted
    trusted vlan 1-4094
    lacp group 0 mode active
    lacp timeout short
!
interface gigabitethernet 0/0/3
    description Core02
    lacp group 0 mode active
    lacp timeout short
```

B.
```
interface port-channel 0
    description Connected_to_Core
    switchport mode trunk
    trusted
    trusted vlan 100
!
interface gigabitethernet 0/0/2
    description Core01
    lacp group 0 mode active
    lacp timeout short
!
interface gigabitethernet 0/0/3
    description Core02
    lacp group 0 mode active
    lacp timeout short
```

C.
```
interface port-channel 0
    description Connected_to_Core
    switchport mode trunk
    trusted
    trusted vlan 1-4094
!
interface gigabitethernet 0/0/2
    description Core01
    lacp group 0 mode active
    lacp timeout short
!
interface gigabitethernet 0/0/3
    description Core02
    lacp group 0 mode active
    lacp timeout short
```

D. 
```
    description Connected_to_Core
    switchport mode trunk
    trusted vlan 1-4094
!
interface gigabitethernet 0/0/2
    description Core01
    switchport mode trunk
    switchport trunk native vlan 100
    trusted
    trusted vlan 1-4094
    lacp group 0 mode active
!
interface gigabitethernet 0/0/3
    description Core02
    switchport mode trunk
    switchport trunk native vlan 100
    trusted
    trusted vlan 1-4094
```

Answer: A (メーッセージを残す**)**

オプション A に示されている構成は、マルチシャーシ リンク アグリゲーション (MC-LAG) セットアップの有効な構成です。これは、高速な LACP PDU 交換による LACP (リンク アグリゲーション コントロール プロトコル) の使用を指定します。これは、復元力と高スループットのリンク アグリゲーションの作成に適しています。「vlan train allowed all」コマンドは、トランク全体のすべての VLAN を許可し、「vlan トランク ネイティブ 100」は、VLAN 100 をタグなしトラフィックのネイティブ VLAN として設定します。

最新問題**: 21**

展示する。

ある大学は市内で独自のテレビ局を運営しています。IT 部門は、帯域幅の消費を改善するために、マルチキャスト ベースの通信を使用して、IP ネットワーク経由でテレビ制作物をキャンパス全体に送信できるようにマルチメディア サーバーを導入しています。PIM スパース モードと IGMP スヌーピング機能が有効になっています。

ワイヤレス ユーザーがマルチキャスト グループに参加すると、同じ WLAN に接続しているすべてのユーザーのネットワーク パフォーマンスが低下します。ただし、有線ユーザーはこのような影響を受けません。トラブルシューティング中に、ネットワーク管理者は展示に示されているパケット キャプチャを保存し、マルチキャスト グループに参加していないユーザーも含めて、すべてのユーザーが低速で同じマルチキャスト フローを受信していると結論付けました。

問題を解決するには、ネットワーク管理者はどの機能を有効にする必要がありますか?

A. 動的マルチキャスト最適化とマルチキャスト送信最適化

B. UCC QoS 補正とマルチキャスト送信の最適化

C. ARP ブロードキャストからユニキャストおよびマルチキャスト送信への変換の最適化

D. 動的マルチキャスト最適化と UCC QoS 補正

Answer: A (メーッセージを残す)

動的マルチキャスト最適化 (DMO) とマルチキャスト送信最適化は、ワイヤレス環境におけるマルチキャスト トラフィックの問題の解決に役立つ機能です。DMO は、マルチキャスト ストリームを必要なクライアントへのユニキャスト ストリームに変換することにより、マルチキャスト トラ

フィックが無線で送信される方法を最適化します。これにより、マルチキャスト グループに加入していないクライアントの不必要なトラフィックが削減され、ネットワーク全体のパフォーマンスが向上します。マルチキャスト送信の最適化は、マルチキャスト フレームが最適な速度で送信されるようにマルチキャスト フレームの送信速度を調整し、すべてのユーザーがマルチキャスト フローを低速で受信する問題に対処します。

最新問題: **22**
ある大学は、L3 で分離された東棟と西棟に分かれたいくつかの建物からなるキャンパスを所有しています。東棟には 1600 の AP があります。西棟には 1200 の Aps があります。各ウィングには、HPE Aruba Networking Central によって管理される単一のゲートウェイ クラスターがあります。各クラスタには 1 つの 7210 モビリティ ゲートウェイが含まれます。ゲートウェイは DHCP リレーを使用して設定され、すべてのクライアント VLAN をルーティングします。新しいビジネスクリティカルな教員のリアルタイム アプリケーションでは、ユーザーは切断や遅延の増加なしにウィング内ではなくウィング内をローミングする必要があります。
ベスト プラクティスに合わせてパフォーマンスを低下させることなく要件を満たすために、ネットワーク管理者はどのような変更を行う必要がありますか? (2つ選択してください。)
A. 西ウィングの 7210 モビリティ ゲートウェイを 7030 モビリティ ゲートウェイのペアに置き換えます。
B. 単一の 7210 モビリティ ゲートウェイを各クラスターに追加します。
C. ゲートウェイから DHCP リレーを削除し、代わりに DHCP サーバーを有効にします。
D. 東ウイングの 7210 モビリティ ゲートウェイをペアまたは 9012 モビリティ ゲートウェイに置き換えます。
E. すべての SSID に対して L2 を実行し、ゲートウェイのアップリンクでユーザーの VLAN を許可します。
Answer: (解答を表示する**)**
ウィング間ローミングなしでウィング内でのシームレスなローミングを必要とする、ビジネス クリティカルな教員のリアルタイム アプリケーションをサポートするには、高可用性と十分な容量を確保することが不可欠です。各クラスタに 7210 モビリティ ゲートウェイを追加すると、必要な冗長性と容量が提供されます。
すべての SSID に対して L2 を実行し、ゲートウェイ アップリンクでユーザー VLAN を許可すると、L3 セグメンテーションの問題が発生せずに必要なトラフィック フローが促進され、各ウィング内でのシームレスなローミングがサポートされます。