HP.HPE7-A06.v2026-05-01.q73

試験コード：	HPE7-A06
試験名称：	HPE Campus Access Switching Expert Written Exam
認証ベンダー：	HP
無料問題の数：	73
バージョン：	v2026-05-01
ページの閲覧量：	118
問題集の閲覧量：	1104

https://www.jpnshiken.com/shiken/HP.HPE7-A06.v2026-05-01.q73.html

質問: **1**
顧客がVoIP電話からのタグ付きトラフィックを中央の拠点にトンネリングしたいと考えています。どのUBTモードを設定すればよいですか？
A. トンネルタグ
B. マルチVLAN
C. ローカルVLAN
D. VLAN拡張
正解: **B** (コメントを発表する)
HPE Aruba Networkingでは、UBT（ユーザーベーストンネリング）が複数のモードをサポートしています。タグ付きトラフィック（IP電話からの音声VLANなど）を中央の拠点にトンネリングする必要がある場合は、マルチVLANモードを使用します。このモードでは、複数のVLAN（例データと音声）をVLANタグを維持しながらトンネリングできます。これは、中央トンネリングを必要とするVoIP電話の導入に適したモードです。

質問: **2**
ドラッグアンドドロップの質問
ダイナミック セグメンテーションを使用してユーザー デバイスがネットワークに接続したときに発生するイベントの正しいシーケンスは何ですか?

正解:

Explanation:
ダイナミックセグメンテーションでは、デバイスはまずClearPassで認証を行います。認証結果に基づいて、ClearPassはロールを割り当てます。その後、スイッチまたはAPは適切なVLANまたは

ポリシーを適用することでロールを適用し、最終的にデバイスにネットワークへのフルアクセスを許可します。

質問: **3**
VSX クラスタに 2 台の CX 8325 スイッチを構成した場合、プロトコルベースのポート冗長性をサポートするためのゼロタッチ プロビジョニングのために 7000 ゲートウェイのリンク アグリゲーションをどのように準備すればよいですか。

A.
```
int lag 1 multi-chassis
     lacp mode active
     lacp fallback
```

B.
```
int lag 1
     lacp mode active
     lacp fallback
```

C.
```
int lag 1 multi-chassis
     lacp mode on
     lacp fallback
```

D.
```
int lag 1
     lacp mode on
     lacp fallback
```

正解: **A** (コメントを発表する)
VSX ペアでプロトコルベースのポート冗長性を備えた 7000 ゲートウェイ ZTP の場合、LAG は LACP がアクティブなマルチシャーシである必要があります。LACP フォールバックにより、ピアが検出されるまで単一のメンバーが起動できるため、プロビジョニング中の接続が確保されます。

質問: **4**
ダイナミック セグメンテーションを使用するためのベスト プラクティスは何ですか?
A. LUR を使用してデバイスの場所に基づいてロールを割り当て、DUR を使用してユーザー ID に基づいてデバイスにロールを割り当てます。
B. UBT を使用して、特定の種類のデバイス用の分離されたネットワークを作成します。
C. ロールベースのアクセスとオーバーレイ技術を組み合わせて、階層化されたセキュリティアプローチを作成します。
D. Wi-Fi 経由でネットワークに接続されているデバイスでのみ、ダイナミック セグメンテーションを使用します。
正解: (正解を表示します)

質問: **5**
お客様からVLAN 151を分離VLANにするという要件がありました。同僚が設定の一部をコピー&ペーストしましたが、期待通りの結果になりませんでした。追加されたコードは次のとおりです。望ましい結果を得るには、このコードの前に構成に何を追加する必要がありますか?

A.
```
vlan 15
private-vlan primary
vsx-sync
```

B.
```
vlan 15
isolated-vlan primary
vsx-sync
```

C.
```
vlan 15
primary-vlan isolated 151
vsx-sync
```

D.
```
vlan 15
private-vlan isolated 151
vsx-sync
```

正解: **A** (コメントを発表する)

お客様はVLAN 151を独立したプライベートVLANとして設定することを希望しています。部分的な設定を追加しましたが、期待通りの結果は得られませんでした。プライベートVLAN構造を正しく設定するには、（未指定の）部分的な設定の前にどの設定スニペットを追加すべきかを判断する必要があります。

* プライベートVLAN構成の基礎:

* プライマリVLANを定義する必要があります。このVLANは、プロミスキャスポートと関連付けられたセカンダリVLAN内のポート間のトラフィックを伝送します。

* セカンダリ VLAN (分離またはコミュニティ) はプライマリ VLAN に関連付けられます。

* ポートはプライマリVLAN（プロミスキャスポート、通常はルータ/ファイアウォール接続）またはセカンダリVLAN（ホストポート）のいずれかにマッピングされます。同じ分離VLAN内の分離ポートは相互に通信できません。

* オプションの分析 (VLAN 15 がプライマリであると想定):

* A)

VLAN 15

プライベートVLANプライマリ

vsx同期

これにより、VLAN 15 がプライマリプライベートVLANとして正しく定義されます。vsx-sync コマンドにより、この設定がVSXペア（該当する場合）間で同期されます。これは、VLAN 151 を独立したセカンダリVLANとして定義し、VLAN 15 に関連付ける前に必要な前提条件です。

* B)isolated-vlan primary は構文が間違っています。コマンドは private-vlan primary です。

* C)primary-vlan isolation 151 は、プライマリ VLAN コンテキスト内でプライマリまたはセカンダリ VLAN タイプ/関連付けを定義するための構文が正しくありません。

* D) VLAN 15 コンテキスト内での private-vlan isolated 151 は構文エラーです。private-vlan isolated コマンドは、セカンダリ VLAN（この場合は VLAN 151）の設定に属します。

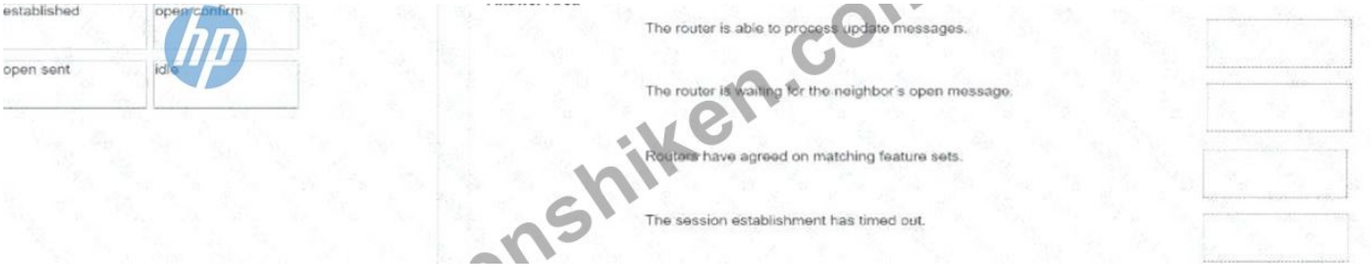
* 結論:VLAN 151 を private-vlan isolation として設定し、関連付ける前に、プライマリ VLAN を定義する必要があります。オプション A は、対象のプライマリ VLAN (VLAN 15) の設定でコマンド (private-vlan primary) を実行し、VLAN 15 をプライマリ VLAN として設定する方法を正しく示しています。

参考資料：AOS-CXセキュリティガイド（プライベートVLANの設定手順とコマンド）。これは、「スイッチング」（19%）と「セキュリティ」（10%）の目標。

質問: **6**
HPE ネットワークのマルチエリア設計に OSPF を構成する場合、エリア間でアドバタイズされるルートの数を減らすことでルーティングを最適化する機能はどれですか。
A. デフォルトルートの伝播
B. ルート集約
C. スタブエリアの設定
D. LSAフィルタリング
正解: **(**正解を表示します**)**

質問: **7**
ユーザーがEAP-TLSを使用した802.1X認証を使用して有線ネットワークに接続できません。ユーザーのデバイスは正しく設定されており、ユーザーは有効な証明書を所有しています。RADIUSサーバーのログには、ユーザーが認証に成功していることが示されています。
この問題の原因は何でしょうか?
A. スイッチ インターフェイスの構成に問題があります。
B. ユーザーのデバイスは正しい証明機関を使用していません。
C. スイッチは EAP-TLS を使用するように設定されていません。
D. RADIUS サーバーは EAP-TLS を使用するように構成されていません。
正解: **(**正解を表示します**)**
RADIUSログには有効な証明書による認証成功が示されているため、クライアントとRADIUSサーバー間のEAP-TLSは正常に機能しています。それでもユーザーが接続できない場合は、スイッチインターフェースの設定（VLAN割り当ての不足、ロールの誤り、ポートアクセス設定など）に問題がある可能性が高く、認証成功後にネットワークアクセスが妨げられています。

質問: **8**
BGP 接続スレートを、その状態を引き起こした可能性のある条件と一致させます。

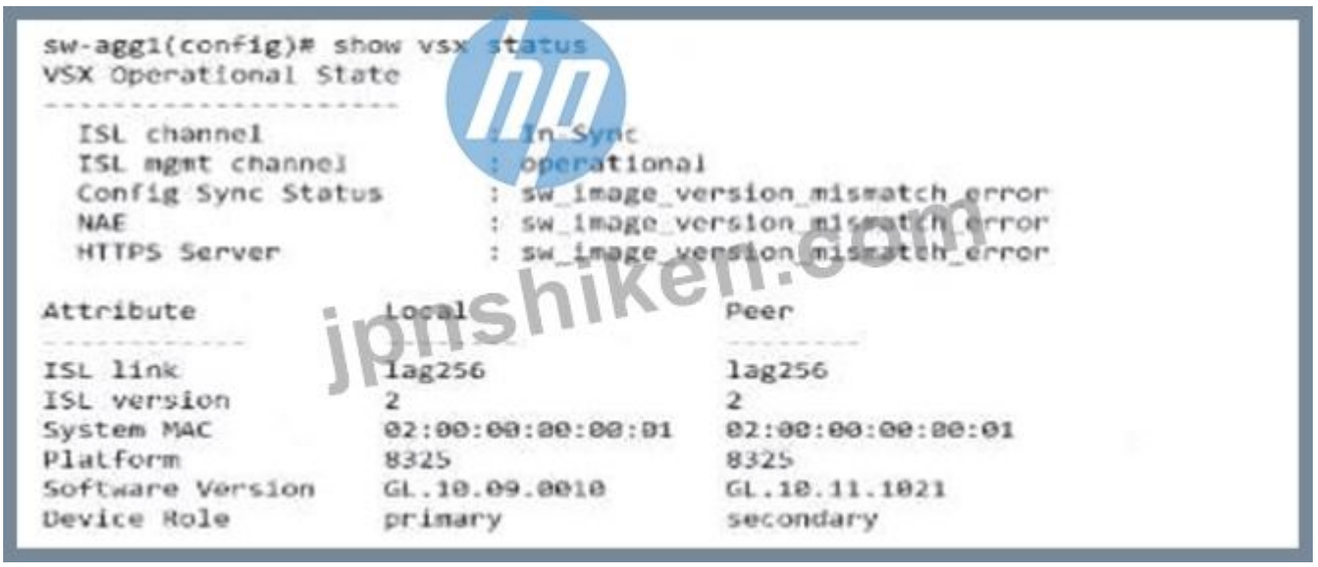


正解:

Explanation:

ルータは更新メッセージを処理できます。-->確立
ルータはネイバーのオープンメッセージを待っています。-->オープンが送信されました
ルータは一致する機能セットに同意しました。--> 開いて確認
セッションの確立がタイムアウトしました。-->アイドル
この質問では、BGP 有限状態マシン (FSM) からの BGP 接続状態を、その状態内で発生するか、その状態に至る条件の説明と一致させる必要があります。
* アイドル: BGPが開始イベントを待機するか、失敗後に再試行する初期状態です。また、接続試行中のタイムアウトなど、エラー検出時やセッション終了時にもアイドル状態になります。
* 一致: 「セッションの確立がタイムアウトしました。」- 接続プロセス中にタイムアウトが発生すると、BGP プロセスはアイドル状態に戻り、後で再試行できるようになります。
* OpenSent: TCP 接続が確立された後、ローカル ルータはパラメータ (AS 番号、機能など) を含む BGP OPEN メッセージを送信し、BGP ネイバーからの OPEN メッセージの受信を待機しながら OpenSent 状態に移行します。
* 一致: 「ルータはネイバーのオープン メッセージを待機しています。」
* OpenConfirm :ルータはネイバーからOPENメッセージを受信し、パラメータ（ASの一致、互換性のある機能など）を検証すると、KEEPALIVEメッセージを送信し、OpenConfirm状態に移行します。ネイバーからのKEEPALIVEメッセージを待機し、セッションを確認します。このフェーズで、基本的なパラメータチェックと機能ネゴシエーションが正常に完了します。
* 一致: 「ルータは一致する機能セットに同意しました。」- この合意は、交換された OPEN メッセージの検証が成功したときに発生します。
* 確立 :これはBGPピアリングが成功した最終的な安定状態です。両方のルータはOPENメッセージを介して互いのパラメータを受け入れ、KEEPALIVEでセッションを確認しました。この状態では、ルータはルーティング情報を含むUPDATEメッセージを交換できます。
* 一致: 「ルータは更新メッセージを処理できます。」
参考資料 :RFC 4271 「BGP4仕様 - セクション8、有限状態機械」、AOS-CXのBGP設定およびトラブルシューティングガイド。これは 「ルーティング」（16%）および 「トラブルシューティング」（10%）の目標に関連します。

質問**: 9**
展示品を参照してください。



スクリーンショットに基づいて、セカンダリスイッチの MCLAO インターフェースをオンラインにするには何が必要ですか?

A. セカンダリで vsx-software-upgradeado を使用します。

B. セカンダリ上の MAE エージェントを更新します。

C. プライマリと同じ CX OS バージョンを使用します。

D. プライマリと同じ ServiceOS バージョンを使用します。

正解**: (**正解を表示します**)**

この図は、sw-agg1 における show vsx status の出力を示しています。主な情報は次のとおりです。

* 構成同期ステータス: sw_image_version_mismatch_error
* NAE: sw_image_version_mismatch_error
* HTTPS サーバー: sw_image_version_mismatch_error
* プライマリソフトウェアバージョン: GL.10.09.0010
* セカンダリソフトウェアバージョン: GL.10.11.1021

これらのエラーは、プライマリVSXスイッチとセカンダリVSXスイッチで異なるAOS-CXソフトウェアバージョンが実行されていることを明確に示しています。設定の同期やMC-LAGインターフェースなどの機能の有効化など、VSXが正常に動作するには、ペア内の両方のスイッチで完全に同じソフトウェアバージョンが実行されている必要があります。

* オプションの分析:

* 回答: vsx-software-upgrade はアップグレードに使用されますが、現在の不一致要件は解決されません。

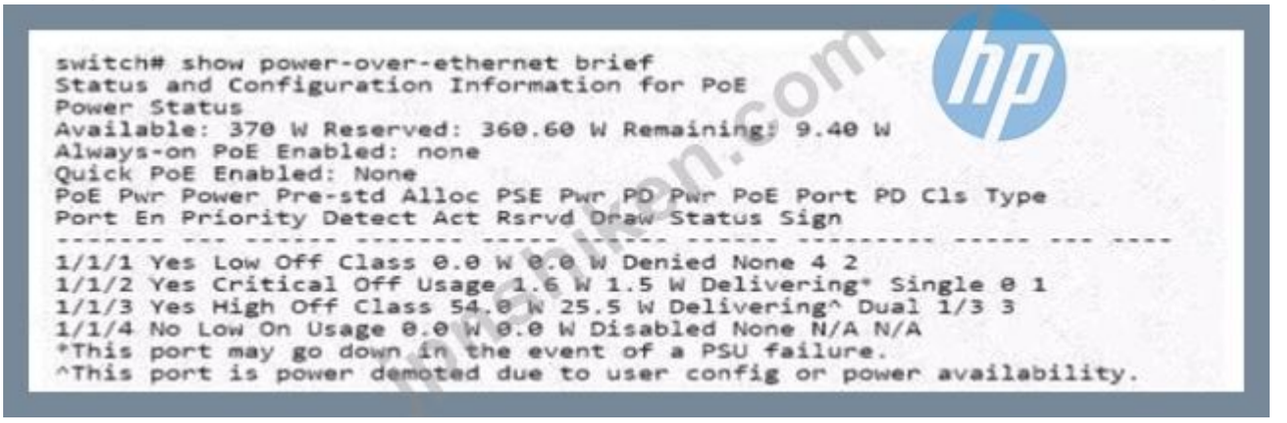
* B: NAE エラーは、基礎となるバージョンの不一致の症状です。

* C: プライマリ スイッチとセカンダリ スイッチの両方で同じ CX OS バージョンを使用することは、不一致エラーをクリアし、安定した VSX 動作状態を実現するための基本的な要件です。

* D: ServiceOS はシステムの一部ですが、主な要件とエラー メッセージはメインの AOS-CX ソフトウェア バージョンに関連しています。

参考資料：AOS-CX VSXガイド（VSXの要件、トラブルシューティング、ソフトウェアアップデートに関する章）。これは、「ネットワークの回復力と仮想化」（8%）および「トラブルシューティング」（10%）の目標に関連します。

質問: **10**
ネットワーク運用チームのシニアエンジニアから、一部のPoE給電デバイスがランダムに電力を失うという断続的な問題が発生していると報告がありました。調査の結果、Acc-1スイッチのポート1で、Acc-1のCLI出力に示されているような動作が発生していることがわかりました。



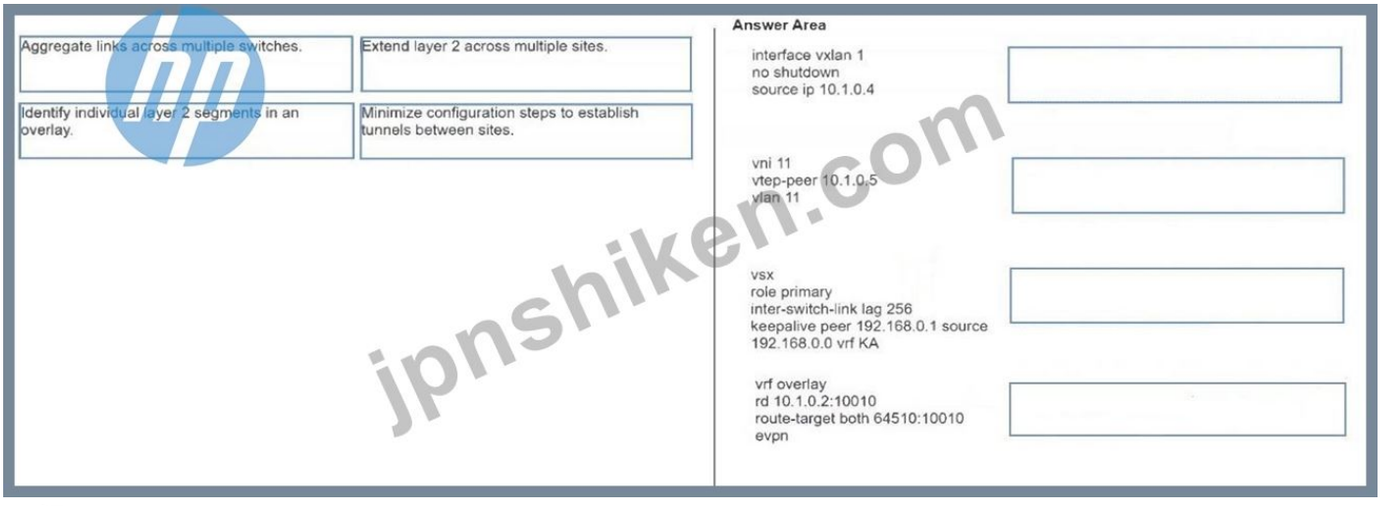
1/1/1 が PoE を否定する原因として考えられるものは何ですか?
A. このスイッチは PoE クラス 4 をサポートしていません。
B. スイッチの PoE 電力バジェットを超えました
C. PoEポートの優先度を低く設定
D. ポート 1/1/1 の PoE が手動で無効にされました。
正解: **(正解を表示します)**
質問は、AOS-CXスイッチ（Acc-1）のCLI出力（提供されていません）にはPoEの問題が示されています。考えられる原因を特定することが課題です。
* オプションの分析:
* オプション A: 不正解です。AOS-CX スイッチは通常、ほとんどのデバイスに十分な PoE クラス 4 (802.3at、30W) をサポートしています。
* オプションB:正解。スイッチのPoE電力バジェットを超えた場合、ポート1/1への電力供給が拒否される可能性があります。
/1 により、断続的なデバイス障害が発生します。
* オプション C: 不正解です。PoE ポートの優先度が低いとポートの優先度が下がる可能性がありますが、予算の問題を考えると、電力が完全に失われる可能性は低くなります。
* オプション D: 不正解です。PoE を手動で無効にすると、断続的な問題ではなく、継続的な電力損失が発生します。
* オプションBが正しい理由：AOS-CXスイッチのPoE電力供給量は限られています（モデルと電源によって370Wまたは740Wなど）。接続デバイスからの総電力需要がこの供給量を超えると、スイッチは一部のポートへの電力供給を拒否します。これは、デバイスの電源サイクルや電源ネゴシエーション時に断続的に発生します。ポート1/1/1の場合、接続デバイスの電力供給がランダム

に停止する可能性があります。CLI出力には「power denied」（show power-over-ethernet briefなど）と表示される可能性があります。HPE Aruba NetworkingのPoEトラブルシューティングガイドラインに沿って、PoE供給量（show power-over-ethernet）を確認し、電源をアップグレードするか、重要なポートを優先することで問題を解決できます。
* 認定目標との関連性:
* 接続性 (9%):PoE 展開の問題のトラブルシューティング。
* トラブルシューティング (10%): キャンパス ネットワークにおける電力関連の問題の診断。
* スイッチング (19%): レイヤー 2 デバイスの PoE 構成を実装します。
参考文献:
HPE Aruba Networking AOS-CX 構成ガイド: PoE 構成とトラブルシューティング。
HPE7-A06 学習ガイド: PoE 管理と診断について説明します。
HPE Aruba ネットワーク技術ドキュメント: PoE 予算のトラブルシューティング。

質問**: 11**
AOS-CX スイッチで 802.1X サプリカント機能を設定するときにサポートされる EAP 方式はどれですか?
(2つ選択してください。)
A. EAP-TLS
B. EAP-TTLS
C. EAP-MD5
D. EAP-PEAP
E. EAP-TEAP
正解**: A,D (**コメントを発表する**)**
質問は、AOS-CX スイッチ (つまり、別のデバイスに対して認証するクライアントとして機能するスイッチ) で 802.1X サプリカント機能を構成するときに、どの EAP (拡張認証プロトコル) 方式がサポートされるかを尋ねています。
* AOS-CX 802.1X サプリカント: スイッチ自体が 802.1X を使用して認証できるようにします。
* サポートされているEAP方式 :スイッチ実装では通常、サプリカントロール用の一般的なEAP方式のサブセットがサポートされています。セキュアな方式が推奨されます。AOS-CXのdot1x supplicant eap-methodコマンドに関するドキュメントには、通常、サポートされているタイプが記載されています。ドキュメントに記載されている一般的なセキュアな方式には、EAP-TLSとEAP-PEAP（通常はMSCHAPv2を使用）が含まれます。EAP-MD5は多くの場合サポートされていますが、セキュアではありません。
* オプションの分析（2つ選択）:
* A. EAP-TLS: 企業のサプリカントで一般的にサポートされている、安全な証明書ベースの方式。サポートされている可能性があります。
* B. EAP-TTLS: もう一つの安全なトンネル方式ですが、スイッチサプリカントではPEAPの方が一般的に使用される場合があります。サポートについては、AOS-CXの特定のドキュメントで確認が必要です。

* C. EAP-MD5: シンプルなチャレンジレスポンス方式ですが、安全性に欠けます。レガシーシステム上の理由からサポートされていることが多いです。
* D. EAP-PEAP: サーバー側の証明書と通常はユーザー名を使用した安全なトンネル方式 /password (MSCHAPv2) が内部にあります。一般的にサポートされています。
* E. EAP-TEAP: 新しいトンネリング方式。スイッチ サプリカントでは PEAP/TLS よりもサポートされる可能性が低くなります。
* 結論: 一般的な企業要件と、サプリカント機能について文書化された AOS-CX 機能に基づくと、選択肢の中でサポートされる可能性が最も高いのは、安全な方法である EAP-TLS(A) と EAP-PEAP (D) です。
参考資料 :AOS-CX セキュリティガイド 802.1X サプリカントの設定、サポートされる EAP 方式)。これは セキュリティ」(10%)と 認証/承認」(9%)に関連します。

質問: **12**
ドラッグアンドドロップの質問
顧客の要件を、その要件を満たすために使用されるネットワーク テクノロジを部分的に構成するために使用されるコマンドと一致させます。



正解:

質問: **13**

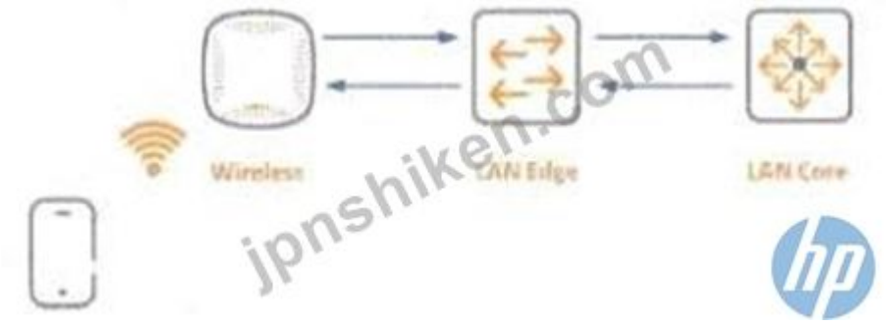
OSPF グレースフル リスタートの考慮事項を正確に説明している記述はどれですか (2 つ選択してください)。
A. GR ヘルパーに猶予期間タイマーを設定する必要があります。
B. 猶予期間を長く設定しすぎるとルーティングの更新が抑制される可能性があるため、注意が必要です。
C. GR リスタータ機能は、AOS-CX 6200、CX 6300、CX 6400、および CX 8400 モデルでのみサポートされます。
D. GR を開始するために、リスタータはリンクローカル マルチキャストを送信します。
E. GR ヘルパーとして機能する場合は、VSF スタックにセカンダリ メンバーがあることを確認する必要があります。
正解: **(**正解を表示します**)**
GR ヘルパーは、再起動ルータが回復する間に隣接関係のアドバタイズを継続する期間を認識できるように、猶予期間タイマーを使用して設定する必要があります。
猶予期間を長く設定しすぎると、ルーティング更新が不必要に抑制され、収束が遅れる可能性があります。

質問: **14**
トラブルシューティング中に、エンジニアがネットワーク内で過剰なARP要求を発見しました。この問題を軽減するには、どのような設定が有効でしょうか？
A. DHCPスヌーピングの有効化
B. ARPキャッシュサイズの増加
C. プロキシARPの設定
D. MACエージングタイマーの調整
正解: **A (**コメントを発表する**)**

質問: **15**
管理者は HPE Aruba Networking Central でサードパーティの WLAN 送信機を監視していますが、そのうちのいくつかは不正または不正の疑いがあると分類されています。
ルールのデフォルトの分類方法を使用する場合、不正の疑いのあるプログラムはどのように分類されるか
HPE Aruba Networking Central に 「オンプレミスの AP が疑わしい」と表示されていますか?
A. 信号レベル = "-65 dBM" かつ WLAN 分類 = "オンプレミス"
B. 信号レベル = "-65 dBM" かつ WLAN 分類 = "干渉中"
C. 信号レベル = "-50 dBM" かつ WLAN 分類 = "干渉オン"
D. 信号レベル = "-50 dBM" かつ WLAN 分類 = "On Wire"
正解: **A (**コメントを発表する**)**
HPE Aruba Networking Centralでは、信号強度が-65dBm 以上（近隣またはオンプレミス）のAPが検出され、WLAN分類がオンプレミスの場合、デフォルトの分類ルール 「オンプレミスの疑いのある

AP」がトリガーされます。これにより、管理者は組織敷地内にある不正なAPの疑いがあるかどうかを判断できます。

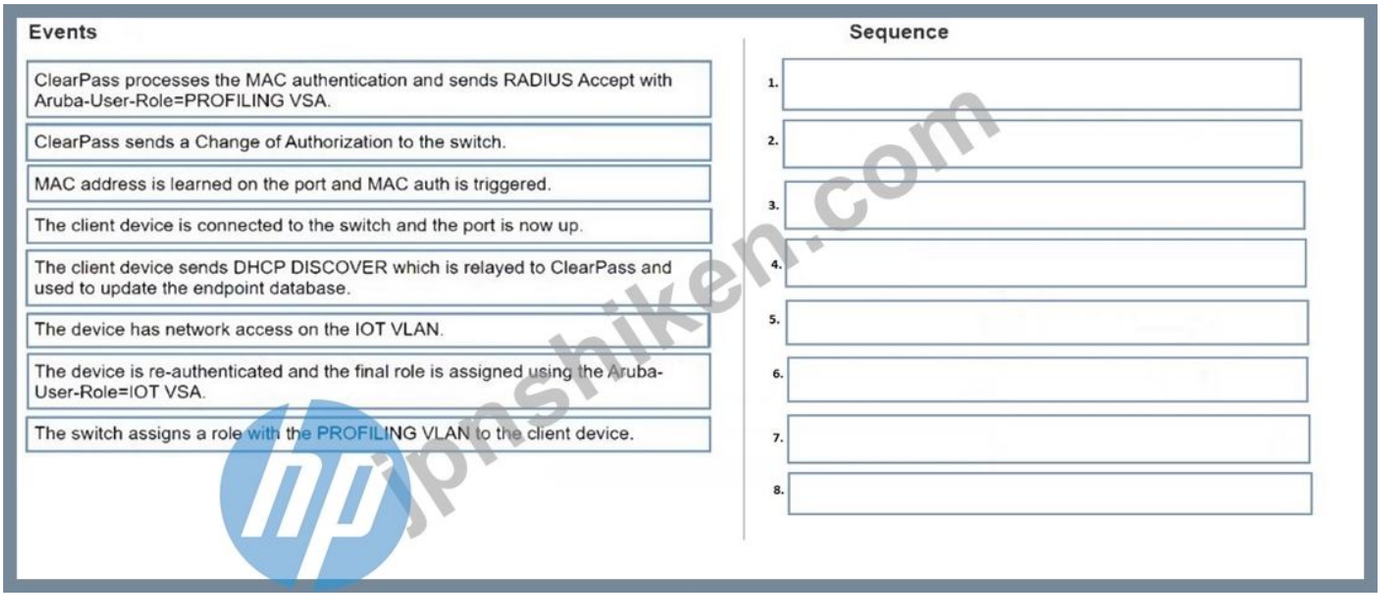
質問: **16**
展示する。



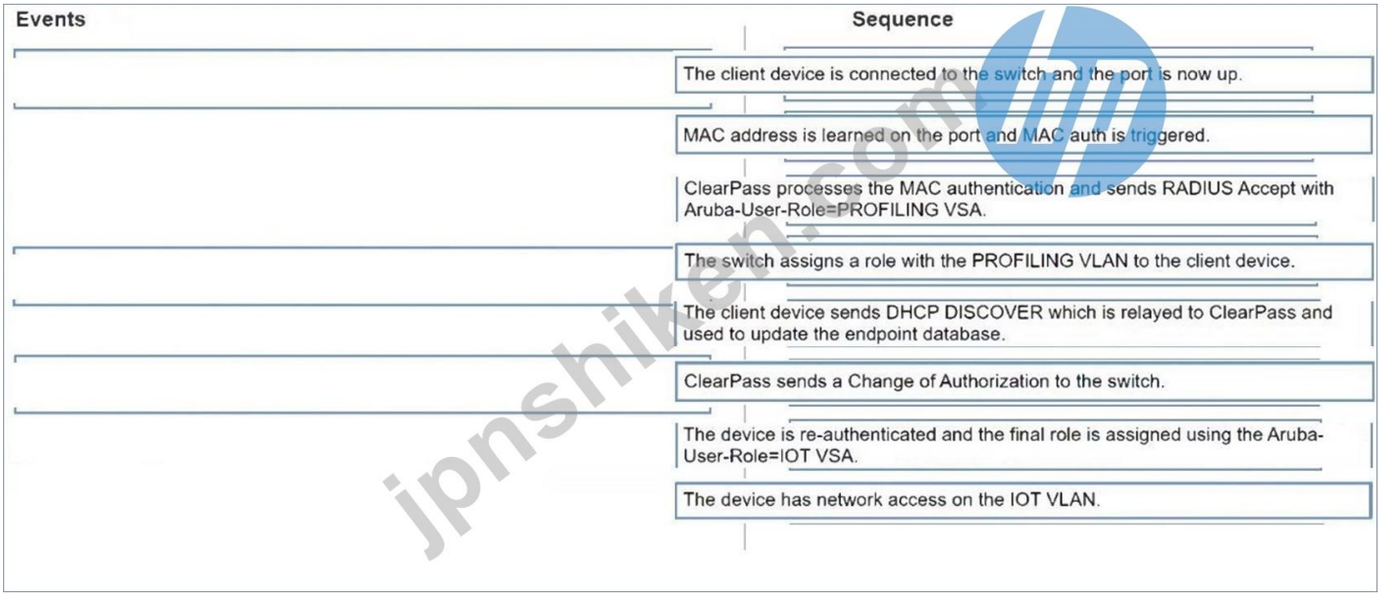
有線と無線の両方において、エンドツーエンドのQoS設計を実装する必要があります。正しいDSCPタグを維持するために、LAN側で何が必要ですか？
A. WLAN側でWMMとDSCPのマッピングを作成する
B. WLAN DSCP値が異なるため、カスタムDSCPマッピングを作成します
C. QoS内部ポートでDSCPマークされたパケットを信頼する
D. LANエッジにWMMからDSCPへのマッピングを作成する
正解: **(**正解を表示します**)**

質問: **17**
ドラッグアンドドロップの質問
以下の構成に基づいて、HPE Aruba Networking ClearPass を使用した IoT デバイスの有線 DHCP プロファイリングの正しいイベント シーケンスを特定します。

```
radius-server host 10.1.1. key plaintext Aruba123!
!
aaa group server radius clearpass
    server 10.1.1.1
```



正解:



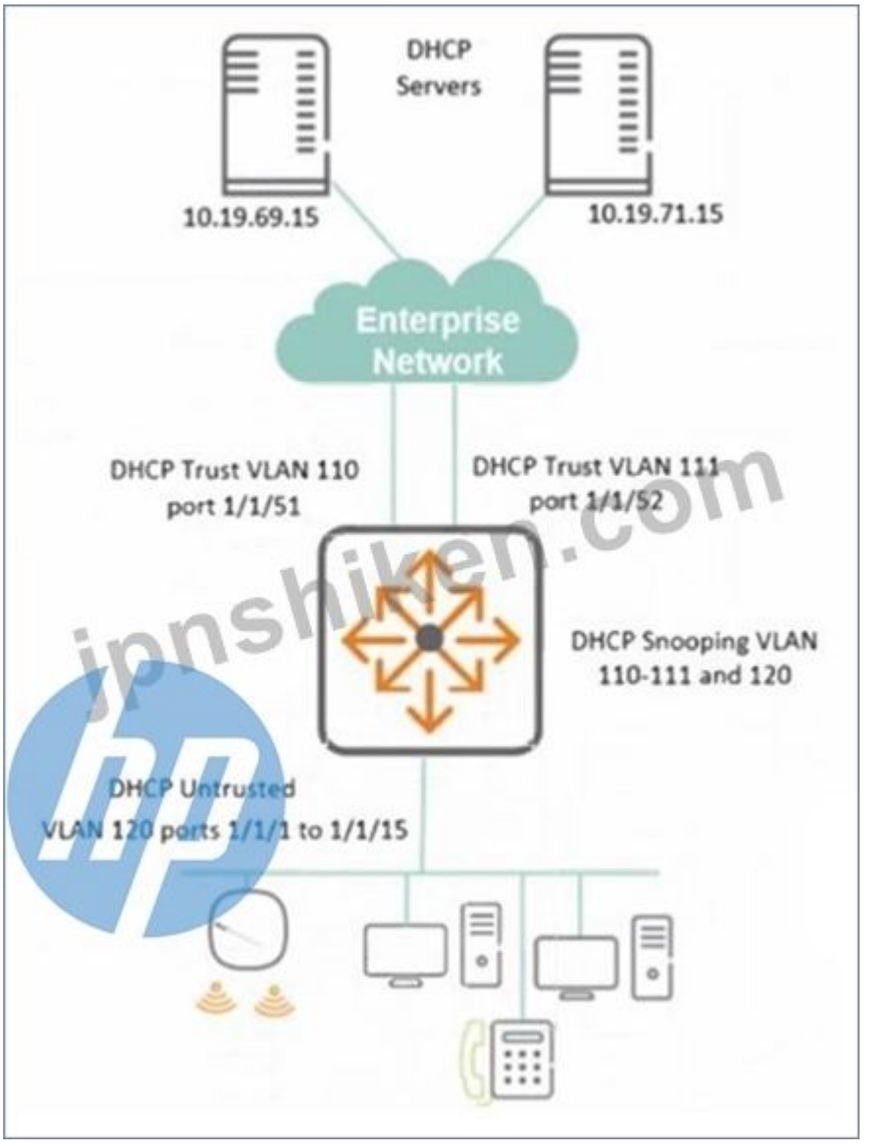
Explanation:

1. クライアント デバイスがスイッチに接続され、ポートが起動しています。
2. ポートで MAC アドレスが学習され、MAC 認証がトリガーされます。
3. ClearPass は MAC 認証を処理し、Aruba-User-Role=PROFILING VSA を使用して RADIUS Accept を送信します。
4. スイッチは、クライアント デバイスに PROFILING VLAN の役割を割り当てます。
5. クライアント デバイスは DHCP DISCOVER を送信し、これが ClearPass に中継されてエンドポイント データベースの更新に使用されます。
6. ClearPass はスイッチに認可変更を送信します。
7. デバイスは再認証され、Aruba-User-Role=IoT VSA を使用して最終的なロールが割り当てられます。
8. デバイスは IoT VLAN 上でネットワークにアクセスできます。

シーケンスは、デバイスの接続とMAC認証のトリガーから始まります。ClearPassがプロファイリングロールを提供し、スイッチがそれを割り当て、DHCPプロファイリングが実行されま

す。ClearPassはエンドポイントデータベースを更新し、認可変更 (CoA) をトリガーし、IoTロールでデバイスを再認証して、最終的なネットワークアクセスを許可します。

質問: **18**
展示品を参照してください。



```
dhcpv4-snooping
dhcpv4-snooping authorized-server 10.19.69.15
dhcpv4-snooping authorized-server 10.19.71.15
vlan 110
    description uplink
    dhcpv4-snooping
vlan 111
    description uplink
    dhcpv4-snooping
vlan 120
    description User
    dhcpv4-snooping
interface 1/1/1
    no shutdown
    description User
    vlan access 120

...
```

```
interface 1/1/15
    no shutdown
    description User
    vlan access 120
interface 1/1/51
    no shutdown
    vlan trunk native 1
    vlan trunk allowed 110
interface 1/1/52
    vlan trunk native 1
    vlan trunk allowed 111
interface vlan 110
    description uplink
    ip address 172.16.69.1/30
interface vlan 111
    description uplink
    ip address 172.16.71.1/30
interface vlan 120
    description User
    ip address 172.16.10.1/254
    ip helper-address 10.19.69.15
    ip helper-address 10.19.71.15
...
ip route 0.0.0.0/0  172.16.69.2 distance 10
ip route 0.0.0.0/0  172.16.71.2 distance 20
...
```

AOS-CX アクセス スイッチで DHCPv4 スヌーピングを有効にする場合、DHCP サーバーから IP を取得できるようにするには、どのような変更を行う必要がありますか?

A.
```
vlan 110-111,120
    dhcpv4-snooping trust interface 1/1/51-1/1/52
```

B.
```
interface 1/1/51-1/1/52
    dhcpv4-snooping trust
```

C. dhcpv4-snooping 信頼インターフェース 1/1/51-1/1/52

D.
```
interface vlan 110-111,120
    dhcpv4-snooping trust
```

正解: **B** (コメントを発表する)
VLAN 120のクライアントがIPアドレスを取得できるようにするには、スイッチが上流のDHCPサーバーに接続されたインターフェースを信頼する必要があります。正しい設定は次のとおりです。
インターフェース 1/1/51-1/1/52
DHCPv4スヌーピング信頼
これにより、これらのポート上のサーバーからの DHCP オファーと確認応答が DHCP スヌーピングによってドロップされなくなります。

質問: **19**
クライアントはネットワークに接続できません。HPE Aruba Networking ClearPass アクセス トラッカーで EAP タイムアウトが表示されます。このメッセージの考えられる原因は何ですか?
A. RADIUSサーバーはクライアント証明書を信頼しません
B. RADIUS サーバーは、クライアント証明書の有効期限が切れていることを確認します。
C. クライアントは、RADIUS サーバ証明書の有効期限が切れていることを確認できます。
D. クライアントは RADIUS サーバー証明書を信頼していません。
正解: **(**正解を表示します**)**
質問は、802.1 X 認証の試行中に HPE Aruba Networking ClearPass Access Tracker で EAP タイムアウトが発生し、考えられる原因を特定するというものです。
* オプションの分析:
* オプションA: 不正解です。クライアント証明書の信頼の問題は、EAPタイムアウトではなく、別のエラーを引き起こします。
* オプションB: 不正解です。期限切れのクライアント証明書はタイムアウトではなく認証失敗を引き起こします。
* オプションC: 不正解です。クライアントが期限切れのRADIUSサーバー証明書を発見した場合、証明書は拒否されますが、通常はタイムアウトではなく信頼エラーが発生します。
* オプションD: 正解。クライアントがRADIUSサーバーの証明書を信頼していない場合（CA証明書が見つからない、発行元が信頼できないなど）、EAPハンドシェイクを続行できず、EAPタイムアウトが発生する可能性があります。
* オプションDが正しい理由：EAP（EAP-TLSまたはEAP-PEAPなど）を使用した802.1X認証では、クライアントはRADIUSサーバーの証明書を信頼して安全なTLSトンネルを確立する必要があります。クライアントの信頼ストアに証明機関（CA）証明書がない場合、またはサーバーの証明書が信頼されていない場合（適切にインストールされていない自己署名証明書など）、クライアントはEAPハンドシェイクを中止し、ClearPassにEAPタイムアウトが記録されます。これは802.1X導入でよく発生する問題であり、HPE Aruba Networkingのセキュリティガイドラインに従い、クライアントが正しいCA証明書を持っていることを確認するか、信頼できるサーバー証明書を使用することで解決できます。
* 認定目標との関連性:
* 認証/承認 (9%):802.1X および ClearPass 認証の問題のトラブルシューティング。

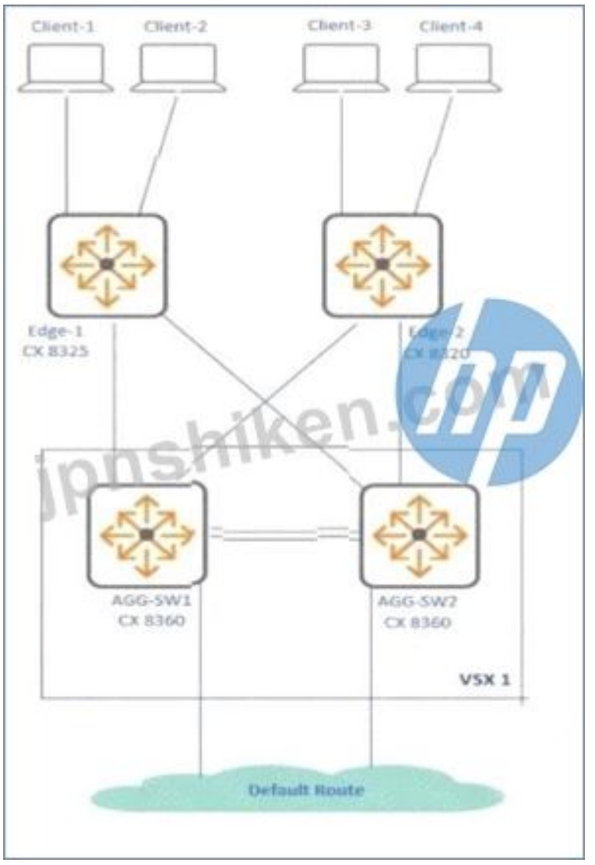
* セキュリティ (10%): EAP-TLS 障害による有線 802.1X の診断。
* トラブルシューティング (10%): キャンパス ネットワークでの認証タイムアウトの解決。
参考文献:
HPE Aruba Networking ClearPass Policy Manager ユーザー ガイド: 802.1X 認証のトラブルシューティング。
HPE7-A06 学習ガイド: EAP ベースの認証と証明書の問題について説明します。
HPE Aruba ネットワーク技術ドキュメント: 802.1X 証明書ベース認証のベストプラクティス。

質問: **20**
VSXクラスタのネットワーク問題をトラブルシューティングしています。昨日まではネットワークは正常に動作していましたが、今日はネットワークオペレーションセンターにアラートが届いています。2台のVSXメンバーのうち1台で「show interface brief」を実行したところ、すべてのVSX LAGが「機能によりダウン」していることが示されました。
この症状の原因は何でしょうか?
A. スプリットブレイン状態が検出されたため、LAG は無効になりました。
B. 両方の VSX メンバーがプライマリとして構成されています。
C. VSX はファームウェア バージョンの不一致を検出しました。
D. クラスターで VSX 同期が有効になっていません。
正解: **(正解を表示します)**
VSXでは、キープアライブリンクがダウンし、システムがスプリットブレイン状態の可能性（両方のピアがプライマリであると認識している状態）を検出すると、セカンダリスイッチはすべてのVSX LAGを停止し、「機能によるダウン」として報告することでループを防止します。これは、前述の状況と一致します。

質問: **21**
工場出荷時のデフォルト設定のゲートウェイを導入しようとしています。ZTPはさまざまな理由で使用できませんが、有効な代替手段を探しています。ZTPの有効な代替手段を2つ挙げてください。
（2つ選択してください。）
A. ポート 0/0/0 に接続して OTP を使用し、Web ブラウザを使用してプロビジョニングを完了します。
B. ポート 0/0/1 に接続して OTP を使用し、Web ブラウザを使用してプロビジョニングを完了します。
C. コンソールポートに接続してOTPを使用し、ターミナルソフトウェアを使用してプロビジョニングを完了します。「Full-Setup」を使用してください。
D. コンソールポートに接続してOTPを使用し、ターミナルソフトウェアのプロビジョニングを使用します。「Static-Activate」を使用する必要があります。
E. 静的 IP を使用してポート 0/0/1 に接続して OTP を使用し、Web ブラウザを使用してプロビジョニングを完了します。

正解: (正解を表示します)
正解 - Web ブラウザでポート 0/0/0 に接続し、ワンタッチ プロビジョニング (OTP) を使用してプロビジョニングを完了できます。
正解 - コンソール ポート経由で接続し、「ウルセットアップ」オプションを指定したターミナル ソフトウェアを使用して OTP プロビジョニングを完了できます。

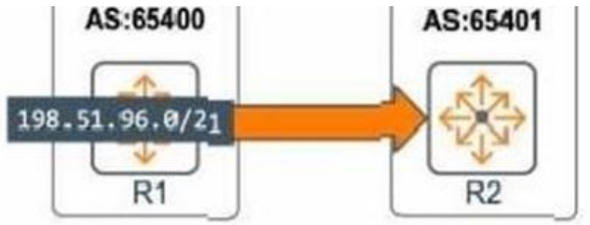
質問: **22**
展示する。



会議会場では、ネットワーク内で独立したネットワーク ユーザーを相互に保護する必要があります。
Edge-1 に次の構成が作成されます。
A. VLAN 152のプライベートVLANコミュニティを変更する
B. VLAN 151のプライベートVLANコミュニティを変更する
C. VLAN 152のタイプを変更します。primary-vlan 152
D. VLAN 151 primary-vlan 151 を変更します
正解: (正解を表示します)
要件は、Edge-1 を使用して会議会場で独立したネットワーク ユーザーを相互に保護することです。
このシナリオでは通常、プライベート VLAN が必要となり、具体的には「分離」タイプを使用して、同じセカンダリ VLAN 内のホスト間の通信を防止します。
* オプションの分析:

* プライベートVLANは、プライマリVLANと1つ以上のセカンダリVLAN（分離VLANまたはコミュニティVLAN）で構成されます。分離ポートは、同じVLAN内の他の分離ポートとは通信できず、プロミスキャスポート（通常はルーターのアップリンク）とのみ通信できます。コミュニティポートは、コミュニティポート同士およびプロミスキャスポートと通信できます。
* オプション A: VLAN 152 をプライベート VLAN コミュニティとして設定します。
* オプション B: VLAN 151 をプライベート VLAN コミュニティとして設定します。
* オプションC: VLAN 152をそれ自身に関連付けられたプライマリVLANとして定義します。これは標準の構文ではありません。
/論理。
* オプション D: VLAN 151 を、自身に関連付けられたプライマリ VLAN として定義します。
* 目標は分離です。いずれのオプションも、分離VLANを直接設定しません。オプションAとBはコミュニティVLANを設定しますが、これはそのVLAN内のユーザー間の通信を許可するため、要件に反します。オプションCとDは、プライマリVLANを誤った方法で定義しようとする可能性があります。
* 注意：提供されているオプションに問題があるようです。VLAN 151を分離するための標準的な設定では、プライマリVLAN（例：vlan 152 private-vlan primary）を定義してから、VLAN 151を分離VLANとして定義します（vlan 151 private-vlan isolated）。いずれのオプションも分離VLANを正しく設定しておらず、要件は分離であるため、質問またはオプションに欠陥がある可能性があります。ただし、意図を解釈する必要がある場合、質問はプライベートVLANの種類に関する理解を問う場合があります。VLANをコミュニティタイプに変更する（VLAN 151のオプションB）ことは、たとえそれが明示された分離の目標を満たしていなくても、別のアクションです。「分離」に関する正しいオプションがないと、「最適な」欠陥のあるオプションを選択することは困難です。質問がVLAN 151を何らかのタイプのプライベートセカンダリVLANとして設定することを意図していると仮定すると、オプションBはVLAN 151のプライベートVLANの特性を変更します。
* 結論：分離の要件に基づくと、提示された選択肢はどれも正しくありません。ただし、質問または選択肢に潜在的な誤りがあり、VLAN 151のプライベートVLANタイプに関連する最も近い変更を選択する必要がある場合、設定が「B」であるにもかかわらず、暫定的に選択肢Bが選択されます。必要な「孤立した」ではなく「コミュニティ」です。
参考資料：AOS-CX セキュリティガイド（プライベートVLAN設定）、プライベートVLANの概念（プライマリ、分離、コミュニティ）。これは「スイッチング」（19%）および「セキュリティ」（10%）の目標に関連します。

質問: **23**
展示物とコードサンプルを参照してください。




```
hostname R1
ip prefix-list 198-Network seq 10 permit 198.51.96.0/21
route-map BGP-COMMUNITY permit seq 10
 match ip address prefix-list 198-Network
 set community no-advertise
!
router bgp 65400
 neighbor 10.2.0.3 remote-as 65401
 neighbor 10.2.0.3 update-source loopback 0
 address-family ipv4 unicast
  neighbor 10.2.0.3 activate
  neighbor 10.2.0.3 route-map BGP-COMMUNITY out
  neighbor 10.2.0.3 send-community both
```

IPv4 アドレス ファミリに「neighbor 10.2.0.3 send-community both」というステートメントを追加すると、どのような効果がありますか? (2 つ選択してください。)

A. R1 が R2 と標準コミュニティおよび拡張コミュニティを送受信する機能をネゴシエートします。

B. この機能は、R1 と R2 が確立したセッションに影響を与えることなく有効になります。

C. R1 が、受信方向と送信方向の両方で NLRI レコードを持つコミュニティの交換を許可します。

D. R1 と R2 間の既存の BGP ピアリングがフラップする原因になります。

E. R1 は、R2 とタイプ 1 およびタイプ 2 のすべてのコミュニティをインポートおよびエクスポートする機能についてネゴシエートします。

正解: **(**正解を表示します**)**

send-community both コマンドは、標準 BGP コミュニティと拡張 BGP コミュニティの両方がネイバーに送信されることを保証し、この機能はセッションのセットアップ中にネゴシエートされます。

send-community both コマンドを使用すると、ルータは発信方向だけでなく、両方向の BGP NLRI アップデートにコミュニティ属性を付加できるようになります。

質問: **24**

セキュリティ メカニズムとして 802.1X を使用する SSID を設定しています。

Wi-Fi 6E (6GHz) を展開しながら Wi-Fi 6 (5GHz) ネットワークとの互換性を維持する場合、考慮すべきことは何ですか?

A. WPA3-Enterprise (CNSA) は必須です

B. WPA3-Enterprise (CCM-128) は必須です

C. WPA2-Enterprise は必須です

D. WPA3-Enterprise (GCM-256) は必須です
正解: (正解を表示します)
802.1Xを使用するWi-Fi 6E（6GHz）展開では、6GHz帯ではWPA2が許可されていないため、少なくともCCM-128暗号化を備えたWPA3-Enterpriseが必須です。これにより、Wi-Fi Allianceのセキュリティ要件への準拠を確保しながら、WPA2-Enterpriseが引き続きサポートされている既存のWi-Fi 6（5GHz）ネットワークとの互換性を維持できます。

質問: **25**
コマンドを初めて実行したときには、出力が不明になりますが、次回実行したときには次の情報が表示されます。

```
Cable Impedance
Status (Ohms) Description
-------------------------------------------------------------------
good 85-115 No cable faults found
open >115 Open circuit detected
intra-short <85 Short-circuit within the same wire pair
inter-short <85 Short-circuit with another wire pair
high-imp >115 Cable impedance was higher than expected
low-imp <85 Cable impedance was lower than expected
unknown --Cable test was inconclusive
```

問題をトラブルシューティングするためにスイッチで確認できる点は何ですか? (2 つ選択してください。)
A. 診断ケーブル 1/1/X
B. 診断インターフェース 1/1/X トランシーバーすべて
C. 1/1/Xトランシーバーすべて診断
D. 診断ケーブル - 診断 1/1/X
E. インターフェーストランシーバーすべて診断
正解: (正解を表示します)
diag cable 1/1/X → ポートに接続されたケーブルで診断テストを実行し、障害がないか確認します。
diag cable-diagnostic 1/1/X → インピーダンス、ショート、またはオープン回路を識別するために詳細なケーブル診断を実行します。

質問: **26**
ある病院では、各部屋のテレビ用に別々のVLANでネットワーク上のマルチキャスト設定を使用しています。不要なスイッチへの不要なマルチキャストを防ぐ機能はどれですか？
A. IGMPスヌーピング
B. IGMP 静的グループ
C. 不要なスイッチでIGMPが無効になっています
D. IGMPプロトコル
正解: (正解を表示します)

マルチキャストが不要なスイッチでIGMPを無効にすると、不要なマルチキャストトラフィックが処理または転送されるのを防ぐことができます。これにより、マルチキャストは実際に必要なVLANとスイッチでのみ有効になります。

質問: **27**
ネットワーク管理者は、特定のIPアドレス宛てまたは送信元のトラフィックのダンプを収集したいと考えています。AOS-CXスイッチでこれを実現するための最も簡単な診断コマンドは何ですか？
A. diag ユーティリティ tcpdump 送信元宛先-IP
B. 診断ユーティリティ tcpdump ホストIP
C. 診断ユーティリティ tcpdump ソースIP
診断ユーティリティ tcpdump 宛先IP
D. diag ユーティリティ tcpdump 宛先 IP
診断ユーティリティ tcpdump ソースIP
正解: **B (**コメントを発表する**)**
AOS-CXスイッチでは、特定のIPアドレスとの間のトラフィックをキャプチャする最も簡単な方法は、diag utilities tcpdump host <ip>を使用することです。hostキーワードは、指定されたIPアドレスの送信元と宛先の両方に一致するため、送信元と宛先のフィルターを個別に実行する必要がありません。

質問: **28**
HPE Aruba Networking ClearPass を使用した IoT デバイス用の MAC 認証ソリューションが稼働しており、DHCP フィンガープリントに基づいてデバイスの役割を動的に変更したいと考えています。
セキュリティチームが関連するClearPass設定を更新しました。これにより、デバイスが適切なプロファイリングルールに一致する場合、「IoT」ArubaユーザーロールVSAが返されます。ClearPassアプライアンスはファイアウォールの背後に配置されています。
以下の構成を展開しました。

```
radius dyn-authorization client 10.1.1.1 secret-key plaintext
Aruba123!
!
port-access role profiling
    vlan access name PROFILING
!
Port-access role IoT
    vlan access name IoT
!
interface 1/1/1
no shutdown
description DHCP-PROFILING-TEST
aaa authentication port-access preauth-role profiling
aaa authentication port-access mac-auth
    enable
```

ソリューションを機能させるには、どのようなアクションを実行する必要がありますか? (2 つ選択してください。)

A. RADIUSサーバーのTLSを有効にする

B. グローバルコンテキストで動的承認を有効にする

C. すべてのスイッチからClearPassへのファイアウォールUDPポート3799を設定します

D. ClearPassからすべてのスイッチへのUDPポート3799を許可するようにファイアウォールを設定します。

E. IoT VLAN SVIのClearPass IPアドレスを使用してIPヘルパーアドレスを設定します。

正解: **(**正解を表示します**)**

DHCPフィンガープリントに基づく動的なロール変更には、RADIUS CoA（認可変更が必要です。以下の手順を実施してください。

スイッチで動的認証をグローバルに有効にして、CoA 要求を受け入れるようにします。

■

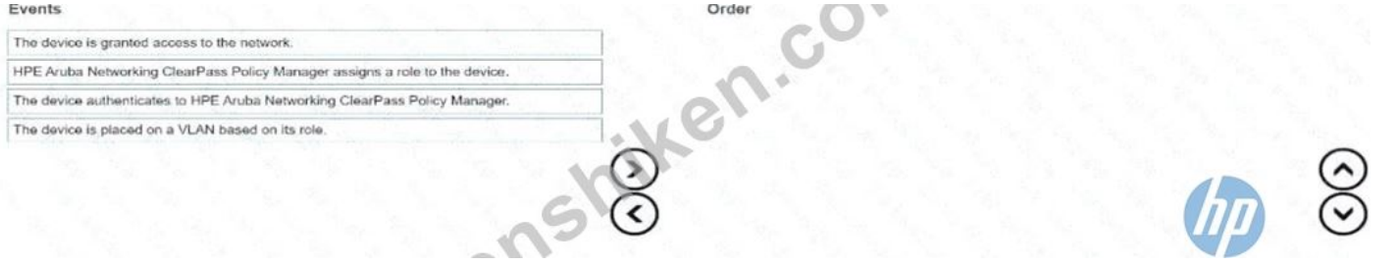
CoAが開始されるため、ClearPassからファイアウォール経由でスイッチへのUDP 3799を許可する

■

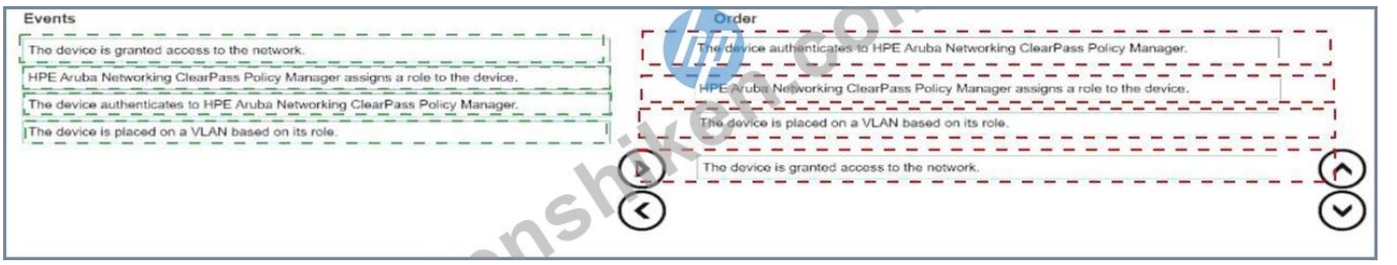
ClearPass によって NAD へ向かいます。

質問: **29**

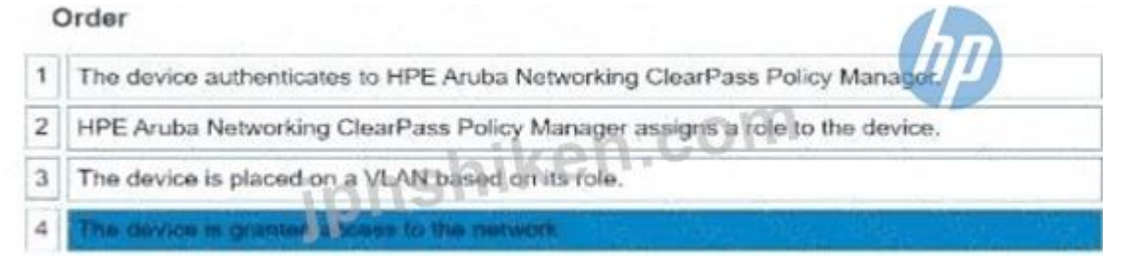
ダイナミック セグメンテーションを使用してユーザー デバイスがネットワークに接続したときに発生するイベントの正しいシーケンスは何ですか?



正解:



Explanation:



この質問では、ダイナミック セグメンテーションを利用してユーザー デバイスがネットワークに接続する際のイベントのシーケンスを尋ねます。ダイナミック セグメンテーションには通常、ClearPass による認証とロールベースのポリシー割り当てが含まれます。

* 認証 :デバイスが接続（有線または無線）されると、安全なアクセスを実現するための最初のステップは認証です。スイッチまたはAP（認証装置）は、通常RADIUS経由でClearPass Policy Manager（RADIUSサーバー）と通信することで、このプロセスを容易にします。デバイスは認証情報を提供するか、証明書（802.1X、MAC認証など）を使用します。

* ロールの割り当て:認証が成功すると、ClearPassはデバイスに基づいてポリシーを評価します。ユーザのコンテキスト（アイデンティティ、ポスチャ、時刻など）を取得し、RADIUS属性を認証装置に返します。重要な属性は、割り当てられたユーザロールです。このロールは、デバイスのアクセス権限とネットワーク設定をカプセル化します。

* ネットワーク配置/セグメンテーション：認証装置（スイッチ/AP）は、ClearPassから受信した割り当てられたロール情報を使用して、デバイスを適切なネットワークセグメントに配置します。これには、ポート/クライアントに特定のVLAN IDを割り当てるか、ユーザーベーストンネリング（UBT）シナリオでは、そのロールに関連付けられたArubaゲートウェイへのトンネルを確立することが含まれる場合があります。「ロールに基づいてVLANに配置する」というステップは、割り当てられたロールに基づくセグメンテーションの一般的な方法の1つです。

* アクセスの許可 :デバイスが認証され、ロールが割り当てられ、適切なネットワークセグメント（VLANまたはトンネル）に配置されると、割り当てられたロール内で定義されたファイアウォールルール、QoS設定、その他のポリシーに従ってアクセスが許可されます。トラフィックは、これらの適用されたポリシーに従って流れます。

参考資料 :Aruba Dynamic Segmentation ソリューションガイド、ClearPass Policy Manager ドキュメント、AOS-CX セキュリティガイド（ロール、ポートアクセス）。これは、「認証/認可」（9%）、「セキュリティ」（10%）、「スイッチング」（19%）、「WLAN」（9%）の目標に関連します。

質問: **30**

AOS-CX スイッチの BGP キープアライブ タイマーとホールドダウン タイマーをデフォルトに一致させます。

正解:

Explanation:

質問では、AOS-CX スイッチのデフォルトの BGP キープアライブ タイマーとホールドダウン タイマーをそれぞれの値に一致させる必要があります。

* オプションの分析:

* キープアライブタイマー :キープアライブタイマーは、セッションを維持するためにBGPキープアライブメッセージを送信する頻度を決定します。AOS-CXスイッチのデフォルト値は60秒です。

* ホールドダウンタイマー :ホールドダウンタイマーは、BGPセッションがキープアライブまたはアップデートメッセージを受信せずにアクティブ状態を維持できる最大時間を指定します。この時間を超えるとセッションはダウンしたとみなされます。AOS-CXスイッチのデフォルト値は180秒です。

* このマッピングが正しい理由 :BGP標準（RFC 4271）およびHPE Aruba Networking AOS-CXのドキュメントによると、デフォルトのBGPキープアライブタイマーは60秒、ホールドダウンタイマーは180秒（キープアライブ間隔の3倍）です。これらのタイマーにより、BGPセッションの安定性が確保され、ピア障害のタイムリーな検出が可能になります。AOS-CXの実装は、明示的に設定されない限り、これらのデフォルトに従います。

* 認定目標との関連性:

* ルーティング (16%): タイマー構成を含む BGP ルーティング トポロジの設計とトラブルシューティングが含まれます。

* トラブルシューティング (10%): タイマーに関連する BGP セッションの問題の診断が含まれます。

参考文献:

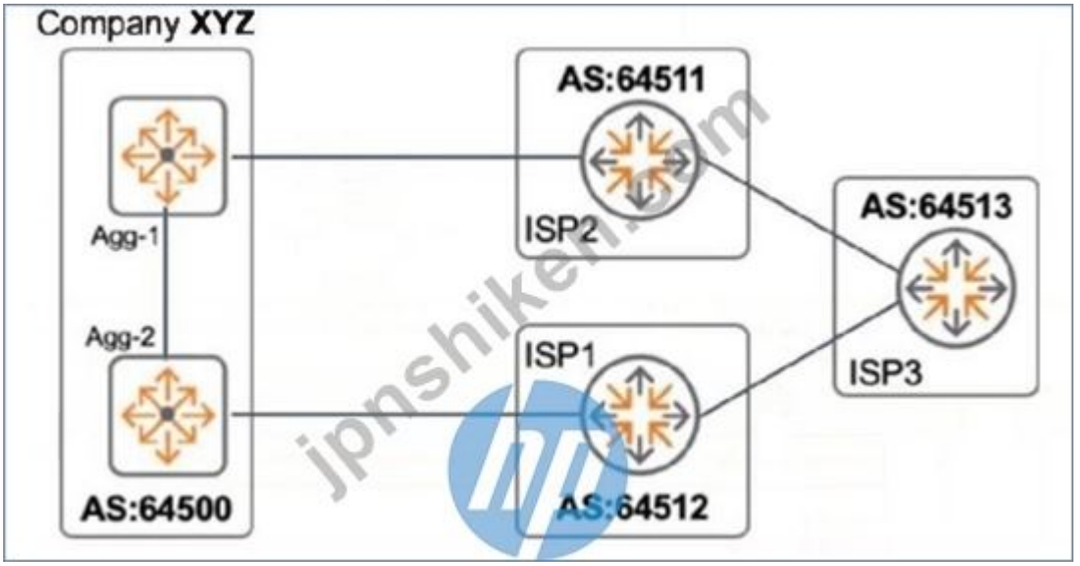
HPE Aruba Networking AOS-CX 構成ガイド: BGP 構成、デフォルトのタイマー値の詳細。

HPE7-A06 学習ガイド: BGP セッション管理とタイマーについて説明します。

RFC 4271: ボーダー ゲートウェイ プロトコル 4 (BGP-4)。デフォルトのキープアライブ タイマーとホールドダウン タイマーを指定します。

質問: **31**
ユーザーのデバイスは、EAP-TLS認証を使用した802.1X認証に失敗しています。クライアント側の証明書は有効です。この問題の原因として考えられるものは何ですか？ 2つ選択してください。）
A. ユーザーのデバイスは正しいゲートウェイを使用するように構成されていません。
B. スイッチ ポートに適用された ACL に問題があります。
C. EAP タイプが一致しません。
D. ユーザーのデバイスが間違った MAC アドレスを使用しています。
E. NAD は DNS サーバーと通信できません。
正解: **(**正解を表示します**)**
スイッチポート上の制限的なACLは、必要な認証またはEAPトラフィックをブロックし、802.1X 障害。
クライアントとネットワーク間の EAP タイプの不一致 (たとえば、スイッチまたは RADIUS が EAP-TLS 用に設定されていない場合) も、証明書が有効であっても認証が失敗します。

質問: **32**
展示品を参照してください。



XYZ社は、Agg-1とAgg-2でAOS-CXを使用しています。図に示すように、両方のルータは既にeBGP接続を確立していますが、XYZ社のエンジニアは、これらのルータが他のISPのトランジットASになる可能性があることを懸念しています。
XYZ のエンジニアは、Agg-1 と Agg-2 の両方で次の構成変更を提案しました。

```
router bgp 64500
 address-family ipv4 unicast
  neighbor <ip of ebgp-neighbor> route-map bgp-ebgp-out out
```

以下のどのスクリプトが、XYZ がトランジット AS になることを回避しながら、示されている構成を補完しますか?

A.

```
ip aspath-list bgp-local permit ^64500$
route-map bgp-ebgp-out permit
 match aspath bgp-local
 exit
```

B.

```
ip aspath-list bgp-local permit ^64500$
route-map bgp-ebgp-out deny
 match aspath bgp-local
 exit
router bgp 64500
 address-family ipv4 unicast
  neighbor <ip of ebgp-neighbor> route-map bgp-ebgp-out both
  exit
```

C.

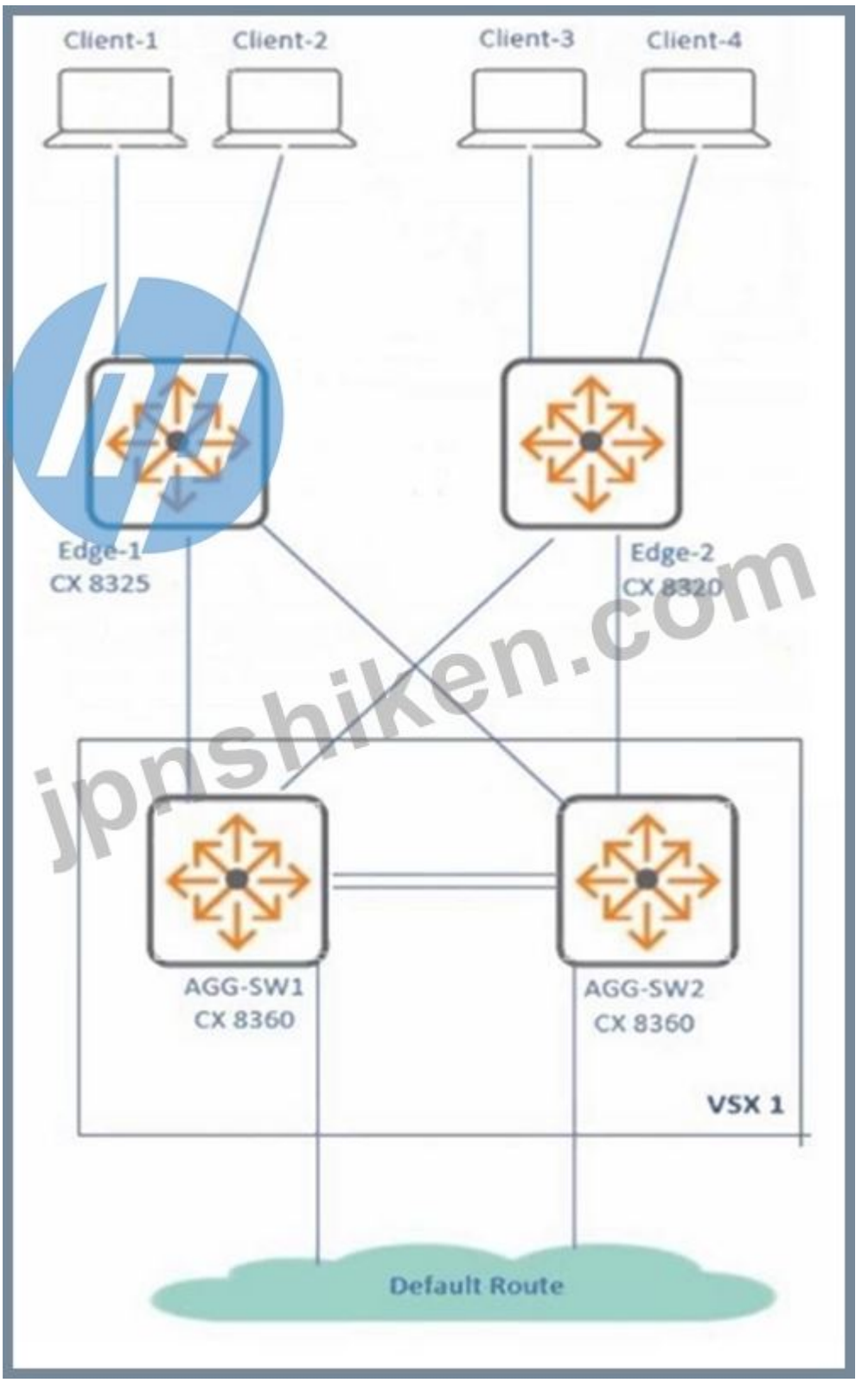
```
ip aspath-list bgp-local permit ^$
route-map bgp-ebgp-out permit
 match aspath bgp-local
 exit
```

D.

```
ip aspath-list bgp-local permit ^$
route-map bgp-ebgp-out deny
 match aspath bgp-local
 exit
```

正解: **C** (コメントを発表する)
トランジットASとなることを避けるため、ローカルで生成されたプレフィックスのみをアドバタイズします。空のパス (^$) に一致するASパスフィルタを使用し、各eBGPネイバーに適用されたアウトバウンドルートマップ内のルートのみを許可します。これにより、あるISPから学習したルートが別のISPに再アドバタイズされることを防ぎます。

質問: **33**
展示品を参照してください。



会議会場では、ネットワーク内で独立したネットワーク ユーザーを相互に保護する必要があります。

顧客の機器を使用してクライアントが相互に通信するのを防ぐにはどうすればよいでしょうか?

A. Edge-1 および Edge-2 に接続されたクライアントでは、コミュニティ VLAN を使用できます。

B. Edge-2 接続クライアントでは、分離された VLAN を使用できます。

C. Edge-1 に接続されたクライアントでは、分離された VLAN を使用できます。

D. Edge-1 および Edge-2 に接続されたクライアントでは、分離された VLAN を使用できます。

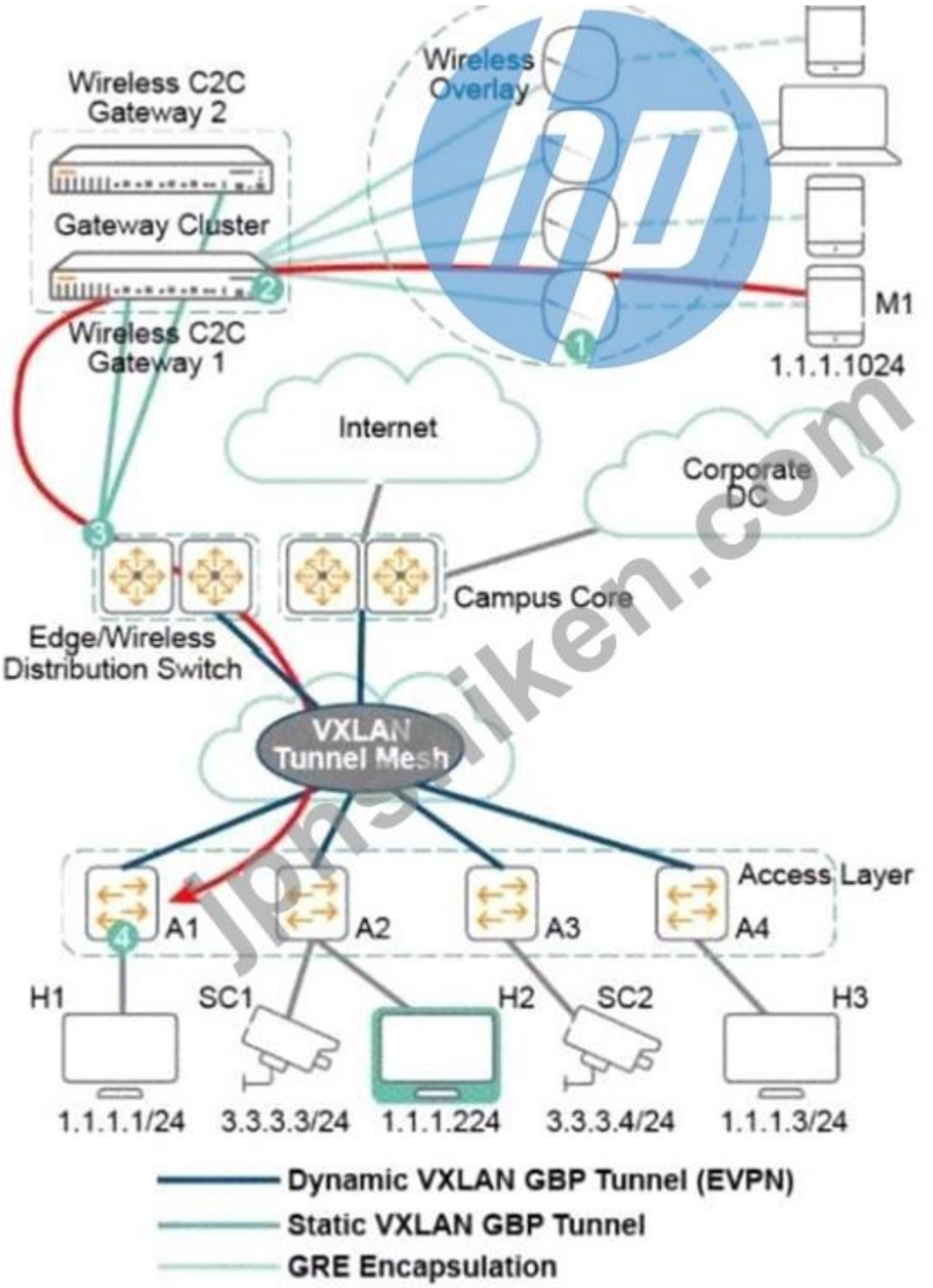
正解: (正解を表示します)
独立したユーザー同士の通信を遮断するには、分離VLANを設定するのが最適な方法です。分離VLANでは、クライアントは外部アクセス用のデフォルトゲートウェイにはアクセスできますが、同じVLAN内の他のクライアントとは直接通信できません。クライアントはEdge-1とEdge-2の両方を経由して接続するため、施設全体でクライアントを完全に分離するには、両方のスイッチに分離VLANを適用する必要があります。

質問: **34**
コマンドを初めて実行したときは、出力は「unknown」と表示されますが、次回実行したときには次の情報が表示されます。

スイッチで問題のトラブルシューティングを行うために実行できる操作にはどのようなものがありますか? (2 つ選択してください)。
A. 診断インターフェーストランシーバーal
B. 診断インターフェース1/VXトランシーバーすべて
C. ケーブル診断 1/1/X
D. 診断ケーブル 1/1/X
E. 1/1/Xトランシーバーすべて診断
正解: **C,E** (コメントを発表する)
問題は、コマンド出力が最初は不明であるものの、その後の実行でインターフェース（1/1/X）の診断情報が表示されるという問題のトラブルシューティングに関するものです。この問題を解決するために適切な診断コマンドを特定することが課題です。
* オプションの分析:
* オプション A (diag interface transceiver al): 構文が正しくありません。「al」は有効なパラメーターではありません。
* オプション B (diag interface 1/VX transceiver all): 構文が正しくありません。「1/VX」は有効なインターフェイス形式ではありません。
* オプションC（diag cable-diagnostic 1/1/X）：正解このコマンドは、インターフェイス1/1/Xでケーブル診断テスト（TDR）を実行し、断線やショートなどのケーブル障害の有無を確認します。
* オプション D (diag cable 1/1/X): 誤り。「diag cable」は有効な AOS-CX コマンドではありません。
* オプションE（diag 1/1/X transceiver all）：正解このコマンドは、ステータス、エラー、信号品質など、トランシーバーの詳細情報を表示し、インターフェースの問題の診断に役立ちます。
* CとEが正しい理由：diag cable-diagnostic 1/1/Xコマンドは、接続の問題を引き起こす可能性のあるケーブル障害を特定するためのTDRテストを実行するために使用されます。diag 1/1/X transceiver allコマンドは、電力レベル、エラー、ハードウェアの問題など、詳細なトランシーバ診

断情報を提供し、インターフェースまたは接続デバイスの問題を正確に特定するのに役立ちます。これらのコマンドは、物理層の問題に関するAOS-CXのトラブルシューティングワークフローに準拠しています。
* 認定目標との関連性:
* トラブルシューティング (10%): 診断コマンドを使用してキャンパス ネットワークの問題をトラブルシューティングします。
* 接続性 (9%): ケーブルやトランシーバーの問題など、デバイスの展開における問題領域の特定が含まれます。
参考文献:
HPE Aruba Networking AOS-CX 構成ガイド: ケーブル診断とトランシーバー診断を網羅した診断コマンド。
HPE7-A06 学習ガイド: AOS-CX スイッチのトラブルシューティング ツールの詳細を説明します。
HPE Aruba ネットワーク技術ドキュメント: AOS-CX トラブルシューティング、診断コマンドの使用方法の説明。

質問**: 35**
展示品の 4 つの numborod スロップを参照してください。



モバイル デバイス M1 からロール H2 へのトラフィックにロール間 ACL を適用する際の 4 番目のステップはどのアクションですか。

A. スイッチ A1 は、宛先 MAC または宛先 IP に基づいて宛先ロールを決定し、ロール間 ACL を適用します。

B. ゲートウェイ 1 は、シアリック VXLAN トンネルを介してトラフィックをエッジ スイッチに転送します。このパケットは、M1 のロールに対応するグループ ポリシー ID を伝送します。

C. AP はパケットを M1 からゲートウェイ 1 に転送します。

D. エッジ スイッチは中間ノードとして機能し、グループ ポリシー ID を静的 VXLAN から動的 VXLAN トンネルに転送し、パケットをスイッチ A1 に転送します。

正解: (正解を表示します)
この質問は、VXLANによるダイナミックセグメンテーションを用いたネットワークにおいて、モバイルデバイス（M1）からロール（H2）へのトラフィックにロール間ACLを適用する際の4番目のステップについて尋ねています。これは、APがパケットをゲートウェイに転送することを最初のステップとして特定した質問17に続くものです。
* オプションの分析:
* オプションA：正解。4番目のステップでは、宛先スイッチ（スイッチA1）が宛先MACアドレスまたはIPアドレスに基づいて宛先ロール（H2）を決定し、ロール間ACLを適用してトラフィックを許可または拒否します。
* オプション B: ゲートウェイが VXLAN トンネルを介してトラフィックを転送する、以前のステップ (おそらく 2 番目または 3 番目) について説明します。
* オプション C: 質問 17 で特定された最初のステップについて説明します。
* オプション D: エッジ スイッチがグループ ポリシー ID を VXLAN 経由で転送する中間ステップ (おそらく 3 番目) について説明します。
* オプション A が正しい理由:HPE Aruba Networking のダイナミック セグメンテーション アーキテクチャでは、VXLAN 環境におけるロールベース ACL のトラフィック フローは次の手順に従います。
* AP はパケットを M1 からゲートウェイに転送します (質問 17)。
* ゲートウェイはソース ロール (M1 のロール) を割り当て、グループ ポリシー ID を使用して VXLAN トンネル経由でパケットを転送します。
* エッジスイッチは、グループポリシーIDをVXLAN経由で宛先スイッチ（A1）に転送します。
* スイッチ A1 は、宛先 MAC または IP アドレスに基づいて宛先ロール (H2) を決定し、グループベース ポリシー (GBP) で定義されているロール間 ACL を適用します。
4 番目のステップはポリシーの適用にとって重要であり、トラフィックがソース ロールと宛先ロール間で定義されたセキュリティ ポリシーに準拠していることを確認し、安全なネットワークセグメンテーションを提供します。
* 認定目標との関連性:
* セキュリティ (10%): 顧客ネットワークにおけるロールベースのセキュリティ ポリシーの設計とトラブルシューティング。
* スイッチング (19%): ポリシー適用のための VXLAN などのレイヤー 2/3 相互接続テクノロジを実装します。
* WLAN (9%): ダイナミック セグメンテーションにおけるワイヤレス トラフィック フローのトラブルシューティング。
参考文献:
HPE Aruba Networking AOS-10 構成ガイド: 動的セグメンテーションと VXLAN、ロールベースのポリシー適用の詳細。
HPE7-A06 学習ガイド: グループベースのポリシーと動的セグメンテーションのワークフローについて説明します。
HPE Aruba ネットワーク技術ドキュメント: トンネル ノードとロールベースの ACL。

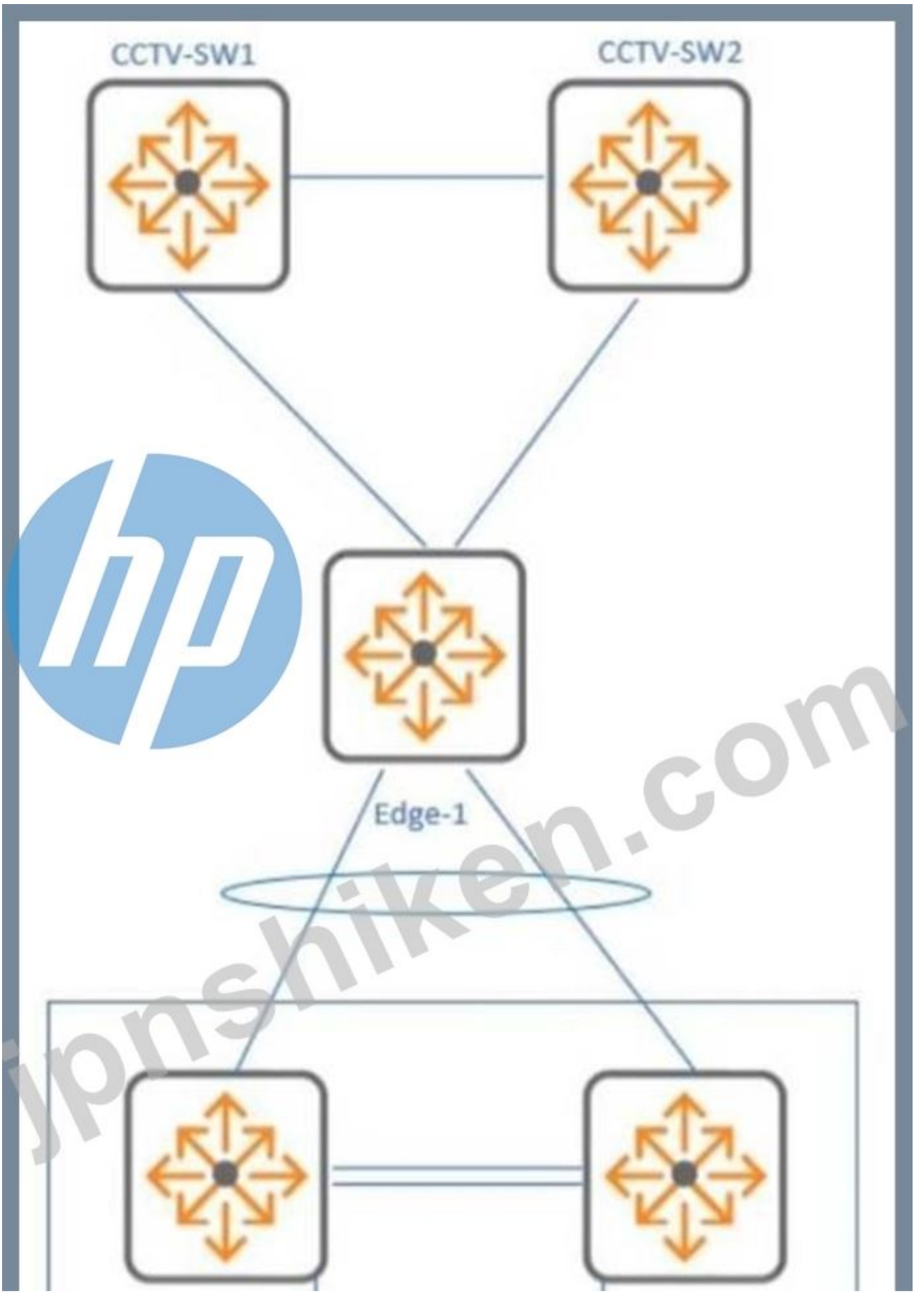
質問: **36**
セキュリティメカニズムとして802.1Xを使用するSSIDを設定しています。Wi-Fi 6ネットワークを展開する際にWPA3-Enterprise（CCM-128）を使用する理由は何ですか？
A. WPA3-Enterprise (CCM-128) は、WPA3-Enterprise Transition Mode とも呼ばれます。これにより、WPA2 クライアントからの接続が可能になります。
B. WPA3-Enterprise (CCM-128) は、WPA3-Enterprise 互換モードとも呼ばれます。WPA2 クライアントからの接続を許可します。
C. WPA3-Enterprise (CCM-128) は WPA3-Enterprise Only Mode とも呼ばれます。WPA2 クライアントはサポートされません。
D. WPA3-Enterprise (CCM-128) は、WPA3-Enterprise 192ビットモードとも呼ばれます。WPA3のみに対応し、特定のEAP証明書暗号を適用します。
正解: **B** (コメントを発表する)
WPA3-Enterprise（CCM-128）は、WPA3-Enterprise互換モードとも呼ばれます。WPA3のセキュリティを提供しながら、WPA2クライアントの接続も許可するため、Wi-Fi 6ネットワークの導入時に下位互換性を確保できます。そのため、混在クライアント環境でWPA2-EnterpriseからWPA3-Enterpriseに移行する場合に最適な選択肢となります。

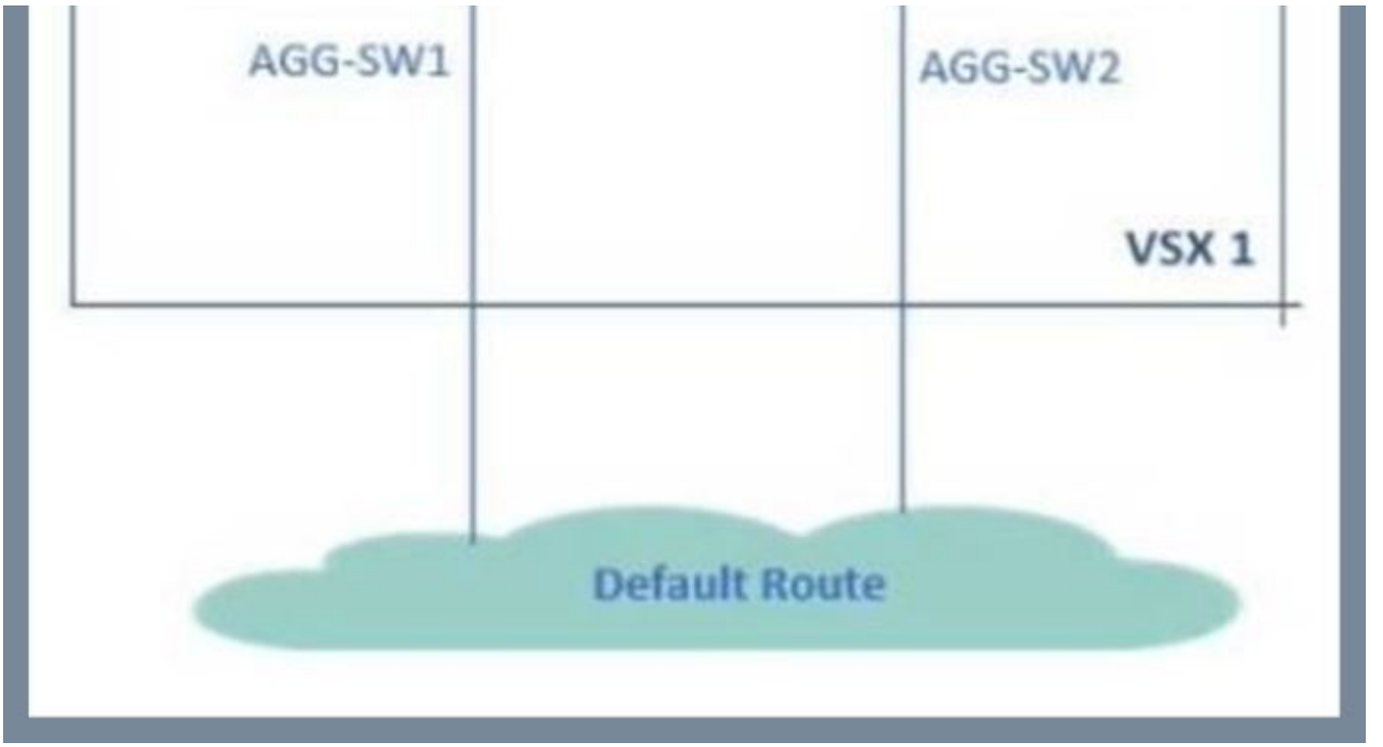
質問: **37**
展示品を参照してください。

```
sw-agg1(config)# show vsx status config-sync
Admin state              : Enabled
Operational State        : Non-Operational
Error State              : SW version mismatch
Recommended remediation : Execute 'show images' to determine which software image is loaded and load the same for both peers
Current time             : Tue Oct  3 11:01:26 2023
Last sync time           : Tue Oct  3 09:56:19 2023
```

スクリーンショットに基づいて、展示物に表示されている状態を修正するには何が必要ですか?
A. プライマリでアクティブなものと同じ OS-CX イメージをセカンダリでも使用します。
B. セカンダリ スイッチで copy running-config vsx-peer を使用します。
C. 拡張ソフトウェア更新プロセスを使用して状態を修正します。
D. 強制 vsx-sync を使用して同期プロセスを開始します。
正解: **A** (コメントを発表する)
この図では、VSX config-sync がエラー状態「SW version mismatch」で動作不能になっていることが示されています。これは、プライマリスイッチとセカンダリスイッチで異なる ArubaOS-CX ソフトウェアバージョンが実行されている場合に発生します。この問題を解決するには、両方のピアで同じ OS-CX イメージを実行する必要があります。推奨される修復手順では、show images を実行してソフトウェアイメージを確認し、両方のピアに同じバージョンがロードされていることを確認することが明示的に示されています。

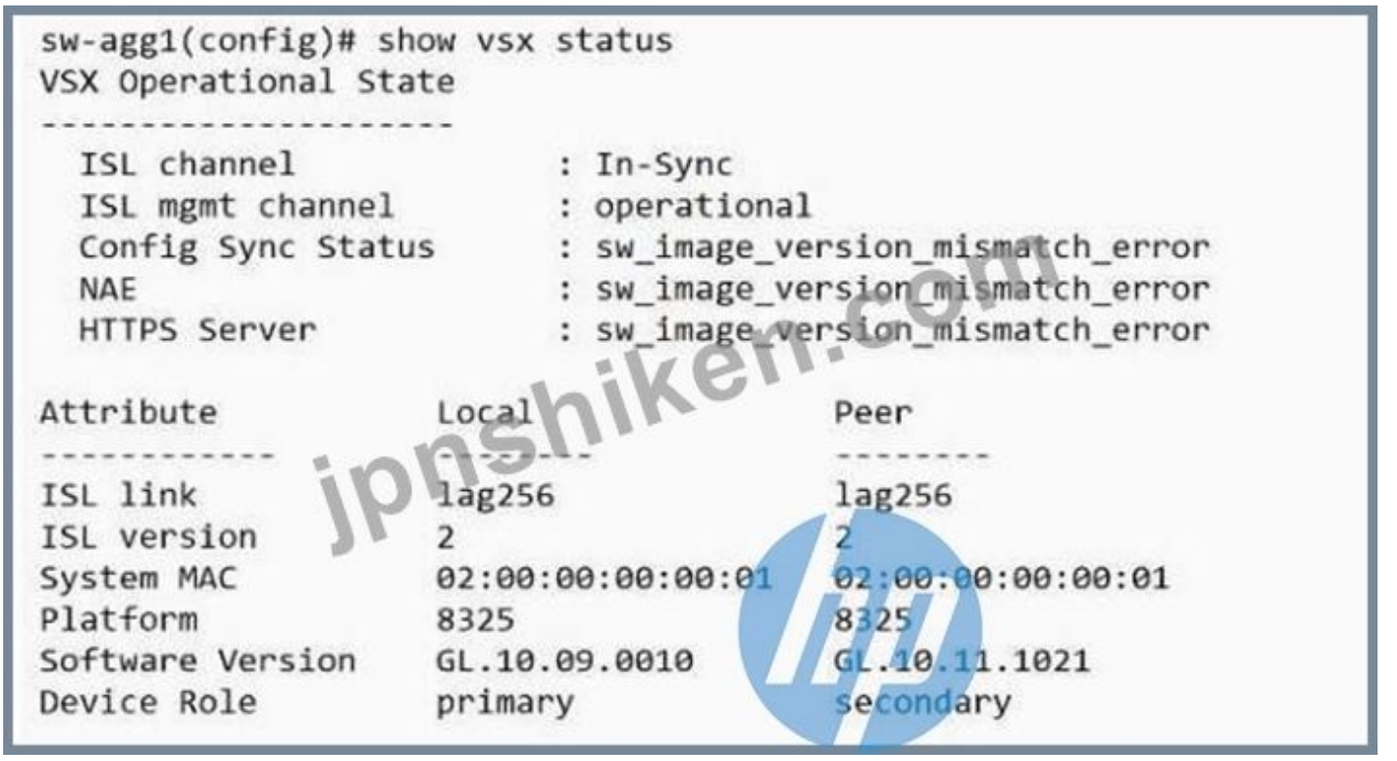
質問: **38**
展示品を参照してください。





VSXクラスタはすでに構成されています。あなたのタスクは、スイッチングインフラストラクチャを導入するCCTVプロバイダーに接続されたEdge-1スイッチの正しい構成を検証することです。CCTVスイッチはSTPをサポートしていません。
自動回復機能を備えた既存のセットアップでループの問題を防ぐために、CCTV-SW1 および CCTV-SW2 に接続する Edge-1 スイッチ ポートで何を設定する必要がありますか?
A. CCTVスイッチポートのLACPフォールバックによるラグを設定する
B. CCTVスイッチポートのスパニングツリーとTNガードタイムアウトを設定します
C. CCTVスイッチポートのBPDUガードタイムアウト値を使用してスパニングツリーを設定します。
D. CCTVスイッチポートにUDLDを使用したスパニングツリーを設定する
正解: **(**正解を表示します**)**
CCTVスイッチはSTPを実行していないため、Edge-1はこれらのポートでSTPを有効にし、自動タイムアウト/リカバリ機能を備えたBPDUガードを使用することで、潜在的なループから自身を保護する必要があります。ループが発生したスイッチがBPDUの送信を開始すると、ポートはエラーディセーブル状態になり、タイムアウト後に自動的に回復します。

質問: **39**
展示品を参照してください。



スクリーンショットに基づいて、セカンダリスイッチの MCLAG インターフェイスをオンラインにするには何が必要ですか?

A. セカンダリで vsx-software-upgrade を使用します。

B. セカンダリ上の NAE エージェントを更新します。

C. プライマリと同じ CX OS バージョンを使用します。

D. プライマリと同じ ServiceOS バージョンを使用します。

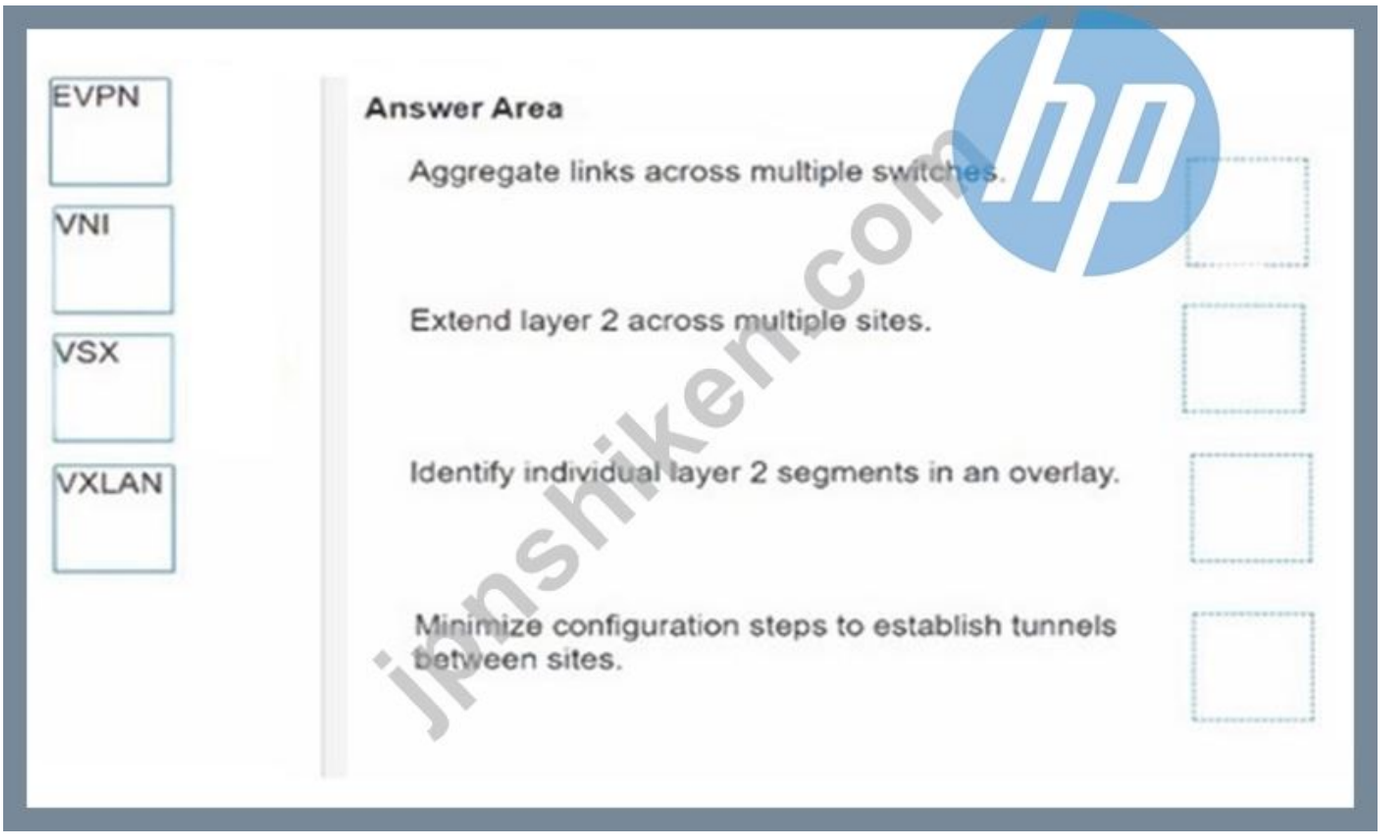
正解: **(**正解を表示します**)**

VSXステータス出力のエラーメッセージ（sw_image_version_mismatch_error）は、プライマリスイッチ（GL.10.09.0010）とセカンダリスイッチ（GL.10.11.1021）で異なるバージョンのAOS-CXソフトウェアが実行されていることを示しています。VSXピアが同期してMCLAGインターフェースをオンラインにするには、両方のデバイスで同じバージョンのAOS-CXソフトウェアが実行されている必要があります。

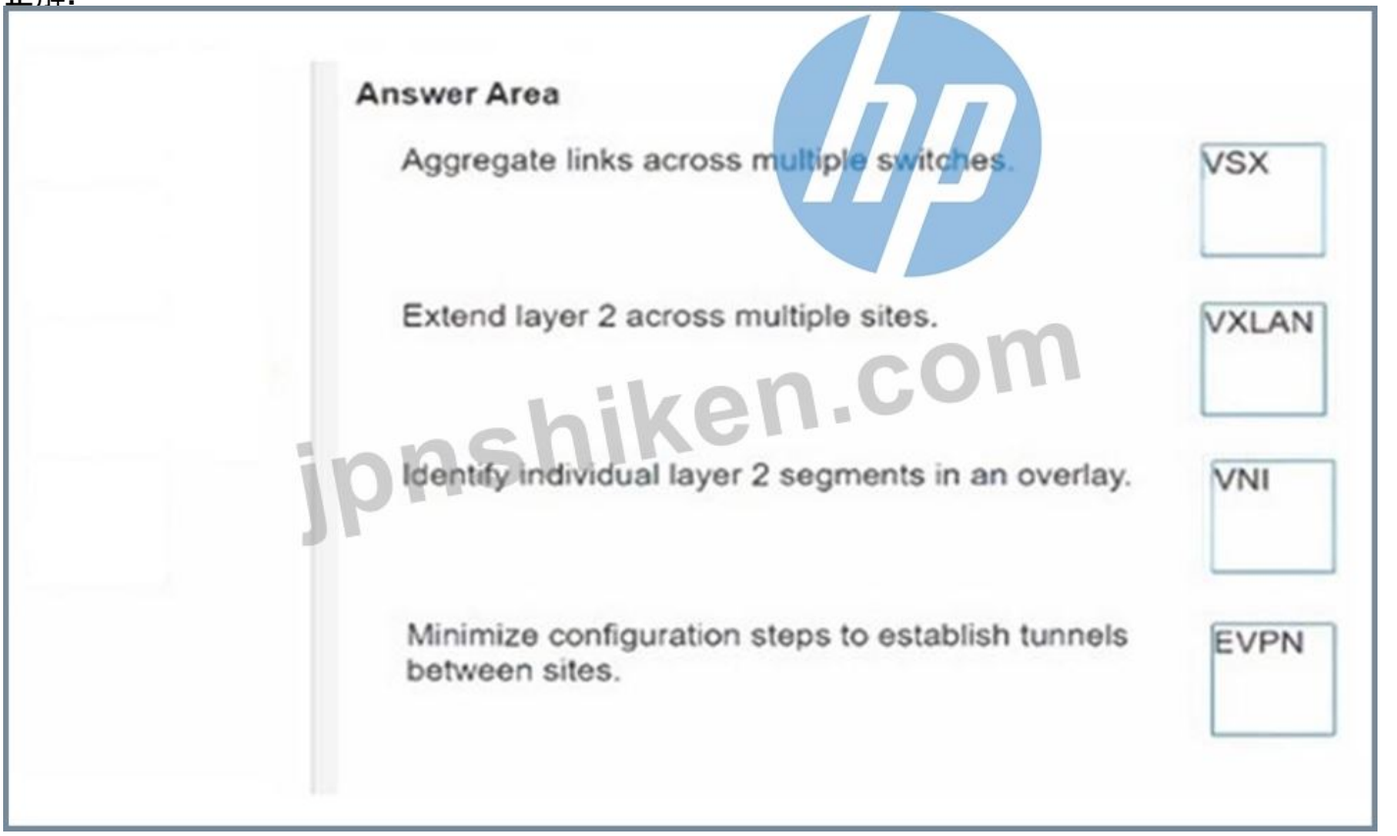
質問: **40**

ドラッグアンドドロップの質問

ネットワーク テクノロジーを顧客の要件に合わせて調整します。



正解:



Explanation:

VSXは、スイッチ間のアクティブ/アクティブリンクアグリゲーションを可能にします。VXLANは、レイヤー2トラフィックをカプセル化し、サイト間のレイヤー3ネットワークに拡張します。VNI（VXLANネットワーク識別子）は、VXLANオーバーレイ内のレイヤー2セグメントを識別します。EVPNは設定を簡素化し、サイト間のVXLANトンネルのコントロールプレーンシグナリン

グを自動化します。

質問: **41**
ドラッグアンドドロップの質問
顧客の要件を関連するコマンドと一致させます。

正解:

質問: **42**
同僚にVSXについて説明するという課題があります。AOS-CXにVSXを実装するためのベストプラクティスと考えられる項目を3つ選択してください。3つ選択してください。）
A. ダウンストリーム デバイスの ZTP を容易にするために、すべてのトランク上で VLAN 1 を許可します。
B. 必要に応じてプライマリのスイッチ交換を簡素化するために、VSX システム MAC を手動で設定します。
C. エンドポイントで必要な場合にジャンボ フレームの転送を許可するように ISL リンク上の MTU を調整します。
D. vsx-sync を有効にする前に、プライマリ ノードとセカンダリ ノードの両方ですべての VLAN を手動で構成します。
E. デフォルトのキープアライブ タイマーを ISL ホールド間隔と一致するかそれを超えるように調整します。

F. 両ノード間のキープアライブ接続に直接 L3 回線を使用します。
正解: **(**正解を表示します**)**
手動で VSX システム MAC を設定すると一貫性が確保され、ハードウェア障害が発生した場合の交換が簡単になります。
エンドポイントがジャンボ フレームを使用するときに断片化を回避するには、ジャンボ フレームをサポートするように ISL 上の MTU を調整するのがベスト プラクティスです。
VSX ピア間のキープアライブに直接 L3 回線を使用すると、信頼性が確保され、中間デバイスへの依存を回避できます。

質問: **43**
OSPF ルータは、E1 アドバタイズメントと E2 アドバタイズメントの両方によって外部ネットワークへのパスを学習しました。両方のルートのパス コストは同じです。
ルータはどのパスを優先しますか?
A. パスの競合が解決されるまで、両方のルートが抑制されます。
B. ルータは ECMP を使用して両方のパスを均等に使用します。
C. ルータは E1 パスを優先します。
D. ルータは E2 パスを優先します。
正解: **C (**コメントを発表する**)**
同じ宛先に等コストのOSPF E1（外部タイプ1）ルートとE2（外部タイプ2）ルートの両方が存在する場合、ルータは常にE1パスを優先します。これは、E1ルートにはASBRに到達するための外部コストと内部OSPFコストの両方が含まれるため、パス選択の精度が向上するためです。

質問: **44**
クライアントは、問題のトラブルシューティングプロセスを自動化し、可視性を向上させたいと考えています。どのようなソリューションをクライアントに推奨しますか？
A. HPE Aruba ネットワーキング F3bric Compose
B. HPE Aruba ネットワーキング スイッチ マルチ編集ソフトウェア
C. Python などのスクリプトを使用してプロセスを自動化します。
D. HPE Aruba Networking Centralに統合されたAIOps
正解: **(**正解を表示します**)**
お客様はトラブルシューティングプロセスを自動化し、ネットワークの可視性を向上させたいと考えています。推奨されるArubaソリューションを特定する必要があります。
* オプションの分析:
* A. HPE Aruba Networking Fabric Composer: 一般的なキャンパスのトラブルシューティングの自動化ではなく、主にデータセンター ファブリックのプロビジョニングと管理を目的としたツールです。
* B. HPE Aruba Networking Switch マルチ編集ソフトウェア: 複数のスイッチに変更を適用するための構成管理機能 (Central や NetEdit など) を指す可能性があり、主に自動トラブルシューティングや可視性に重点が置かれていません。
* C. Pythonなどのスクリプトによるプロセスの自動化 :AOS-CXはオンボックススクリプト

NAE）とREST APIをサポートしており、監視とトラブルシューティングのためのカスタム自動化を実現します。強力ではありますが、開発には労力がかかります。
* D. HPE Aruba Networking Centralに統合されたAIOps：Aruba CentralのAIOps機能は、可視性を高め、トラブルシューティングの側面を自動化するために特別に設計されています。AIを活用しています。
/ML は、ネットワーク データを分析し、異常を検出し、潜在的な問題に関する洞察を提供し、イベントを相関させ、規範的な推奨事項を提供することで、可視性の向上とトラブルシューティングの自動支援に対するクライアントのニーズに直接対応します。
* 結論：カスタムスクリプト（C）は自動化を可能にしますが、Aruba Central AIOps（D）は、HPE Aruba Networkingが特別に販売・設計したプラットフォーム統合ソリューションであり、キャンパスネットワークのトラブルシューティングにおける可視性の向上と自動化されたインサイトを提供します。Arubaエコシステム内でこれらの目標を達成するための選択肢の中で、最も直接的で推奨されるソリューションです。
参考資料:Aruba Central ドキュメント (AIOps 機能)、AOS-CX NAE および REST API ドキュメント。
これは、「トラブルシューティング」（10%）と「パフォーマンスの最適化」（6%）の目標に関連しています。

質問: **45**
AP の新しいドアロックが機能しない原因はどのような問題でしょうか?
A. AP への AT 電力が大きすぎます。
B. AP への BT 電力が大きすぎます。
C. AP への AF 電力が不十分です。
D. AP への AT 電力が不十分です。
正解: **C (**コメントを発表する**)**
802.3af（AF）PoEは最も少ない電力を供給します。APに接続されたドアロックなど、多くの新しいデバイスは、より多くの電力（ATまたはBT）を必要とします。AF電力のみの供給では、APと接続デバイスの両方に十分な電力を供給できない可能性があります。

質問: **46**
VSX クラスタ内の CX 10000 スイッチのペア間で同期されるテーブルはどれですか? (2 つ選択してください。)
A. リンク層検出プロトコル (LLDP)
B. 動的ホスト制御プロトコル (DHCP)
C. アドレス解決プロトコル (ARP)
D. IPルーティング
E. BGPネイバー
正解: **(**正解を表示します**)**
VSXクラスタでは、CX 10000ピア間でARPテーブルとIPルーティングテーブルが同期されます。これにより、一貫した転送とシームレスなフェイルオーバーが確保され、両方のスイッチで同じ

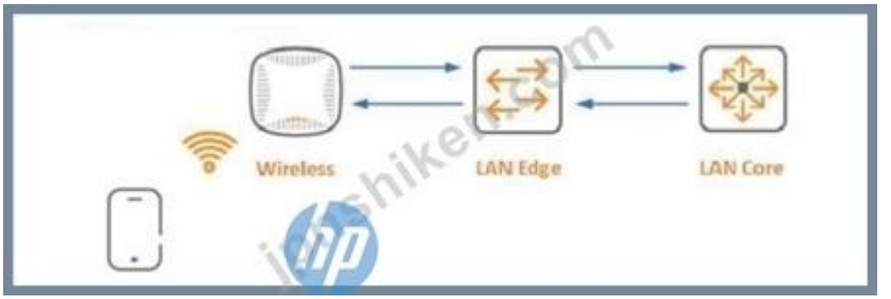
ホストとルーティング情報を参照できます。BGPネイバーやLLDPなどのプロトコル固有の状態は同期されず、各ピアで個別に確立されます。

質問: **47**
AOS-10を使用してHPE Aruba Networkingゲートウェイクラスターを構成しています。ゲートウェイの機能について正しいものはどれですか（2つ選択してください）。
A. PAPI トラフィックは IPSEC トンネルを通過しています。
B. ゲートウェイを手動でプロビジョニングする場合、LACP はサポートされません。
C. AP とゲートウェイ間のマルチバージョンはサポートされていません。
D. AOS-10 は、最初のフェイルオーバーに対してのみ、高価値クライアント セッションの同期をサポートします。
E. トンネル モードのユーザー トラフィックはデフォルトで暗号化されます。
正解: **A,E (**コメントを発表する**)**
PAPIトラフィックはIPSECトンネルを通過します → 正解です。AOS-10では、AP-ゲートウェイ制御トラフィック（PAPI）はIPsecを使用して保護されます。
トンネルモードのユーザートラフィックはデフォルトで暗号化されます → 正解です。トンネルSSIDモードで送信されるクライアントトラフィックは、AP-ゲートウェイトンネルを介して自動的に暗号化されます。

質問: **48**
ユーザーのデバイスがEAP-TLS認証を使用した802.1X認証に失敗しています。クライアント側の証明書は有効です。この問題の原因として考えられるものは何ですか？（2つ選択してください。）
A. ユーザーのデバイスは正しいゲートウェイを使用するように構成されていません。
B. スイッチポートに適用されたACLに問題があります
C. EAP タイプが一致しません。
D. ユーザーのデバイスが間違ったMACアドレスを使用しています
E. NAD は DNS サーバーと通信できません。
正解: **(**正解を表示します**)**
ユーザーのデバイスは 802.1X EAP-TLS 認証に失敗しましたが、クライアント側の証明書は有効であることがわかっています。
考えられる原因を 2 つ挙げてください。
* EAP-TLS プロセス: クライアントと RADIUS サーバー (NAD によってプロキシされる) 間の相

互証明書検証と TLS ハンドシェイクが含まれます。
* 原因 (クライアント証明書は正常):
* サーバー証明書の問題: クライアントがサーバー証明書を信頼していません (信頼されていない CA、名前の不一致、期限切れ)。
* EAP タイプの不一致: クライアント サプリカントが RADIUS サーバ ポリシーとは異なる EAP タイプに設定されています。
* RADIUS サーバーの問題: ポリシーの構成ミス、ユーザーが見つからない、内部エラー。
* NAD <-> RADIUS 通信障害:スイッチが RADIUS サーバーに到達できません (IP 接続、ファイアウォール、ルーティング)。共有秘密が正しくありません。
* クライアント サプリカントの誤った構成: 証明書自体以外の ID、設定が正しくありません。
* ネットワーク パケット損失。
* オプションの分析 (2つ選択):
* A: ゲートウェイが間違っていると、L3 の事後認証に影響します。
* B: ACL による EAPoL/RADIUS のブロックは可能ですが、構成エラーほど一般的ではありません。
* C:EAP タイプの不一致: 失敗につながる非常に一般的な構成エラー。
* D: MAC アドレスが間違っていることは、EAP-TLS の失敗自体には関係ありません。
* E: NAD が DNS サーバーと通信できません: DNS は EAP-TLS に直接関与していません。
ただし、より広く解釈すると、NAD が RADIUS サーバーと通信できない (IP ルーティング、ファイアウォール、またはサーバー アドレスが正しくない) と解釈され、これは非常に一般的な失敗の原因となります。
* 結論: 基本的な証明書の有効性が想定される場合、EAP タイプの不一致 (C) が主な原因として考えられます。
ネットワーク アクセス デバイス (NAD - スイッチ) が RADIUS サーバー (E、広義には RADIUS 到達可能性と解釈されます) と通信できないことも、障害の原因のもう 1 つの主要なカテゴリです。
参考資料 :EAP-TLS (RFC 5216)、802.1Xトラブルシューティングガイド、ClearPassドキュメント。これは 「トラブルシューティング」(10%)、 「セキュリティ」(10%)、 「認証/承認」(9%)に関連します。

質問: **49**
展示品を参照してください。



有線と無線の両方に対してエンドツーエンドの QoS 設計を実装する必要があります。
正しい DSCP タグを維持するために LAN 側で何が必要ですか?

A. WLAN DSCP値が異なるため、顧客DSCPマッピングを作成します
B. QoS内部ポート内のすべてのDSCPマークされたパケットを信頼する
C. WLAN側でWMMからDSCPへのマッピングを作成する
D. LANエッジにWMMからDSCPへのマッピングを作成する
正解: **B** (コメントを発表する)
エンドツーエンドのQoS設計では、トラフィックが有線LANに入ると、APは既にWMM（ワイヤレスQoS）値をDSCP値にマッピングしています。これらのQoSマーキングを維持するには、LANエッジデバイスとLANコアデバイスがDSCP値を再マーキングするのではなく、信頼するように設定する必要があります。DSCPマーキングされたパケットを信頼することで、ワイヤレス側からのQoSタグが有線LANを通じて一貫して伝送されることが保証されます。

質問: **50**
HPE ネットワーク経由で大容量ファイルを転送中にパケット ドロップが発生した場合、パフォーマンス チューニングのためにどのパラメータをチェックする必要がありますか?
A. LACP優先度
B. VLAN優先度
C. MANサイズ
D. MACエージングタイマー
正解: **C** (コメントを発表する)

質問: **51**
顧客は、次のスイッチ ポートを持つ CX 6300 VSF スタックの 2 つのルータとローカル AS 65000 を使用して eBGP ピアリングを設定しました。
[ルーターに接続するポート - 1 10.10.10.2]

```
int lag 1
- int 1/1/1
- int 2/1/1
  -interface vlan 10
        ip address 10.10.10.1/30
```

[ルータに接続するポート - 2 ip 10.10.20.2]

LAGはサードパーティ製のL2スイッチに接続されており、eBGPルーターのトランジットネットワークとして使用されます。BGPピアリングの問題を最適化するため、AOS-CXスイッチはグローバル設定で構成されています。

```
bfd
    bfd min-receive-interval 2000
    bfd min-transmit-interval 2000
    bfd detect-multiplier 3
```

eBGP ピアとの双方向転送を有効にするには、AOX-CX スイッチで何を行う必要がありますか?

A.
```
router bgp 65000
    address-family ipv4 unicast
       neighbor 10.10.10.2 fall-over bfd
       neighbor 10.10.20.2 fall-over bfd
```

B.
```
router bgp 65000
      neighbor 10.10.10.2 fall-over bfd
      neighbor 10.10.20.2 fall-over bfd
```

C.
```
int 1/1/1-1/1/2, 2/1/1-2/1/2
  fall-over-bfd
```

D.
```
interface lag1-2
  fall-over bfd
```

正解: **D** (コメントを発表する)

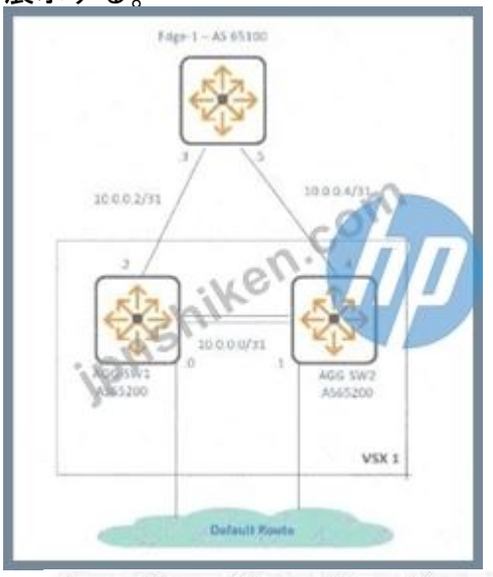
BFDは高速な障害検出プロトコルです。BGPピアリングに使用されるLAGインターフェースでフォールオーバーBFDを有効にすると、LAGが論理レベルでまだ稼働している場合でも、BFDによって検出されたリンク障害にBGPが即座に反応することが保証されます。これにより、ブラックホール化やルーティングの問題を回避できます。

質問: **52**

お客様のAOS-CXネットワークでBGPの問題が発生しています。ユーザーには適切なロールと権限が割り当てられているにもかかわらず、ネットワーク上の特定のリソースにアクセスできませ

ん。
この問題の最も可能性の高い原因は何でしょうか?
A. HPE Aruba Networking ClearPass の構成が正しくありません。
B. GBP タグがユーザーのトラフィックに正しく適用されていません。
C. GBP データベースが破損しています。
D. ユーザーに正しい GBP クラスが割り当てられていません。
正解: **B** (コメントを発表する)
AOS-CXでは、グループベースポリシー（GBP）はユーザートラフィックの正しいタグ付けに依存しています。GBPタグが適切に適用されていない場合、適切なロールと権限を持つユーザーであっても、意図したネットワークリソースにアクセスできません。そのため、ここで説明したBGP関連の問題は、タグの不適切な適用が原因である可能性が最も高いと考えられます。

質問: **53**
展示する。



A.
```
router bgp 65100
  10.0.0.2 remote-as 65200
  10.0.0.4 remote-as 65200
     address-family ipv4 unicast
     neighbor 10.0.0.2 update-source loopback 0
     neighbor 10.0.0.4 update-source loopback 0
```

B.
```
router bgp 65100
  10.0.0.2 remote-as 65200
  10.0.0.4 remote-as 65200
     address-family ipv4 unicast
     neighbor 10.0.0.2 route-reflector-client
     neighbor 10.0.0.4 route-reflector-client
```

C.
```
router bgp 65100
  10.0.0.2 remote-as 65200
  10.0.0.4 remote-as 65200
     address-family ipv4 unicast
     neighbor 10.0.0.2 default-originate
     neighbor 10.0.0.4 default-originate
```

```
router bgp 65100
  10.0.0.2 remote-as 65200
  10.0.0.4 remote-as 65200
     address-family ipv4 unicast
     neighbor 10.0.0.2 activate
     neighbor 10.0.0.4 activate
```

D.

正解**: (**正解を表示します**)**

質問は、OSPF仮想リンクを設定してエリア0を非バックボーンエリアに拡張することに関するもので、図（提供されていません）と4つの設定オプション（A～D）に基づいています。図は入手できないため、トランジットエリア（例エリア1）を介して2つのエリア0セグメントを接続するために仮想リンクが必要となる典型的なシナリオを想定します。

* オプションの分析（想定されるコンテキスト）：仮想リンクは、OSPFプロセスで area <transit-area> virtual-link <router-id> コマンドを使用して設定されます。正しいオプションには以下が含まれる可能性があります。

* オプション A: 仮想リンクの構文が正しくないか、ルータ ID/エリアが正しくありません。

* オプション B: 構成が正しくありません。仮想リンクが欠落しているか、間違ったパラメータを使用している可能性があります。

* オプションC：正解です。適切なコマンド（例area 1 virtual-link 2.2.2.2）が含まれている可能性があります。ここで、area 1 はトランジットエリア、2.2.2.2 はリモートABRのルータIDです。

* オプション D: 誤り。不要な仮想リンクまたは誤った仮想リンクが構成されている可能性があります。

* オプションCが正しい理由:OSPFでは、すべてのエリアがバックボーンエリア（エリア0）に接続する必要があります。2つのエリアが
0セグメントが非バックボーンエリア（例えばエリア1）によって区切られている場合、エリア境界ルータ（ABR）間に仮想リンクが設定され、トランジットエリアを介してエリア0が論理的に拡張されます。コマンドエリア
<transit-area> virtual-link <remote-router-id> は、トランジットエリアとリモートABRのルータIDを指定するために使用されます。オプションCは、標準のOSPF仮想リンク設定に基づく正しい構文とパラメータを提供し、エリア0の接続性と適切なルートアドバタイズメントを確保するものと想定されています。

* 認定目標との関連性:

* ルーティング (16%): 仮想リンクを含む OSPF トポロジの設計とトラブルシューティング。

* トラブルシューティング (10%): OSPF エリアの接続性の問題を解決します。

参考文献:

HPE Aruba Networking AOS-CX 構成ガイド: OSPF 構成、仮想リンクのセットアップの詳細。

HPE7-A06 学習ガイド: 仮想リンクなどの OSPF の高度な構成について説明します。

RFC 2328: OSPF バージョン 2、仮想リンク機能について説明します。

質問**: 54**

VSX クラスタ内の 2 つの CX 8325 スイッチの構成で、プロトコルベースのポート冗長性をサポートするためのゼロタッチ プロビジョニングのために 7000 ゲートウェイのリンク アグリ

ゲーションをどのように準備しますか?

A.
```
int lag 1
     lacp mode active
     lacp fallback
```

B.
```
int lag 1 multi-chassis
     lacp mode active
     lacp fallback
```

C.
```
int lag 1 multi-chassis
     lacp enable
     lacp fail-over
```

D.
```
int lag 1
     lacp enable
     lacp fail-over
```

正解: **B** (コメントを発表する)

目標は、ゼロタッチプロビジョニング（ZTP）中のAruba 7000シリーズゲートウェイに接続するVSXクラスタ（CX 8325スイッチのペア）上にリンクアグリゲーショングループ（LAG）を設定することです。LAGは「プロトコルベースのポート冗長性」（LACP）をサポートし、ZTP中の接続を許可する必要があります。

* VSX要件：LAGはVSXペアとして動作する2つの別々の物理スイッチに接続するため、スイッチ上でLAGをマルチシャーシLAG（MC-LAG）として設定する必要があります。これにより、ゲートウェイは両方の上流デバイスにわたって単一のLAGを形成できます。これは、インターフェース lag <id>コンテキストのコマンドmulti-chassisで有効になります。

* プロトコル冗長性の要件：「プロトコルベースのポート冗長性」とは、スイッチとゲートウェイ間のLAGバンドルを動的にネゴシエートおよび管理するために、Link Aggregation Control Protocol（LACP）を使用する必要があることを意味します。コマンド lacp mode active は、LACPをアクティブネゴシエーションモードで有効にします。

* ZTP要件：ZTP実行中、ゲートウェイはLACP設定を含むすべての設定がすぐに有効にならない場合があります。ゲートウェイがZTPの基本的なIP接続（DHCP/DNS経由でActivate/Centralへ接続するなど）を確立できるようにするには、LACPネゴシエーションが完了していない場合でも、スイッチポートはトラフィックを許可する必要があります。LACPフォールバック機能はこれを可能にし、ピアからLACP PDUを受信しない場合に、個々のLAGメンバーポートをアクティブにすることができます。

* オプションの分析:

* A) lacp mode active および lacp fallback を設定しますが、VSX に必要な multi-chassis コマンドがありません。

* B) LAGをマルチシャーシとして正しく設定し、LACPモードをアクティブにし、LACPフォールバックを有効にします。これですべての要件を満たします。

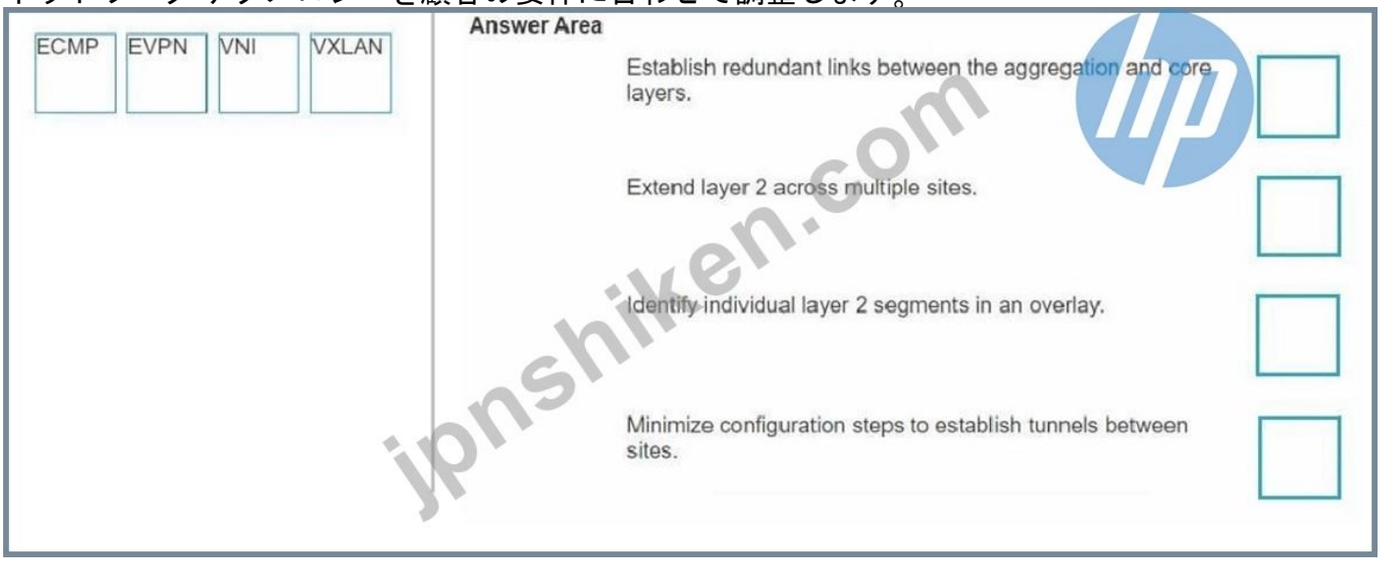
* C) マルチシャーシを構成しますが、lacp mode active および lacp fallback の代わりに、潜在的に古いまたは標準的でない構文 lacp enable および lacp fail-over を使用します。

* D) マルチシャーシ コマンドが欠如しており、潜在的に古い/標準的ではない構文が使用されています。

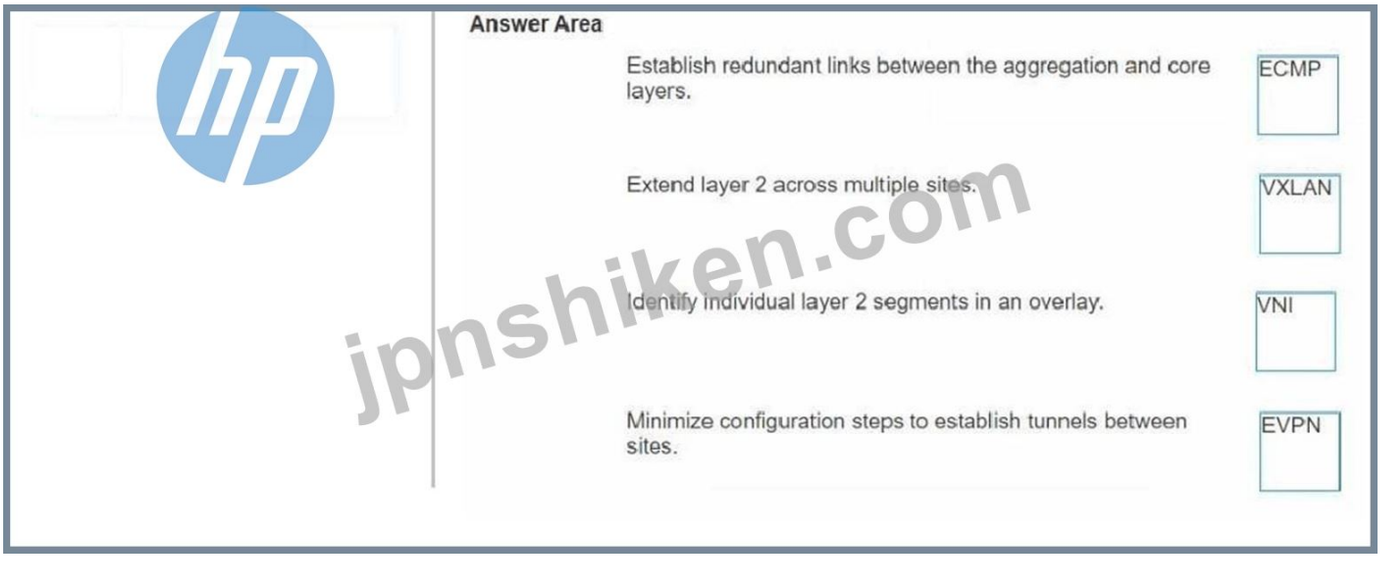
* 結論: オプション B は、標準の AOS-CX 構文を使用して、冗長性のために LACP が有効にされ、ZTP 中のゲートウェイ接続をサポートするために LACP フォールバックが有効にされた VSX ペアで MC-LAG を作成するための完全かつ正しい構成を提供します。

参考資料：AOS-CX VSXガイド（MC-LAG構成）、AOS-CXリンクアグリゲーションガイド（LACP、LACPフォールバックコマンドとその使用方法）、ArubaGateway ZTPドキュメント。これは、「ネットワークの回復力と仮想化」（8%）、「スイッチング」（19%）、「接続性」（9%）の目標に関連します。

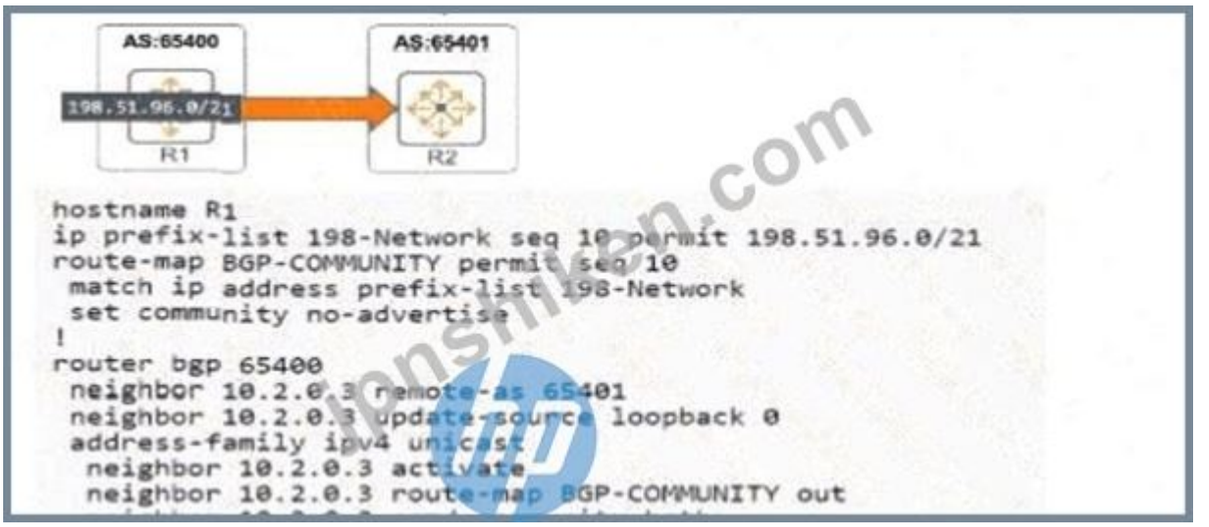
質問: **55**
ドラッグアンドドロップの質問
ネットワーク テクノロジーを顧客の要件に合わせて調整します。



正解:



質問: **56**
展示品および譲渡サンプルを参照してください。



IPv4 アドレス ファミリに「neighbor 10.2.0.3 send-community both」というステートメントを追加すると、どのような効果がありますか? (2 つ選択してください。)

A. R1 が R2 と標準コミュニティおよび拡張コミュニティを送受信する機能をネゴシエートします。

B. この機能は、R2 との R1 確立セッションに影響を与えることなく有効になります。

C. R1がNLRIレコードを持つコミュニティのインバウンドとアウトバウンドの両方向での交換を許可するようになります。

D. R1 と R2 間の既存の BGP ピアリングがフラップする原因になります。

E. R1 が、R2 とタイプ 1 およびタイプ 2 のすべてのコミュニティをインポートおよびエクスポートする機能についてネゴシエートするようになります。

正解**: (**正解を表示します**)**

質問は、ルータ R1 上のネイバー R2 (10.2.0.3) の IPv4 アドレス ファミリ コンテキストの下にある BGP 設定にコマンド neighbor 10.2.0.3 send-community both を追加した場合の効果について尋ねています。

* send-community both:このコマンドは、R1に標準（RFC 1997）および拡張（RFC 4360）BGPコミュニティ属性の両方をネイバーR2に送信するよう指示します。デフォルトでは、コミュニティは送信されません。

* BGP機能ネゴシエーション :コミュニティアドバタイズメントなどの機能の追加または変更は、セッション確立時にネイバー間で交換されるBGP機能を変更します。これらの機能に変更を加える場合は、ピアが新しい機能を使用して再ネゴシエートできるように、BGPセッションをリセット（フラップ）する必要があります。

* オプションの分析（2つ選択）:

* A: 正解です（一部）。R1は標準コミュニティと拡張コミュニティを送信できます。受信できるかどうかは、ピアとローカルの設定に依存します。この機能はセッションリセット時にネゴシエートされます。

* B: 不正解です。機能を変更するにはセッションのフラップが必要であり、影響がないわけではありません。

* C: 不正解です。これは主にR1からの送信を許可します。ネイバーがアクティブ化されている場合、受信の受け入れは暗黙的に行われます。

* D: 正解です。send-community を有効にするなど、BGP ネイバーの機能を変更すると、変更を有効にするために BGP セッションのリセット (フラップ) が必要になります。
* E: 用語が間違っています (「インポート/エクスポート」、「タイプ 1/タイプ 2 コミュニティ」)。
* 結論: このコマンドにより、R1 はコミュニティを送信できるようになります (A は目的/機能について説明します)。このコマンドを既存のセッションに追加すると、セッションは再ネゴシエーションのためにフラップされます (D は直接的な結果について説明します)。
参考資料:RFC 1997、RFC 4360、AOS-CX BGP構成ガイド（コミュニティ、ネイバー構成）。これは「ルーティング」(16%）の目標に関連します。

質問**: 57**
ダイナミック セグメンテーションを使用するためのベスト プラクティスは何ですか?
A. UBT を使用して、特定の種類のデバイス用に分離されたネットワークを作成します。
B. ロールベースのアクセスとオーバーレイ テクノロジを組み合わせて、階層化されたセキュリティ アプローチを作成します。
C. Wi-Fi 経由でネットワークに接続されているデバイスでのみ、ダイナミック セグメンテーションを使用します。
D. LUR を使用してデバイスの場所に基づいてロールを割り当て、DUR を使用してユーザー ID に基づいてデバイスにロールを割り当てます。
正解**: (**正解を表示します**)**
この質問は、ダイナミック セグメンテーションの使用に関するベスト プラクティスを尋ねています。
* ダイナミックセグメンテーションの概要 :ロールベースアクセス制御、トラフィックトンネリング（UBTなど）、オーバーレイテクノロジー（VXLAN/GREなど）を組み合わせることで、有線および無線クライアントに統一されたポリシーとセグメンテーションを提供するアーキテクチャです。ポリシーは、通常はArubaゲートウェイで一元的に適用されます。
* オプションの分析:
* A: UBT はコンポーネントですが、ダイナミック セグメンテーションは、UBT を使用して分離されたネットワークを作成するだけではありません。
* B: 中核原則を正しく説明しています。ロールベースのアクセス（whogetswhatポリシーの定義）とオーバーレイ技術（ポリシー適用ポイントへのトラフィックの転送とセグメンテーションの提供）を組み合わせて使用します。これにより、階層化されたセキュリティアプローチが実現します。
* C: 不正解です。主な利点は、有線アクセスと無線アクセスの両方でポリシーが統一されていることです。
* D: LUR と DUR はロール タイプですが、その割り当て方法は、ダイナミック セグメンテーション自体の基本的な説明ではありません。
* 結論: オプション B は、ロールベースのポリシーとオーバーレイ ネットワークを統合して安全で統合されたアクセス制御を実現する、ベスト プラクティス アプローチとしての動的セグメンテーションの本質を正確に捉えています。

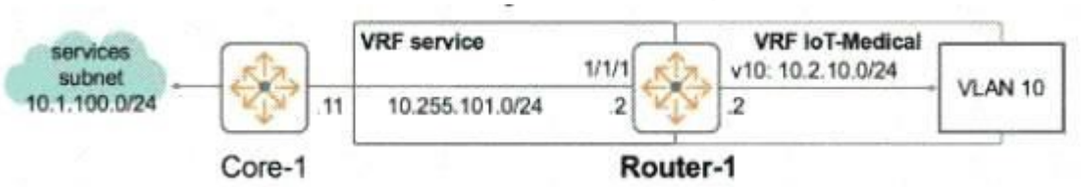
参考資料：Aruba Dynamic Segmentation ソリューションのガイド、ホワイトペーパー、構成例。これは 「セキュリティ」（10%）、 「認証/認可」（9%）、 「接続性」（9%）に関連します。

質問: **58**
セキュリティ管理者から、ユーザー 「radius-test」からのHPE Aruba Networking ClearPass Access Trackerイベントの数について苦情が寄せられています。以下の設定で、イベント数を減らすことは可能でしょうか？

```
radius-server tracking user-name radius-test password plaintext Aruba123!
radius-server host 10.1.1.1 tracking enable
```

A. 追跡の再試行回数を減らします。
B. 'any' トラッキング モードを設定します。
C. 「デッドオンリー」トラッキング モードを設定します。
D. 追跡間隔を長くします。
正解: **(正解を表示します)**
上記の設定により、テストユーザー radius-test を使用したRADIUSサーバーのトラッキングが有効になります。デフォルトでは、すべてのプローブ試行がログに記録されるため、アクセストラッカーイベントが継続的に生成されます。
イベント数を減らすには、トラッキングモードをデッドオンリーに変更する必要があります。これにより、RADIUSサーバーが到達不能とマークされている場合にのみ認証プローブが制限されます。これにより、ClearPassは障害が発生した場合にのみテスト認証を認識するため、不要なログエントリが大幅に削減されます。

質問: **59**
ルータ 1 の現在の構成を示す図を参照してください。



VLAN 10のクライアントは、10.1.100.0/24サブネットでホストされているサービスにアクセスする必要があります。これにより、Rculer-1に現在存在しないルートが1つ追加されます。
ルータ1に10.2.10.0/24から10.1.100.0/24へのルートをインストールするスクリプトはどれですか？ この回答では戻りパスは必要ありません。
A. Core-1 は VRF サービスの一部ではないため、解決策はありません。
B. IPルート 0.0.0.0/0 10.255.101.11 VRFサービス
IPルート 10.1.100.0/24 1/1/1:10.255.101.11 VRF IoT-医療
C. ip route 0.0.0.0/0 10.255.101.11 VRF サービス
IPルート 10.1.100.0/24 1/1/1 VRF IoT-医療
D. IPルート 0.0.0.0/0 10.255.101.11 VRFサービス
IPルート 10.255.101.0/24 1/1/1 VRF IoT-医療
IPルート 10.1.100.0/24 10.255.101.11 VRF IoT-医療

正解: (正解を表示します)
目標は、ルータ1にスタティックルートを追加し、VLAN 10 サブネット10.2.10.0/24、オプションに基づいてVRF「IoT-Medical」内と想定）のクライアントがサブネット10.1.100.0/24内のサービスにアクセスできるようにすることです。図から、インターフェース1/1/1 （IPアドレス10.255.101.10/24）はVRF「service」内であり、宛先へのネクストホップとしてCore-1 （10.255.101.11）が考えられます （VRF「service」経由でも到達可能であることが示唆されています）。そのためには、送信元VRF（「IoT-Medical」）に、「service」VRF内のネクストホップを経由して宛先に向かうルートを追加する必要があります。
* 静的ルート構文 （VRF使用時）:ip route <destination_prefix> <next-hop-ip> [vrf <source-vrf>]
* オプションの分析:
* A: Core-1 は VRF 'サービス' 中ではないと主張していますが、これは考えられる設定と矛盾しています。
* B: 特殊な interface:ip 構文 （1/1/1:10.255.101.11）を使用します。VRF「IoT-Medical」にルートを定義します。
* C: インターフェース1/1/1をネクストホップとして使用します。これはIPアドレスを使用するよりも具体的ではなく、インターフェースがポイントツーポイントであるか、プロキシARPが有効になっていることを前提としています。VRFでルートを定義します。
「IoT-医療」。
* D: ip route 10.1.100.0/24 10.255.101.11 vrf IoT-Medical。これは、IoT-Medical VRFのコンテキスト内で、ネクストホップIPアドレス10.255.101.11を経由して宛先10.1.100.0/24へのスタティックルートを定義するための標準構文を使用しています。このルートが正常に機能するには、「IoT-Medical」VRFと「service」VRF間でVRF間ルーティング （ルートリーク）が設定されている必要がありますが、コマンド自体は必要なスタティックルートを正しく定義しています。
* 結論: オプション D は、指定されたソース VRF (「IoT-Medical」) 内で必要な静的ルートを設定するための正しい標準コマンド構文を提供します。
参考資料 :AOS-CX IPルーティングガイド （スタティックルート）、AOS-CX VRF構成ガイド （VRF間ルーティング）。これは 「ルーティング」（16%）と 「接続性」（9%）の目標に関連します。

質問: **60**
OSPFルータは、外部ネットワークへのパスをE1とE2の両方のアドバタイズメントでチーミングしています。どちらのルートも同じパスコストを持っています。ルータはどちらのパスを優先するでしょうか？
A. ルータはECMPを使用して両方のパスを均等に使用します。
B. ルータは E2 パスを優先します。
C. パスの競合が解決されるまで、両方のルートが抑制されます。
D. ルータは E1 パスを優先します。
正解: **D** (コメントを発表する)
問題は、OSPFルータが外部ネットワークへのE1（外部タイプ1）とE2（外部タイプ2）のアドバタイズメントを同じパスコストで受信した場合です。ルータがどちらのパスを優先するかを決定する

ことが課題です。
* オプションの分析:
* オプション A (ECMP): 等コスト マルチパス (ECMP) は、複数のパスの合計コストが同じであるが、E1 ルートと E2 ルートのメトリック計算が異なる場合に使用されます。そのため、ここでは ECMP は適用されません。
* オプション B (E2 を優先): 誤り。E2 ルートは、E1 ルートが存在しないか、総コストが高い場合にのみ優先されます。
* オプション C (抑制): OSPF はパスの競合によるルートを抑制せず、メトリックに基づいて最適なパスを選択します。
* オプション D (E1 を優先): 正解。OSPF は、E1 ルートには ASBR (自律システム境界ルータ) への内部コストと外部コストが含まれており、より正確な合計コストを提供するため、E2 ルートよりも E1 ルートを優先します。
* オプションDが正しい理由 :OSPFでは、外部ルートはE1またはE2としてアドバタイズされます。E1ルートには、ASBRによってアドバタイズされた外部コストとASBRに到達するための内部コストの両方が含まれるため、パス選択の精度が向上します。E2ルートは外部コストのみを考慮し、明示的にE1として設定されない限り、再配布ルートのデフォルトとなります。OSPFルータは、同じ外部コストを持つE1ルートとE2ルートの両方を受信した場合、内部ネットワークトポロジを含む総パスコストを考慮するため、E1ルートを優先します。これはOSPF標準（RFC 2328）に準拠しています。
* 認定目標との関連性:
* ルーティング (16%): 外部ルート タイプ (E1 と E2) を含む OSPF ルーティング トポロジの設計とトラブルシューティングが含まれます。
* トラブルシューティング (10%): ルーティングの問題を解決するための OSPF パス選択の分析が含まれます。
参考文献:
HPE Aruba Networking AOS-CX 構成ガイド: OSPF 構成、E1 および E2 ルート タイプの詳細。
HPE7-A06 学習ガイド: OSPF の外部ルート選択とパスの優先順位について説明します。
RFC 2328: OSPF バージョン 2、E1 および E2 ルート メトリックと優先順位について説明します。

質問: **61**
ネットワーク テクノロジーを顧客の要件に合わせて調整します。

正解:

Answer Area

Establish redundant links between the aggregation and core layers.	ECMP
Extend layer 2 across multiple sites.	VXLAN
Identify individual layer 2 segments in an overlay.	VNI
Minimize configuration steps to establish tunnels between sites.	EVPN

* アグリゲーション層とコア層の間に冗長リンクを確立：ネットワーク層（アグリゲーション層とコア層など）間でレイヤ3ルーティングを使用する場合、ECMP（等コストマルチパス）により、ルーティングプロトコル（OSPF、BGPなど）は、ルーティングコストが同じ複数のリンクを同時に利用できます。これにより、冗長性（1つのリンクに障害が発生した場合、トラフィックは他のリンクを使用する）とリンク間の負荷分散の両方が実現されます。
参考資料：AOS-CX IPルーティングガイド（OSPF、BGP、ECMP）。「ルーティング」（16%）、「ネットワークの回復力と仮想化」（8%）に関連します。
複数の拠点にまたがるレイヤー2の拡張：VXLAN（Virtual Extensible LAN）は、この目的のために特別に設計されたオーバーレイ技術です。レイヤー2イーサネットフレームをUDPパケット内にカプセル化し、基盤となるレイヤー3ネットワークインフラストラクチャを介してトンネリングすることで、物理的に離れた拠点間でレイヤー2ドメイン（VLAN）を効果的に拡張します。
参考資料:AOS-CX VXLAN ガイド。「スイッチング」(19%)、「接続性」(9%) に関連します。
オーバーレイ内の個々のレイヤー2セグメントを識別：VXLANヘッダー内では、VNI（VXLANネットワーク識別子）がセグメント識別子として機能します。各固有のレイヤー2セグメント（拡張されている特定のVLANなど）は、固有の24ビットVNIにマッピングされます。これにより、オーバーレイネットワークは、同じVTEP（VXLANトンネルエンドポイント）間でトンネリングされている場合でも、異なるレイヤー2ドメインに属するトラフィックを区別できます。
参考資料:AOS-CX VXLAN ガイド、RFC 7348 (VXLAN)。「スイッチング」(19%)、「接続性」(9%) に関連します。
サイト間のトンネル確立に必要な設定手順を最小限に抑えます。VXLANはデータプレーンのカプ

セル化を提供しますが、EVPN（イーサネットVPN）はVXLANオーバーレイの最新のコントロールプレーンとして機能します。MP-BGP拡張機能を使用することで、EVPNはVTEPを動的に検出し、MACアドレスとIP到達可能性情報をアドバタイズします。これにより、従来の静的VXLANやフラッディング＆ラーニング方式と比較して、設定の複雑さが大幅に軽減されます。VTEPのピア関係とエンドポイントの学習はコントロールプレーンによって自動化されるため、接続を確立するための手動手順が最小限に抑えられます。
参考資料:AOS-CX EVPN ガイド。「ルーティング」(16%)、「スイッチング」(19%)、「接続」(9%) に関連します。

質問: **62**
クライアントは、HPE Aruba Networking Central の HPE Aruba Networking Switch MultiEdit ソフトウェア機能を使用したいと考えています。
利用可能なオプションはどれですか?
A. CLI スクリプトを使用して、選択したスイッチに適用します。
B. 選択したスイッチに対して同じ NAE スクリプトを実行します。
C. テンプレートを使用し、選択したスイッチに適用します。
D. 選択したスイッチのインターフェース範囲に設定を適用します。
正解: (正解を表示します)
HPE Aruba Networking CentralのMultiEdit機能を使用すると、管理者はCLIスクリプトをプッシュし、選択したスイッチに一括適用できます。これにより、複数のデバイス間で一貫性のある設定変更を同時に行うことができる柔軟性が得られます。

質問: **63**
顧客は、次のスイッチ ポートを持つ CX 6300 VSF スタックの 2 つのルータとローカル AS 65000 を使用して eBGP ピアリングを設定しました。
[ルータ1 10.10.10.2に接続するポート]

LAGはサードパーティ製のL2スイッチに接続され、リモートeBGPルーターのトランジットネットワークとして使用されます。BGPピアリングの問題を最適化するため、AOS-CXスイッチはグローバル設定で構成されています。

```
bfd
    bfd min-receive-interval 2000
    bfd min-transmit-interval 2000
    bfd detect-multiplier 3
```

eBGP ピアとの双方向転送を有効にするには、AOS_CX スイッチで何を行う必要がありますか?

○
```
router bgp 65000
    address-family ipv4 unicast
        neighbor 10.10.10.2 fall-over bfd
        neighbor 10.10.20.2 fall-over bfd
```

○
```
router bgp 65000
        neighbor 10.10.10.2 fall-over bfd
        neighbor 10.10.20.2 fall-over bfd
```

○
```
int 1/1/1-1/1/2, 2/1/1-2/1/2
  fall-over-bfd
```

○
```
interface lag1-2
  fall-over bfd
```

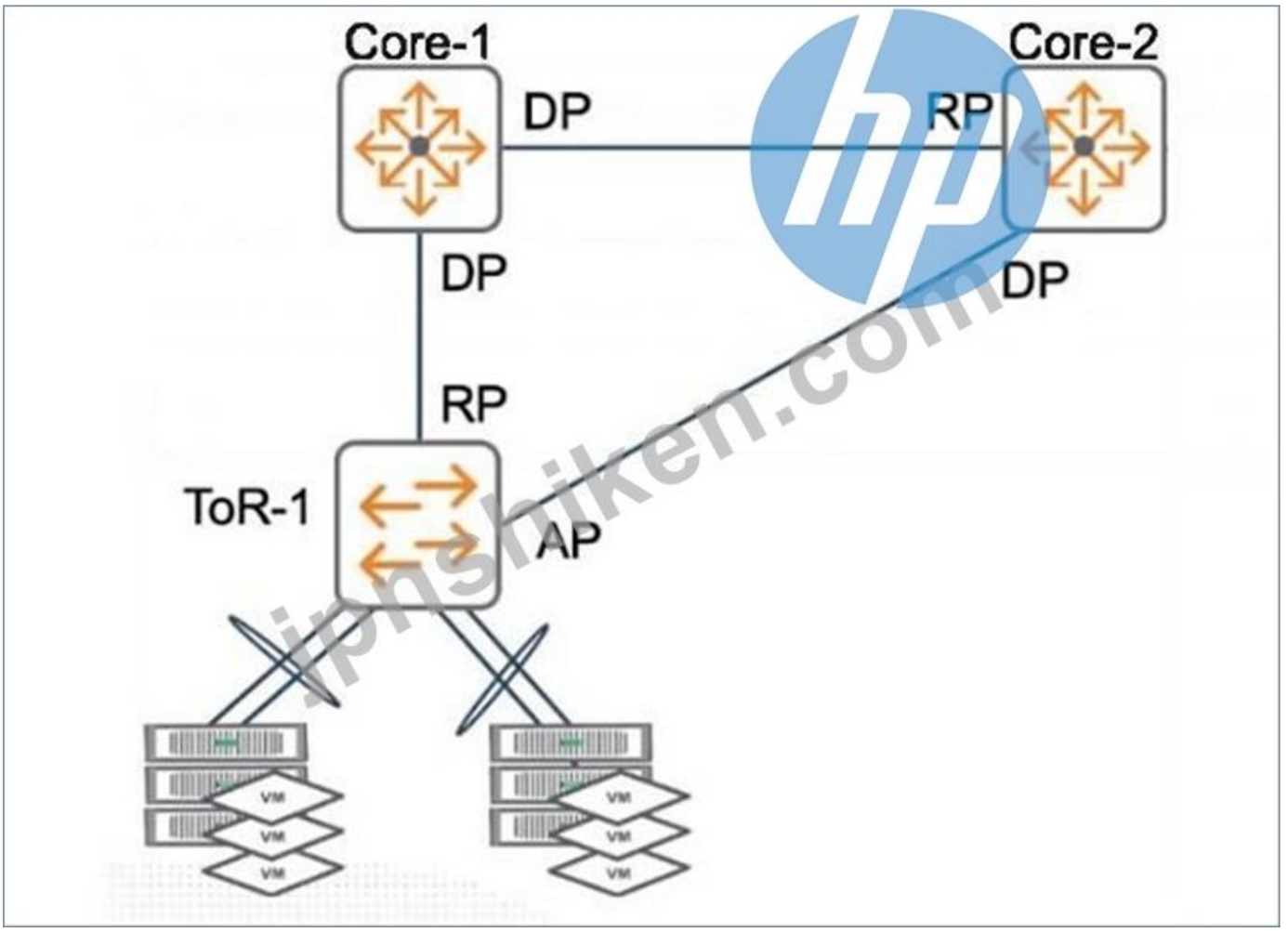
A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解: **B** (コメントを発表する)
目標は、eBGPネイバー10.10.10.2と
AOS-CX VSFスタック（AS 65000）上の10.10.20.2。グローバルBFD設定は既に設定済みです。BFD状態をBGPネイバー関係にリンクするには、特定のコマンドが必要です。
* BGP 構成の BFD: ルータの bgp <asn> 構成階層内の特定のネイバーに対して fall-over bfd パラメータを有効にする必要があります。
* オプションの分析（新しい画像）：
* オプション 1 (上):
ルータ BGP 65000
アドレスファミリ IPv4 ユニキャスト
ネイバー 10.10.10.2 フォールオーバー BFD
ネイバー 10.10.20.2 フォールオーバー BFD
これにより、両ネイバーの IPv4 ユニキャストアドレスファミリコンテキスト内で BFD が有効化されます。これは有効な設定箇所です。
* オプション2（2番目）:
ルータ BGP 65000
ネイバー 10.10.10.2 フォールオーバー BFD
ネイバー 10.10.20.2 フォールオーバー BFD
これにより、ルータ BGP 65000 内のメインの neighbor <ip> 設定行の直下で BFD が有効になります。通常、これにより、そのネイバー関係に設定されているすべてのアドレスファミリ（IPv4 ユニキャストを含む）に BFD が適用されます。これは、有効かつ一般的な設定箇所でもあります。
* オプション3（3番目）:
整数 1/1/1-1/1/2、2/1/1-2/1/2
転倒BFD
不正解です。インターフェース範囲コンテキストで BFD 設定を適用しますが、これは BFD が BGP セッションにリンクされる方法ではありません。
* オプション4（下）
インターフェースラグ1-2
フォールオーバーBFD
不正解です。インターフェース LAG 範囲コンテキストで BFD 設定を適用しますが、これは BFD が BGP セッションにリンクされる方法ではありません。
* 有効なオプションの比較 (1 と 2): オプション 1 とオプション 2 はどちらも、ルータ BGP で fall-over bfd コマンドを正しく使用しています。オプション 1 はアドレスファミリ単位の粒度を提供しますが、オプション 2 はネイバー全体にこれを適用します。IPv4 のみに BFD を有効にするという明確な要件がない場合は、ネイバー レベル (オプション 2) で適用する方が多くの場合、よりシンプルで十分です。どちらのオプションでも、必要な IPv4 ピアリングの目的を達成できま

す。多くのドキュメントの例では、AF 単位の制御が明示的に必要な場合を除き、ネイバー レベルでの設定が示されています。
* 結論: オプション1とオプション2はどちらも有効な設定方法です。ネイバー関係全体にBFDが必要な場合は、オプション2の方がやや一般的と言えるでしょう。
参考資料：AOS-CX BFDガイド、AOS-CX BGPガイド（ネイバーコマンド、フォールオーバーBFDオプション）。これは「ルーティング」（16%）と「ネットワークの回復力と仮想化」（8%）の目標に関連します。

質問: **64**
管理者は HPE Aruba Networking Central でサードパーティの WLAN 送信機を監視していますが、そのうちのいくつかは不正または不正の疑いがあると分類されています。
HPE Aruba Networking Central の「有線で検出」ルールのデフォルトの分類方法を使用する場合、不正はどのように分類されますか?
A. 有線ネットワークに接続されているか、WLAN 分類 = 「干渉」
B. 有線ネットワークに接続
C. 有線ネットワークに接続されており、WLAN 分類 = 「干渉」
D. 有線ネットワークに接続されており、WLAN 分類 = 「有線で検出」
正解: **(**正解を表示します**)**
HPE Aruba Networking Centralでは、デフォルトの分類方法を使用する場合、APが有線ネットワークに接続されていることが検出された場合、不正APとして分類されます。有線接続を経由せず無線接続のみで検出された場合は、不正APの疑いまたは干渉APとして分類される可能性がありますが、「有線接続で検出」はデフォルトで不正APとして分類されます。

質問: **65**
エンジニアが特定のHPEスイッチインターフェースのエラー率が高いことを発見しました。この問題の原因として最も可能性が高い2つのパラメータはどれですか？
A. VLANの設定ミス
B. ポート速度
C. デュプレックスの不一致
D. LACPモード
正解: **(**正解を表示します**)**

質問: **66**
展示品を参照してください。



Acme社では、ToR-1の下流でVMワークロードを実行しており、パフォーマンスの低下に気づいています。ToR-1のアップリンクが定期的に過剰に使用されているのではないかと疑っています。
パートナー企業から、既存の1U Core-1およびCore-2をCX 6400シリーズに移行することを提案されました。
HPE Aruba Networking のベストプラクティスの実装に重点を置きながら、このプラットフォームのどの側面が顧客の問題を解決しますか? (2 つ選択してください。)
A. MC-LAG により、Core-1 と Core-2 はエッジ 802.3ad デバイスを共通の 「システム ID」として提示できるようになります。
B. CX 6400 シリーズは、マルチリージョン設計に基づいて、ToR-1 からの複数のアクティブ転送経路をサポートします。
C. 提案されたソリューションのバックプレーン スタッキングにより、直接接続された ESXI ホストはアクティブ LACP を使用して負荷分散を行うことができます。
D. CX 6400 シリーズ シャーシのポート密度により、VM ハイパーバイザーをコアに直接接続できます。
E. 提案された新しいコアの VSF 機能により、STP の必要性を排除しながら、ToR-1 ベースからの複数のアクティブ転送経路が可能になります。
正解: **(正解を表示します)**
VSX/MC-LAGを搭載したCX 6400に移行すると、Core-1とCore-2はToR-1に対して単一のLACPパートナー（共通システムID）として認識されます。これにより、アクティブ/アクティブアップリ

ンクが実現し、両コア間でトラフィックが分散されるため、アップリンクの過剰使用が軽減されます。
マルチシャーシ/スタック コアを使用すると、ブロックされた STP リンクがなくなるため、ToR-1 には複数のアクティブな転送パスが確保され、使用率と回復力がさらに向上します。

質問: **67**
2台のCX 8325スイッチを、コアロールとしてVSXを使用し、アグリゲーションロールとしてVSFで2台のCX 6300Mを使用してクラスタ構成にしています。スイッチでマイナーソフトウェアアップグレードを実行する場合、アグリゲーションスイッチでヒットレスアップグレードを実現する方法は何ですか？
A. VSF アップデート ソフトウェアは、最初にセカンダリ スイッチでソフトウェア アップグレードを開始し、次にプライマリ スイッチでソフトウェア アップグレードを開始します。
B. ISSU アップデート ソフトウェアは、最初にセカンダリ スイッチでアップグレードを開始し、次にプライマリ スイッチでアップグレードを開始します。
C. VSF アップデート ソフトウェアは、最初にプライマリ スイッチでソフトウェア アップグレードを開始します。次にセカンダリ スイッチでソフトウェア アップグレードを開始します。
D. ISSU アップデート ソフトウェアは、最初にプライマリ スイッチでアップグレードを開始し、次にセカンダリ スイッチでアップグレードを開始します。
正解: **(正解を表示します)**
質問はCXのVSF（仮想スイッチングフレームワーク）スタックのマイナーソフトウェアアップグレードに関するものです。
6300Mスイッチをアグリゲーションロールに配置し、CX 8325スイッチをコアとしてVSXクラスタを構成します。アグリゲーションスイッチのヒットレスアップグレードを実現する方法を特定することが課題です。
* オプションの分析:
* オプション A: 正解です。VSF のアップグレードは、トラフィックの中断なしに継続的な運用を確保するために、セカンダリ スイッチから開始され、次にプライマリ スイッチが続きます。
* オプション B: 不正解です。インサービス ソフトウェア アップグレード (ISSU) は VSF ではなく VSX で使用され、異なるプロセスに従います。
* オプション C: 不正解です。VSF でプライマリ スイッチを最初にアップグレードすると、コントロール プレーンの動作が中断される可能性があります。
* オプション D: 不正解です。ISSU は VSF アップグレードには適用されません。
* オプションAが正しい理由 :VSFスタックでは、update-softwareコマンドは、プライマリ（マンダー）スイッチがトラフィック処理を継続できるように、セカンダリ（スタンバイ）スイッチからローリングアップグレードを開始します。セカンダリスイッチがアップグレードされてスタックに復帰すると、プライマリスイッチもアップグレードされ、ヒットレスな運用が維持されます。このプロセスは、アップグレード中にメンバースイッチをアクティブに保つVSFの機能を活用し、ダウンタイムを最小限に抑えます。CX 6300MのVSF実装は、HPE Aruba Networkingのドキュメントに記載されているように、このヒットレスアップグレードメカニズムをサポートしています。
* 認定目標との関連性:

* ネットワークの復元力と仮想化 (8%): 高可用性とヒットレス アップグレードのための VSF の設計とトラブルシューティング。
* トラブルシューティング (10%): キャンパス ネットワークでのソフトウェア アップグレード中の中断を最小限に抑えます。
参考文献:
HPE Aruba Networking AOS-CX 構成ガイド: VSF ソフトウェア アップグレード、ヒットレス アップグレードの手順の詳細。
HPE7-A06 学習ガイド: VSF のメンテナンスおよびアップグレード プロセスについて説明します。
HPE Aruba ネットワーク技術ドキュメント: CX 6300 シリーズ VSF アップグレードのベスト プラクティス。

質問: **68**
展示物を参照してください。

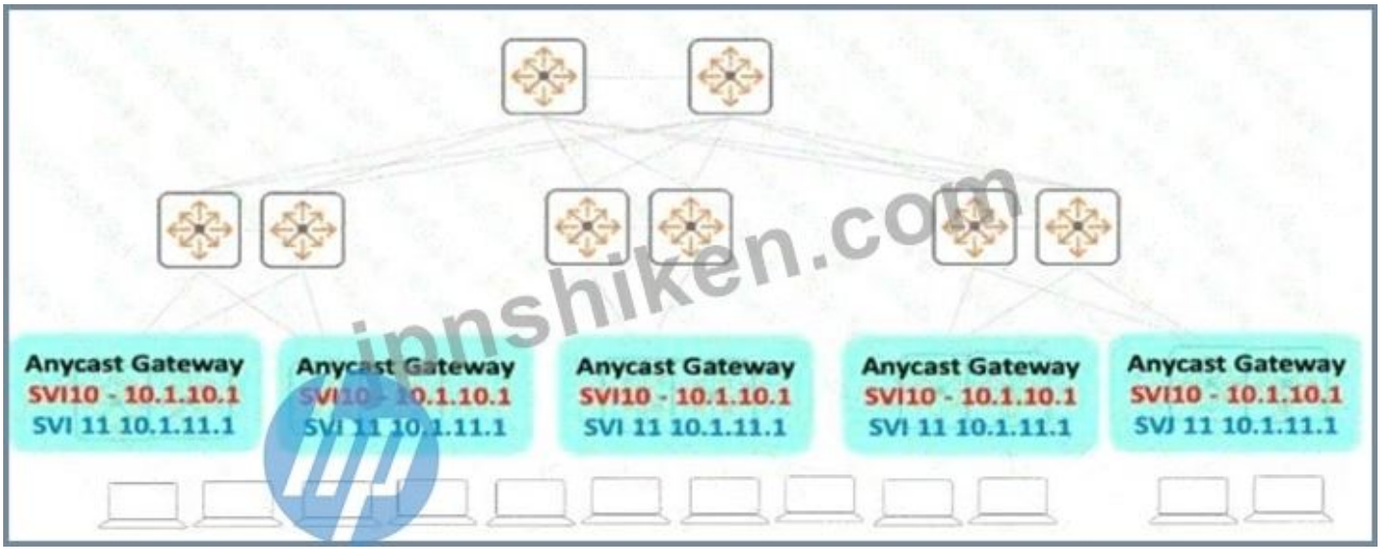
エンジニアは上記の設定を R1 と R2 に適用しましたが、ルーターの OSPF 隣接関係は EXSTART/DR」状態を超えて進みません。

```
R2(config)# show ip ospf neighbors
VRF : default                              Process : 1
==========================================

Total Number of Neighbors : 1

Neighbor ID      Priority  State          Nbr Address       Interface
-------------------------------------------------------------------------
10.255.1.0       1         EXSTART/DR     10.255.1.0        1/1/1
```

どちらのルータでどの設定操作を行うと、R1とR2が EXTART/DR」状態ですか?
A. インターフェース1/1/1に適用されたIPアドレスとマスクをRFCでサポートされている有効なマスクに変更します。

2328。
B. OSPF プロセスがパッシブ インターフェイスのデフォルトで設定されていないことを確認します。
C. L3 MTU 設定を削除します。
D. R1 と R2 をポイントツーポイントのネットワーク タイプに変更します。
正解: **(**正解を表示します**)**
/31リンクではデフォルトでブロードキャストネットワークタイプが使用されているため、OSPF隣接関係はEXSTART/DR状態のままです。/31ポイントツーポイントリンクでは、OSPFネイバーはDR/BDR選出を試みるべきではありません。R1またはR2のいずれかでOSPFネットワークタイプをポイントツーポイントに変更すると、隣接関係が正しく形成され、ルータがFULL状態に移行できるようになります。

質問: **69**
展示する。



分散エニーキャスト ゲートウェイを使用して分散オーバーレイを実装した後、アクセス (リーフ) スイッチごとに複製される ARP パケットが多すぎることに気付きました。ネットワークを最適化するために使用できるコマンドはどれですか。
A. VLAN 10 ARP抑制 VLAN 11 ARP抑制
B. evpn arp抑制
C. evpn ip proxy-arp
D. インターフェースVLAN 10 ip proxy-arp インターフェースVLAN 11 ip proxy-arp
正解: **B (**コメントを発表する**)**
EVPN VXLAN分散オーバーレイネットワークにおいて、すべてのリーフスイッチへの過剰なARPパケット複製（フラッディング）が観測されています。これを最適化するにはコマンドが必要です。
* EVPN ARP最適化：EVPNは、コントロールプレーン（BGP）を使用してMACアドレスとIPアドレスの到達可能性情報を配布します。リーフスイッチ（VTEP）はこれらのマッピングを学習します。VXLANファブリック全体のARPフラッディングを軽減するには、以下の手順を実行します。
* ARP抑制：VTEPはARP要求を傍受します。VTEPが要求されたIPのMACアドレス（EVPN経由で

学習）を既に知っている場合、ARP要求を抑制し、VXLAN経由でARP要求がフラッディングされるのを防ぎます。
* プロキシARP :VTEPはARP要求を傍受します。VTEPが要求されたIPのMACアドレスを知っている場合、リモートホストに代わってARP応答を生成できます。
* AOS-CX コマンド:これらの機能は、EVPN コンテキスト内で設定されます。
* evpn arp-suppression (B): EVPN の ARP 抑制機能を有効にします。
* evpn ip proxy-arp (C): EVPN のプロキシ ARP 機能を有効にします。
* オプション A と D は、標準のインターフェイス/VLAN レベルの arp-suppression または proxy-arp コマンドを使用します。これらは、EVPN VXLAN ファブリック自体内のフラッディングの最適化に固有のものではありません。
* 結論 :EVPN VXLANオーバーレイ全体でARPパケットの複製/フラッディングを削減して最適化するには、evpn arp-suppression オプションB）を直接有効にするコマンドを使用します。これにより、EVPNコントロールプレーンの知識を活用し、不要なARPフラッディングを阻止できます。
参考資料 :AOS-CX EVPN構成ガイド ARP抑制、プロキシARP機能）。これは以下の内容に関連します。
オーバーレイのコンテキストにおける 「スイッチング」（19%）および 「ルーティング」（16%）の目標。

質問: **70**
OSPF を使用して、同じエリア (エリア 0) 内のネイバーに、以下の SVIs の .\16 サマリー ルートのみをアドバタイズします。
どのような構成でこれを実現できるでしょうか?

A.
```
router ospf 1
    redistribute connected
    area 0 range 10.1.0.0/16
```

B.
```
interface vlan 11
    ip ospf 1 area 0
!
interface vlan 12
    ip ospf 1 area 0
!
interface vlan 13
    ip ospf 1 area 0
!
router ospf 1
    summary-address 10.1.0.0/16
```

C.
```
router ospf 1
    redistribute connected
    summary-address 10.1.0.0/16
```

D.
```
router ospf 1
    redistribute connected
    summary-address 10.1.0.0/16
```

E.

正解: (正解を表示します)

目標は、ルータ上で OSPF を設定し、特定の SVI (VLAN 11、12、13、10.1.xx の範囲内にあると想定) の 10.1.0.0/16 サマリー ルートのみを同じエリア (エリア 0) 内の OSPF ネイバーにアドバタイズすることです。

* OSPFエリア内動作 :OSPF（リンクステートプロトコル）の基本原則は、同一エリア内のすべてのルータがそのエリアについて同一のリンクステートデータベース（LSDB）を持つ必要があるということです。これは、すべてのルータがエリア内のすべての特定ネットワーク（タイプ1ルータLSA、タイプ2ネットワークLSA）について学習することを意味します。OSPFv2は、特定ネットワークLSAを同一エリア内の他のルータから隠蔽するようなルート集約をサポートしていません。集約はエリア境界でのみ行われます（タイプ1ルータLSAを使用するABRによって）。

3 つのサマリー LSA（area range コマンド経由）または外部ルート（summary-address コマンド経由のタイプ 5 外部 LSA を使用する ASBR によって）を OSPF に再配布します。

* オプションの分析:

* A) area 0 range 10.1.0.0/16 :このコマンドは、エリア境界ルータ（ABR）上で、エリア0から発信されたルートを別のエリア（例バックボーン）にアドバタイズする際に、それらのルートを集約するために使用されます。エリア0内のLSAフラッディングには影響しません。また、redistribute connectedコマンドも含まれますが、これはここでは関係ありません。

* B) summary-address 10.1.0.0/16: このコマンドは、自律システム境界ルータ（ASBR）上で、OSPFに再配布される外部ルートを集約するために使用されます。OSPFエリア内で定義されたSVIなどの内部OSPFルートの集約には使用されません。

* C) および D) summary-address 10.1.0.0/16: B と同じ問題。内部 OSPF ルートを要約するためのコマンドが正しくありません。

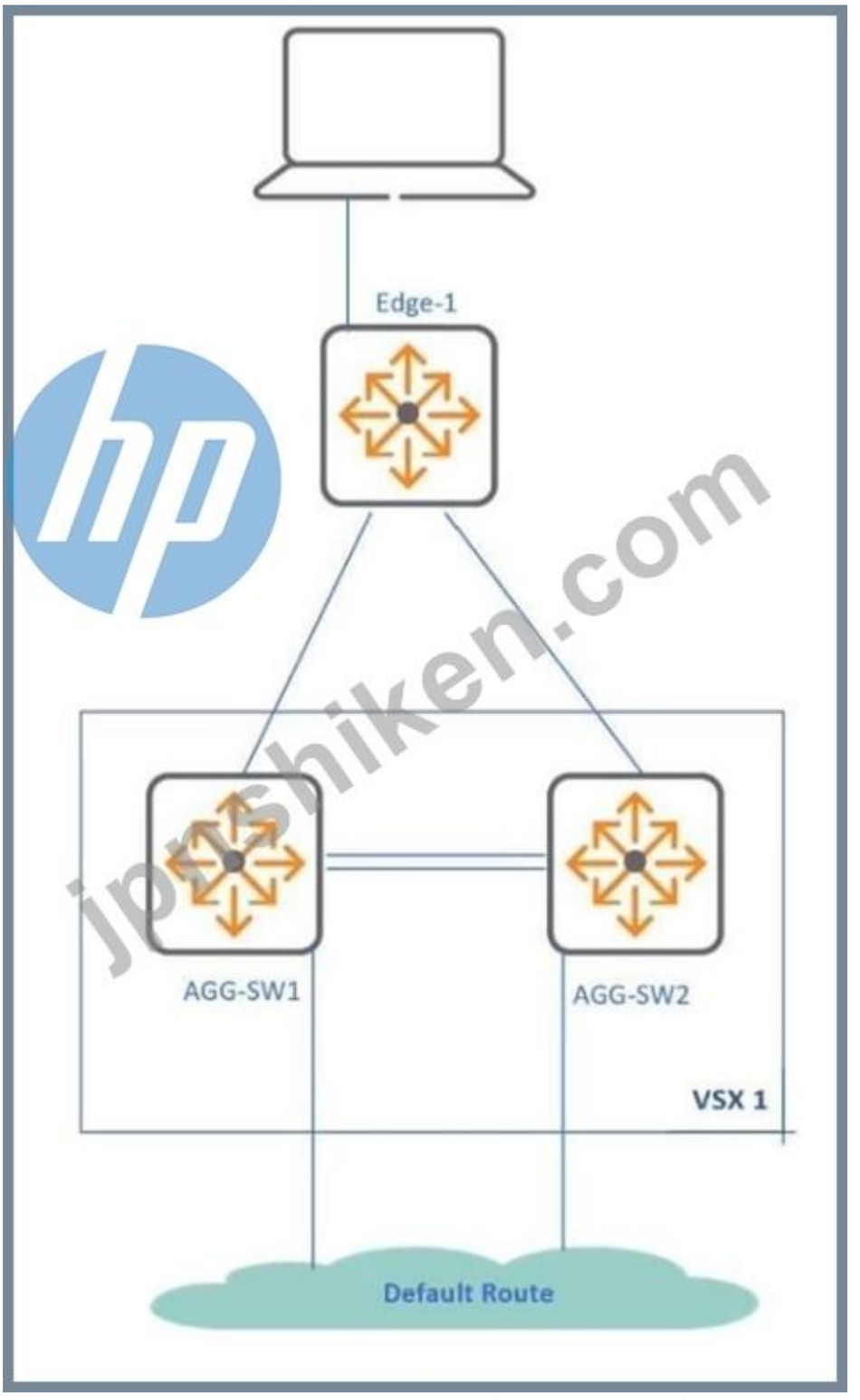
* E) area 0 range 10.1.0.0/16: Aと同様に、area rangeコマンドを使用します。OSPFエリア0に設定されているSVIが最初に正しく表示されます。ただし、Aと同様に、このコマンドはABR上でエリア間集約を実行し、エリア0内の特定のLSAを抑制しません。

* 結論 :この質問は、OSPFv2では不可能なこと、つまり、同一エリア内では集約ルートのみをアドバタイズし、詳細ルートは抑制することを求めています。したがって、どの設定でも、述べられている結果を正確に達成することはできません。しかし、質問に誤りがあり、OSPF内部ルート（エリア間でのみ有効であっても）を集約するための適切なコマンド構造を持つ設定を尋ねているのであれば、area rangeコマンドが適切です。AとEの両方でこのコマンドが使用されています。オプションEは、インターフェースが最初にOSPFエリア0に追加されることを示しているため、やや構造が優れています。具体的な要求が不可能であるにもかかわらず、これが意図された方向である

と仮定すると、与えられたオプションの中でEが最も妥当な選択肢です。
参考資料：RFC 2328 (OSPFv2)、AOS-CX 向け OSPF 構成ガイド（ABR のエリア範囲と ASBR のサマリーアドレスの説明）。これは「ルーティング」（16%）の目標に関連します。

質問: **71**
Python 開発者は、REST API を介して AOS-CX スイッチ上の VLAN データベースを読み取ることはできましたが、変更することはできませんでした。
開発者はどの設定を最初に確認する必要がありますか? (2 つ選択してください。)
A. HTTPS設定
B. SNMP設定
C. SSH設定
D. クッキー設定
E. REST API設定
正解: **(**正解を表示します**)**
HTTPS設定 → AOS-CX REST APIはHTTPS経由で実行されるため必須です。HTTPSが有効になっていない場合、書き込み操作は失敗します。
REST API 設定 → REST API 書き込みモード (読み取り/書き込み vs. 非公開) がオンになっていることを確認するためにチェックする必要があります。
読み取り専用が有効になっています。

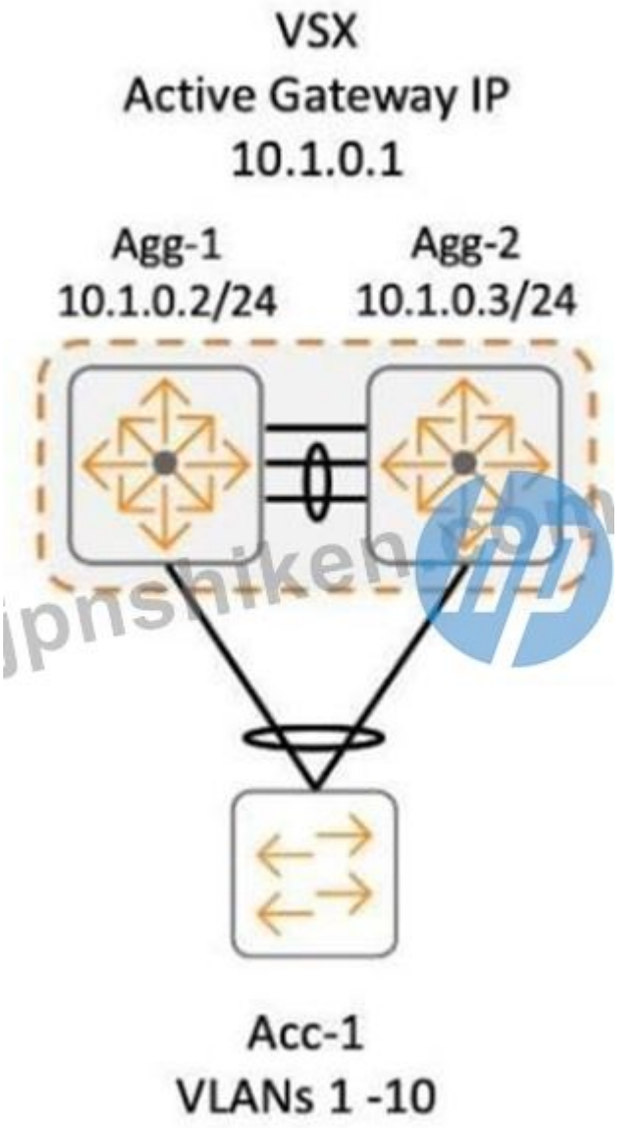
質問: **72**
展示品を参照してください。



CX 8325 VSX 構成の初期セットアップ後、アクティブ ゲートウェイが SVI 10 用に設定されます。テスト目的で、Edge-1 に接続されたクライアントからのトラフィックがデフォルト ルートに向けて開始されている間、sw-agg1 上の SVI 10 はシャットダウンされます。
このテストを実行する際に予想される動作は何ですか?
A. クライアントと宛先の間でトラフィックがドロップされる可能性があります。
B. トラフィックは、パケットがドロップされるリスクなしに ISL 経由で転送されます。
C. トラフィックは影響を受けず、agg-sw2 がトラフィック転送を開始するまでに 50ns のフェイルオーバー時間が予想されます。

D. トラフィックがドロップされ、vsx-sync は agg-sw2 上の SVI10 を自動的に無効にします。
正解: **(**正解を表示します**)**
agg-sw1（VSXアクティブゲートウェイ）のSVI 10がシャットダウンされると、デフォルトゲートウェイ宛てのトラフィックはそのSVIを使用できなくなります。「VSXアクティブフォワーディング」が有効になっていない限り、もう一方のVSXピア（agg-sw2）はそのSVIへのトラフィック転送を開始しないため、パケットがドロップされる可能性があります。
アクティブ転送を有効にするか、SVI ゲートウェイの冗長機能を使用しない限り、デフォルトのフェールオーバーはシームレスではありません。

質問: **73**
展示品を参照してください。



両方のVSXスイッチでIGMP v3が有効になっています。Acc-1スイッチに接続されたクライアントのIGMPクエリアとなるのはどのスイッチですか？
A. アグ2
B. Agg-1とAgg-2の両方
C. アグ−1

D. アクティブゲートウェイ IP が IGMP クエリーとして使用されます。
正解: **(**正解を表示します**)**
IGMPv3対応VLANでは、参加ルータの中で最も小さいIPアドレスに基づいてIGMPクエリアが選出されます。このトポロジでは、次のようになります。
Agg-1は10.1.0.2/24です
■
Agg-2は10.1.0.3/24です
■
アクティブゲートウェイIP（10.1.0.1）は、エンドホストのデフォルトゲートウェイの冗長性のためだけに使用され、
■
IGMP クエリの選択。
10.1.0.2 < 10.1.0.3 なので、Agg-1 が IGMP クエリーになります。