HP.HPE7-A01.v2026-07-14.q100

試験コード:	HPE7-A01
試験名称:	Aruba Certified Campus Access Professional Exam
認定資格:	HP
無料問題数:	100
バージョン:	v2026-07-14
アクセス数:	142
ページビュー数:	1000
https://www.jpnpdf.com/HP.HPE7-A01.v2026-07-14.q100-mondaishu.html	

最新問題: **1**
OSPFトランジットネットワークとは何ですか？
A. トンネルを使って2つのエリアを接続するネットワーク
B. 2つの異なるエリアを接続する特別なネットワーク
C. ルーターが少なくとも1つのネイバーを検出したネットワーク
D. 異なるルーティングプロトコルに接続するネットワーク
Answer: A (メーッセージを残す)

OSPF トランジット ネットワークは、マルチ アクセス リンクで接続され、他のネットワークのトラフィックを転送できるルーターが 2 台以上あるネットワークです 1。トランジット ネットワークは、ルーターが 1 台しか接続されておらず、他のネットワークのトラフィックを転送しないスタブ ネットワークとは異なります 2。トランジット ネットワークは、物理的に隣接していない 2 つのエリア間の論理的な接続である仮想リンクとも異なります 2。トランジット ネットワークは、ルーターが再配布を実行する場合を除いて、必ずしも別のルーティング プロトコルに接続されているとは限りません 2。したがって、正解は C です。ルーターが少なくとも 1 つのネイバーを検出するネットワーク。

最新問題: **2**
管理者は、帯域幅制限を超過した有線ゲストユーザーが切断されていないことに気づきます。ClearPass の Access Tracker では、切断 CoA メッセージが AOS-CX スイッチに送信されていることが示されています。
管理者が以下の設定を実行しました

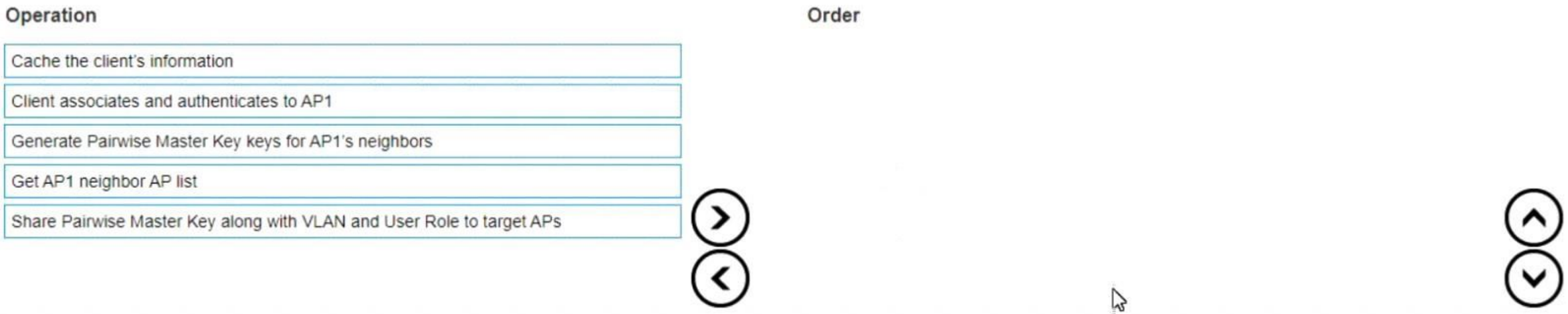
```
Access1(config)# ip dns host cppm.arubatraining.com 10.254.1.23 vrf mgmt
Access1(config)# radius-server host cppm.arubatraining.com key plaintext aruba123 vrf mgmt
Access1(config)# aaa group server radius cppm
Access1(config-sg)# server cppm.arubatraining.com vrf mgmt
Access1(config-sg)# exit
Access1(config)# aaa accounting port-access start-stop interim 5 group cppm
Access1(config)# radius dyn-authorization client cppm.arubatraining.com secret-key plaintext aruba123 vrf mgmt
Access1(config)# radius dyn-authorization enable
```

この問題の最も可能性の高い原因は何ですか？
A. スイッチで認証変更がグローバルに有効になっていません
B. CPPM の SSL 証明書がスイッチの信頼ポイントとして追加されていません
C. スイッチ上のRADIUSシークレットとCPPMに不一致があります。
D. スイッチとClearPass Policy Managerの間には時間差があります

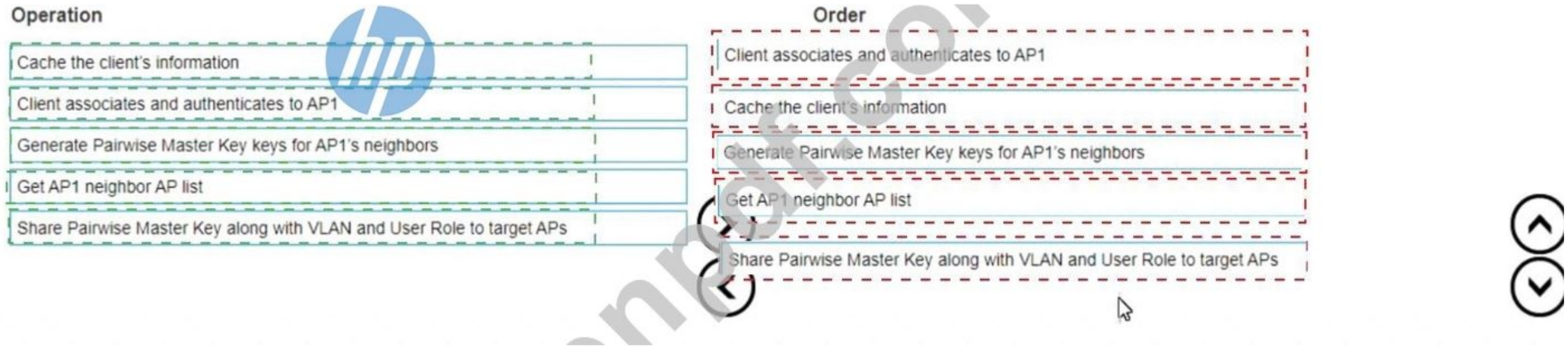
Answer: A (メッセージを残す)
認証変更（CoA）は、ClearPass Policy Manager（CPPM）がスイッチなどのネットワーク機器にメッセージを送信して、ユーザーセッションの認証状態を変更できるようにする機能です。CoAを使用するには、CPPMとネットワーク機器の両方がこの機能をサポートし、有効になっている必要があります。AOS-CXスイッチの場合、CoAはradius-server coa enableコマンドを使用してグローバルに有効にする必要があります。スイッチでCoAが有効になっていない場合、CPPMからの切断CoAメッセージは無視され、ユーザーセッションは終了しません。

最新問題: **3**
ポート1/45と2/45の間で、VSXペアのインタースイッチリンク256間に新しいVLAN 100を許可するにはどうすればよいですか？
A. ポート1/45および1/46に対してVLANトランク100を許可します
B. vlan trunk add 100 in LAG256
C. LAG256 で VLAN トランク 100 を許可
D. vlan trunk add 100 in MLAG256
Answer: C (メッセージを残す)
ポート1/45と2/45のVSXペア間インタースイッチリンク256で新しいVLAN 100を許可するには、LAG256でvlan trunk allowed 100コマンドを使用する必要があります。これにより、VSXピア間のインタースイッチリンクの一部であるトランクポートLAG256の許可VLANリストにVLAN 100が追加されます。他のオプションは、正しいコマンドを使用していないか、正しいポートまたはVLANを指定していないため、正しくありません。参照：
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html

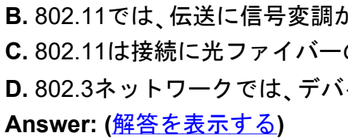
最新問題: **4**
AP1からAP2へローミングするワイヤレスクライアントのキー管理サービスにおける処理順序はどうなりますか？



Answer:



説明



https://www.arubanetworks.com/techdocs/Instant_85_WebHelp/Content/instant-ug/wlan-ssid-conf/conf-fast-roa

最新問題**: 5**

どのAruba APモードが、キャプチャしたRFデータをウォーターフォールプロットのためにAruba Centralに送信していますか？

A. エアモニター

B. デュアルモード

C. ハイブリッドモード

D. スペクトラムモニター

Answer: (解答を表示する**)**

スペクトラムモニターは、キャプチャしたRFデータをAruba Centralに送信してウォーターフォールプロットを作成するAruba APモードです。スペクトラムモニターモードでは、APは2.4GHz帯と5GHz帯の両方で全てのチャネルをスキャンし、干渉源、ノイズフロア、チャネル使用率などのRF環境に関する情報を収集できます。APはこのデータをAruba Centralに送信します。Aruba Centralはクラウドベースのネットワーク管理プラットフォームで、ウォーターフォールプロットを含む様々な形式でデータを表示できます。ウォーターフォールプロットは、RF信号の周波数、振幅、および持続時間を示す、時間経過に伴うRFスペクトルのグラフ表示です。その他のオプションは、APモードではないか、RFデータをAruba Centralに送信していないため、正しくありません。参考資料: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/spectrum_monitor.htm https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/waterfall_plot.htm https://www.arubanetworks.com/products/network-management-operations/aruba-central/

最新問題**: 6**

802.11無線LANと802.3イーサネットの主な違いは何ですか？ 2つ選択してください。）

A. 802.3は、有線メディアを介したデバイス間の直接通信を可能にします。

B. 802.11では、伝送に信号変調が必要です。

C. 802.11は接続に光ファイバーのみを使用する

D. 802.3ネットワークでは、デバイス接続のためにアクセスポイントが必要です。

Answer: (解答を表示する**)**

最新問題**: 7**
入力ポートまたはArubaOS-CXスイッチで、過剰なブロードキャストトラフィックを遮断する必要があります。
この作業に最適な機能は何ですか？
A. DWRRキューイング
B. 厳密なキューイング
C. 律速段階
D. QoSシェーピング
Answer: C (メーッセージを残す**)**
Arubaのドキュメントポータル1によると、ArubaOS-CXスイッチは、レート制限、QoSシェーピング、アクセス制御など、特定のポートへの受信トラフィックを制御するためのさまざまな機能をサポートしています。これらの機能は、過剰なブロードキャストトラフィックがネットワークのパフォーマンスと可用性に与える影響を軽減するのに役立ちます。
これは、レート制限とは、ポート容量の一定割合または1秒あたりの固定バイト数に基づいて、ポートの受信または送信トラフィックを制限できる機能であるためです。レート制限は、ポートに出入りするブロードキャストパケットの量を減らすことで、ブロードキャストストームを防ぐのに役立ちます。
https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-access-control.htm 2:
https://community.arubanetworks.com/blogs/esupport1/2021/02/08/broadcast-storm-containment-in-aruba-pvos-
https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8160_ssw_mcg/content/ch0

最新問題**: 8**
あなたは、社内の小規模拠点向けに標準化されたネットワーク設計に使用する構成をCentralで構築しています。ゲートウェイとアクセスポイントにはGUI構成を、スイッチにはテンプレート構成を使用したいと考えています。Arubaのベストプラクティスに準拠する必要があります。
これらの要件を満たす行動の組み合わせはどれですか？
A. Central にスイッチ用のグループを 1 つ、AP 用のグループを 2 つ、ゲートウェイ用のグループを 3 つ作成します。各ロケーションごとに固有のサイトを作成し、デバイスを適切なサイトに割り当てます。
B. セントラルでスイッチ用のグループを1つ、APとゲートウェイ用のグループをもう1つ作成します。各拠点ごとに固有のサイトを作成し、デバイスを適切なサイトに割り当てます。
C. Centralで単一のグループを作成します。各拠点ごとに固有のサイトを作成し、デバイスを適切なサイトに割り当てます。
D. Centralで単一のグループを作成します。デバイスの種類ごとに固有のサイトを作成し、デバイスを適切なサイトに割り当てます。
Answer: (解答を表示する**)**
これは、オプションCで、デバイスタイプごとに異なる設定方法が定義された単一のグループをCentralで作成する方法が示されているためです。たとえば、「Group」という名前のグループを作成し、そのグループ内で、スイッチにはテンプレートベースの設定方法、Instant APとゲートウェイにはUIベースの設定方法を有効にすることができます。Aruba Centralは、これら2つのグループを「Group」という単一の名前で識別します。グループ内のデバイスタイプがテンプレートベースの設定方法用にマークされている場合、グループ名には「TG」（TG Group）という接頭辞が付きます。「Group」は、ユーザー管理、監視、レポート、監査証跡などのワークフローのグループIDとして使用できます。

最新問題**: 9**
あなたは研究室で以下の機器仕様を用いて試験を実施しています。
* AP1は10 dBmの信号を生成する無線機を搭載しています。
* AP2は11dBmの信号を生成する無線機を搭載しています。
* AP1は9 dBiのゲインを持つアンテナを搭載しています。
* AP2は12dBiのゲインを持つアンテナを搭載しています。
* AP1のアンテナケーブルは2dBの損失があります
* AP2のアンテナケーブルは3dBの損失があります
APTの等価等方放射電力（EIRP）はどのくらいになるでしょうか？

A. 26 dBm
B. 30 dBm
C. 17 dBm
D. -12 dBm
Answer: C (メーッセージを残す**)**
AP1の等価等方放射電力（EIRP）は17 dBmと算出された。
EIRPは、アンテナが特定の方向に放射する電力の測定値です。これは、アンテナへの入力電力にアンテナの利得を乗じた値に等しくなります。また、伝送線路、コネクタ、その他の部品における損失も考慮に入れることができます。EIRPの計算式は次のとおりです。
EIRP = P + G - L
ここで、Pは無線機の出力電力、Gはアンテナの利得、Lはケーブルとコネクタの損失である。
AP1については、以下のとおりです。
P = 10 dBm、G = 9 dBi、L = 2 dB
したがって、
EIRP = 10 + 9 - 2 EIRP = 17dBm

最新問題**: 10**
あなたは研究室で、以下の機器仕様を用いて実験を行っています。
* AP1は20dBmの信号を生成する無線機を搭載しています。
* AP2は8dBmの信号を生成する無線機を搭載しています。
* AP1は7dBiのゲインを持つアンテナを搭載しています。
* AP2は12dBIのゲインを持つアンテナを搭載しています。
* AP1のアンテナケーブルは3dBの損失があります
* AP2のアンテナケーブルは3 OBの損失があります。
AP1の等価等方放射電力（EIRP）はどのくらいになるでしょうか？
A. 22 dBm
B. 24 dBm
C. 2dBm
D. 8 dBm
Answer: B (メーッセージを残す**)**

最新問題**: 11**
Aruba CX 6400スイッチにおいて、仮想出力キューイング（VOQ）は、一般的なキャンパススイッチと比べてどのような点で異なっているのでしょうか？
A. 大きな入力パケットバッファ
B. 大容量出力パケットバッファ
C. ポートごとのASIC
D. VSX
Answer: (解答を表示する**)**
Aruba CX 6400スイッチは、キャンパスネットワークやデータセンターネットワーク向けに、高性能かつ高密度なイーサネットスイッチングをサポートするモジュラースイッチです。Aruba CX 6400スイッチを一般的なキャンパススイッチと区別する特徴の一つは、仮想出力キューイング（VOQ）です。

VOQは、各ポートに大きな入力パケットバッファを実装することで、ヘッドオブラインブロッキングや輻輳によるパケット損失を防ぐ技術です。VOQでは、各ポートが異なる出力ポート用に複数のキューを持つことができ、宛先とQoSクラスに基づいてパケットの優先順位付けを行うことができます。VOQにより、Aruba CX 6400スイッチは、さまざまなトラフィックタイプとシナリオにおいて、高いスループットと低いレイテンシを実現できます。

最新問題: **12**
顧客はアクセス用にスタックされた Aruba CX 6200 および CX 6300 スイッチを使用しており、認証には VSX ペアの Aruba CX 8325 をコアとして使用しています。802 1X が実装されています。ケーブル配線が不足しているため、管理されていないスイッチがまだ使用されています。これらのスイッチの背後にあるデバイスがネットワーク障害を引き起こすことがあります。スイッチは、問題が発生したときにヘルプデスクに警告を送信する必要があります。この問題に対する効果的な解決策を実装するように依頼されました。
これに対する解決策は何ですか？
A. Aruba CX 8325 スイッチでスパニングツリーを設定します。trap-option を設定します。
B. Aruba CX 6200およびCX 6300スイッチのすべてのエッジポートでループ保護を設定します。トラップオプションは不要です。
C. Aruba CX 6200 および CX 6300 スイッチのすべてのエッジ ポートでループ保護を設定します。trap-option を設定します。
D. Aruba CX 6200およびCX 6300スイッチでスパニングツリーを設定します。トラップオプションは不要です。
Answer: (解答を表示する**)**
これは、管理対象外スイッチの背後にあるデバイスがループによってネットワーク障害を引き起こすという問題に対する正しい解決策です。ループ保護は、ループ保護が有効になっている各ポート、LAG、またはVLANにループ保護パケットを送信することで、Aruba CXスイッチがループを検出して防止できるようにする機能です。ループ保護パケットを送信したスイッチが受信した場合、ループが存在することが示され、設定に基づいてアクションが実行されます。ループ保護は、エンドデバイスまたは管理対象外スイッチに接続するポートである、Aruba CX 6200およびCX 6300スイッチのすべてのエッジポートで設定する必要があります。ループが検出されたときにヘルプデスクに警告を送信するように、trap-optionを設定する必要があります。他のオプションは、ループ保護を設定していないか、trap-optionを設定していないため、正しくありません。
参考文献：
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-99A8B276-0DA3-4458-AF
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-85

最新問題: **13**
Aruba NAEエージェントに関する記述のうち、正しいものはどれですか？ 2つ選択してください）
A. 1つのNAEスクリプトを複数のNAEエージェントで使用できます。
B. NAEエージェントは常に活動している
C. NAEエージェントはスイッチプロセッサリソースの10%以上を消費することはありません
D. NAEスクリプトは使用前にArubaによるレビューと署名を受ける必要があります。
E. 1 つの NAE エージェントを複数の NAE スクリプトで使用できます。
Answer: A,E (メーッセージを残す**)**
A) 1つのNAEスクリプトを複数のNAEエージェントで使用できます。
これは、NAEスクリプトがネットワーク内の異なるエージェント間で再利用できるように設計されているためです。
E) 1つのNAEエージェントを複数のNAEスクリプトで使用できます。
これは、個々のNAEエージェントが複数のスクリプトを実行して、ネットワークのさまざまな側面を監視および分析できるという点にも当てはまります。

最新問題: **14**
顧客は、以下の要件を満たすすべてのIoTデバイス向けの無線認証ソリューションを探しています。
IoTデバイスとアクセスポイント間の無線通信は暗号化する必要がある。
- デバイスごとに固有のパスフレーズ

- 指紋情報を使用してロールベースのアクセスを実行します
顧客の要望を満たすソリューションはどれですか？ 2つ選択してください。）
A. MPSKと内部RADIUSサーバー
B. MAC認証付きMPSKローカル
C. ClearPass Policy Manager
D. MPSKローカル（EAP-TLS対応）
E. ローカルユーザー派生ルール
Answer: A,C (メーッセージを残す**)**
説明
MPSKは、WPA2 PSKベースの展開において、デバイス固有またはグループ固有のパスフレーズを可能にする機能です。パスフレーズは、ClearPass Policy ManagerなどのRADIUSサーバーによって生成され、アクセスポイント（AP）に送信されます。IoTデバイスとAP間の無線トラフィックは、これらのパスフレーズを使用して暗号化されます。パスフレーズは、異なるVLANやユーザーロールにマッピングすることで、ロールベースのアクセス制御にも使用できます。
12. ClearPass Policy Managerは、MACアドレス、DHCPオプション、HTTPユーザーエージェントなどのさまざまな属性に基づいてIoTデバイスのデバイスフィンガープリンティングとプロファイリングを提供するネットワークアクセス制御ソリューションです。ClearPass Policy Managerは、他のIoTプラットフォームやサービスと統合して、IoTデバイスの可視性とセキュリティを強化することもできます。参考文献 :1
https://www.arubanetworks.com/techdocs/central/latest/content/aos10x/cfg/aps/wpa2_mpsk.htm 2
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/139640/wireless-client-mac-authentication-and-
3 https://www.arubanetworks.com/assets/ds/DS_ClearPass.pdf
https://www.arubanetworks.com/assets/tg/TB_ClearPass_IoT.pdf

最新問題**: 15**
Aruba CX VSXペアを設定する際、作成される設定において、スイッチ間リンクプロトコルの設定ではどの情報が使用されますか？
A. QSVI
B. MACテーブル
C. UDLD
D. RPVST+
Answer: B (メーッセージを残す**)**
Inter-Switch Link Protocol の設定で作成される設定で使用される情報は、B. MAC テーブルです。
インタースイッチリンクプロトコル（ISL）は、2台のVSXピアスイッチ間でデータと状態情報を同期させるためのプロトコルです。ISLはバージョン管理メカニズムを使用し、VSX同期機能に関して下位互換性を提供します。ISLは長距離（トランシーバーに依存）に対応し、10G、25G、40G、100Gなどの様々な速度をサポートします。
ISLが同期するデータコンポーネントの1つにMACテーブルがあります。これは、スイッチに接続されているデバイスのMACアドレスと、対応するポートまたはVLANを格納するデータベースです。ISLは、両方のVSXピアが同じMACテーブルエントリを持ち、トラフィックを正しい宛先に転送できるようにします。ISLは、ARPテーブル、VSX LAGのLACPステート、MSTPステートなどの他のデータコンポーネントも同期します。

最新問題**: 16**
顧客は、すべてのCXスイッチで有線認証を有効にしたいと考えています。要件の1つは、スイッチがVoIP電話を介して接続された単一のコンピュータを認証できることです。
この要件を満たすには、どの機能を有効にする必要がありますか？
A. マルチドメイン認証
B. デバイスベースモード
C. MAC認証
D. マルチ認証モード
Answer: (解答を表示する**)**

マルチドメイン認証は、スイッチが VoIP 電話を介して接続された単一のコンピュータを認証できる必要があるという要件をサポートするために有効にする必要がある機能です。マルチドメイン認証は、Aruba CX スイッチが同じポートに接続された異なるデバイスに異なる認証方法とポリシーを適用できるようにする機能です。たとえば、VoIP 電話とコンピュータを 1 つのケーブルを使用して同じポートに接続できますが、異なる資格情報を使用して個別に認証し、異なる VLAN に割り当てることができます。他のオプションは、同じポート上の複数のデバイスをサポートしていないか、認証を提供していないため、正しくありません。参照: https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-7D9E9F6E-5C2A-4F7E-BE6D-A2C3A6C7B9F9.html https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

最新問題: **17**
BSS着色の主な利点は何ですか？
A. BSSカラータグは、同じチャネル上のクライアントがエアタイムを共有できるようにすることでパフォーマンスを向上させます。
B. BSSカラータグはクライアントデバイスに適用され、干渉の閾値を下げることができます。
C. BSSカラータグはWi-Fiチャネルに適用され、干渉の閾値を下げることができます。
D. BSSカラータグは、不正なAPを識別してネットワークから排除することでセキュリティを向上させます。
Answer: (解答を表示する**)**
BSSカラーリングとは、Wi-Fi 6デバイスが各フレームに、それが属するBSS（基本サービスセット）を識別するカラーコードを付ける仕組みです。これにより、同じチャネルを共有する異なるBSSからのフレームを区別し、不要な衝突やバックオフを回避することができます。
BSSカラーリングは、干渉に対する適応型しきい値も導入しています。つまり、Wi-Fi 6デバイスは、現在のネットワーク環境に基づいて、チャネルが使用中かどうかを判断する信号強度値を調整できます。これにより、高密度環境において、スペクトルをより効率的に使用し、スループットを向上させることができます。

最新問題: **18**
VSXが設定されたAruba CX 8360スイッチ2台に関する問題のトラブルシューティングを行っています。各スイッチには複数のVRFが設定されています。既知のMACアドレスを持つ特定のクライアントデバイスのIPアドレスを特定する必要があります。
ペアになっているスイッチのプライマリ側で「show arp」コマンドを実行しても、クライアントのMACアドレスに一致するエントリが見つかりません。
クライアントデバイスは、VSX LAG を介して Aruba CX 6100 スイッチに接続されています。IP アドレスを正常に検出するには、どの操作を使用すればよいでしょうか？
A. Run the following command on the CX 6100 switch:
```
show mac-address-table
```
B. Run the following command on the VSX primary switch:
```
show arp all-vrfs
```
C. Run the following command on the VSX primary switch:
```
show mac-address-table
```
D. Run the following command on the CX 6100 switch:
```
show arp all-vrfs
```
Answer: B (メーッセージを残す**)**
show arp コマンドは、スイッチ上の特定の VRF またはすべての VRF の ARP テーブルを表示します。ARP テーブルには、スイッチに直接接続されているホスト、またはゲートウェイ経由で到達可能なホストの IP アドレスと MAC アドレスのマッピングが含まれています。クライアント デバイスが VSX LAG によって別のスイッチに接続されている場合、最近プライマリ スイッチと通信していない限り、クライアント デバイスの ARP エントリはプライマリ スイッチに存在しません。
したがって、クライアントデバイスのIPアドレスを見つけるには、管理者はVSXペアのセカンダリスイッチでshow arpコマンドを実行し、クライアントデバイスのサブネットを含むVRF名を指定する必要があります。

最新問題: **19**
貴社の製造業の顧客は、設置業者に倉庫内にヘッドレススキャナ70台とIPカメラ50台を設置してもらう予定です。これらの新しいデバイスは802 1X認証をサポートしていません。

HPE Arubaは、MPSKを使用して安全な環境を維持しながら、この導入に伴うIT管理の負担をどのように軽減できるでしょうか？
A. インストーラーにClearPassセルフサービス登録を使用してキーを生成してもらいます。
B. MPSKゲートウェイにMAC OUIに基づいて固有の事前共有鍵を導出させる。
C. MPSK Localを使用して、デバイスに固有の事前共有キーを自動的に提供します。
D. MPSKローカルでは、カメラは共通の鍵を共有し、スキャナは別の鍵を共有できます。
Answer: (解答を表示する)
MPSK Localは、802.1X認証をサポートしないデバイスの導入に伴うIT管理の負担を軽減しつつ、安全な環境を維持できる機能です。MPSK Localを使用すると、スイッチはデバイスのMACアドレスに基づいて、デバイス固有の事前共有キーを自動的に生成して割り当てることができます。デバイス側での設定や外部認証サーバーは不要です。他のオプションは、インストーラーまたはMPSKゲートウェイによる手動操作が必要となるか、デバイス固有の事前共有キーを提供しないため、適切ではありません。参照 :https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch05.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch06.html

最新問題**: 20**
顧客はアクセス用にスタック接続されたAruba CX 6200およびCX 6300スイッチを使用しており、認証にはVSXペアのAruba CX 8325をコアとして、802.1X認証を実装しています。ケーブル配線が不十分なため、一部のアンマネージドスイッチがまだ使用されています。これらのスイッチの背後にあるデバイスがネットワーク障害を引き起こすことがあります。問題が発生した場合、スイッチはヘルプデスクに警告を送信する必要があります。この問題に対する効果的な解決策を実装するよう依頼されました。
これに対する解決策は何ですか？
A. Aruba CX 8325 スイッチでスパニングツリーを設定します。trap-option を設定します。
B. Aruba CX 6200およびCX 6300スイッチのすべてのエッジポートでループ保護を設定します。トラップオプションは不要です。
C. Aruba CX 6200 および CX 6300 スイッチのすべてのエッジ ポートでループ保護を設定します。trap-option を設定します。
D. Aruba CX 6200およびCX 6300スイッチでスパニングツリーを設定します。トラップオプションは不要です。
Answer: C (メーッセージを残す)
これは、管理対象外スイッチの背後にあるデバイスがループによってネットワーク障害を引き起こすという問題に対する正しい解決策です。ループ保護は、ループ保護が有効になっている各ポート、LAG、またはVLANにループ保護パケットを送信することで、Aruba CXスイッチがループを検出して防止できるようにする機能です。ループ保護パケットを送信したスイッチが受信した場合、ループが存在することが示され、設定に基づいてアクションが実行されます。ループ保護は、エンドデバイスまたは管理対象外スイッチに接続するポートである、Aruba CX 6200およびCX 6300スイッチのすべてのエッジポートで設定する必要があります。ループが検出されたときにヘルプデスクに警告を送信するように、trap-optionを設定する必要があります。他のオプションは、ループ保護を設定していないか、trap-optionを設定していないため、正しくありません。

最新問題**: 21**
お客様から、新しく導入したマイクロブランチグループで接続の問題が発生しています。このグループのアクセスポイントはAruba Central上ではオンラインになっていますが、VPNトンネルが形成されません。
この問題の最も可能性の高い原因は何ですか？
A. APとゲートウェイの間には時間差があります。ゲートウェイにNTPを追加する必要があります。
B. 接続の暗号化に使用されるゲートウェイのSSL証明書が、APの信頼リストに追加されていません。
C. APとゲートウェイ間のGREトンネルをブロックするファイアウォールが存在する可能性があります
D. ゲートウェイグループが自動クラスタモードで動作していますが、手動クラスタモードに変更する必要があります。
Answer: (解答を表示する)
これは、マイクロブランチグループ内のアクセスポイントがAruba Centralでオンラインになっているにもかかわらず、VPNトンネルが形成されないという問題の最も可能性の高い原因です。マイクロブランチグループは、アクセスポイントとゲートウェイの両方を含むグループであり、安全な通信のためにVPNトンネルを形成できます。VPNトンネルは、カプセル化プロトコルとしてGRE（Generic Routing Encapsulation）、暗号化プロトコルとしてIPSecを使用します。アクセスポイントとゲートウェイ間のGREトラフィックをブロックするファイアウォールが存在する場合、VPNトンネルは確立できません。その他のオプションは、VPNトンネルの形成に影響を与えないか、マイクロブランチグループには適用されないため、誤りです。参照 :https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/gateways/microbranch.htm
https://www.arubanetworks.com/assets/tg/TB_ArubaGateway.pdf

最新問題: **22**
セキュリティ担当ディレクターから、新入社員の職務要件に基づいてAOS-CXスイッチの管理ロールを割り当てるよう依頼されました。設定が完了した後、管理者ロールが割り当てられたユーザーがスイッチ上で適切なアクセスレベルを持っていないことが判明しました。
当該ユーザーは、機密性の低い設定情報の閲覧に限定されておらず、また、その役割にレベル1は割り当てられていなかった。
ユーザーにはどのデフォルト管理ロールが割り当てられるべきだったのでしょうか？
A. 設定
B. システム管理者
C. 演算子
D. ヘルプデスク
Answer: B (メーッセージを残す**)**

最新問題: **23**
アップリンクが1/1/25と1/1/26のAruba CX 6200 24Gスイッチで、クライアントポートがレイヤ2ループを形成するのを防ぐにはどうすればよいですか？
A. int 1/1/1-1/1/24、ループ保護
B. int 1/1/1-1/1/28. ループ保護
C. int 1/1/1-1/1/28. ループガード
D. int 1/1/1-1/1/24. ループガード
Answer: A (メーッセージを残す**)**
コマンド loop-protect は、ループ保護が必要な各レイヤ 2 インターフェイス (ポート、LAG、または VLAN) でループ保護を有効にします。ループ保護は、タグなしレイヤ 2 リンクだけでなく、タグ付き VLAN でもループを検出できます。

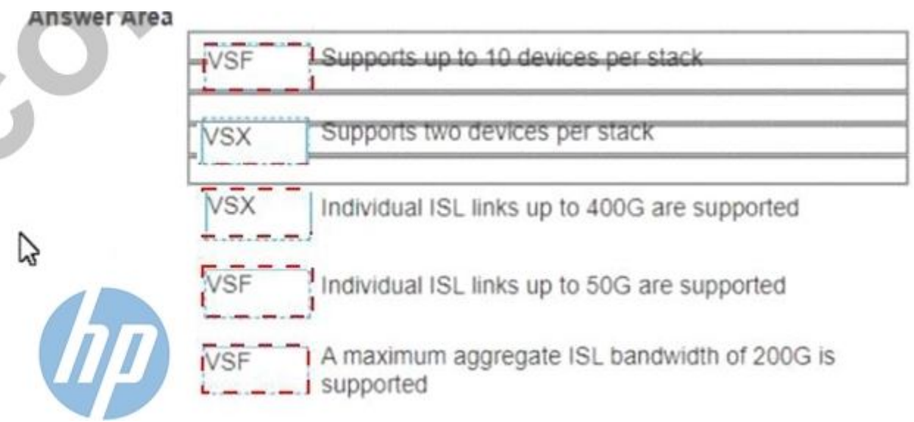
最新問題: **24**
ある企業が最近、複数の支店に新しいArubaアクセスポイントを導入しました。無線LAN 802.1X認証はクラウド上のRADIUSサーバーに対して行われます。セキュリティチームは、アクセスポイントとRADIUSサーバー間の通信が外部に漏洩するのではないかと懸念しています。
この状況における適切な解決策は何でしょうか？
A. すべての無線機器でEAP-TLSを有効にする
B. APとAruba CentralでRadSecを設定します。
C. すべての無線デバイスでEAP-TTLSを有効にする。
D. APとRADIUSサーバーでRadSecを設定する
Answer: D (メーッセージを残す**)**
これは、無線LAN 802.1X認証をクラウド上のRADIUSサーバーに対して行い、セキュリティチームがAPとRADIUSサーバー間のトラフィックが漏洩することを懸念しているシナリオにおいて、適切な解決策です。RadSec（RADIUS over TLSとも呼ばれる）は、TCPおよびTLS上でRADIUSトラフィックの暗号化と認証を提供するプロトコルです。RadSecはAPとRADIUSサーバーの両方で設定でき、RADIUSパケットを交換するための安全なトンネルを確立できます。他のオプションは、RADIUSトラフィックの暗号化または認証を提供しないか、RadSecを使用していないため、適切ではありません。
参考文献：
https://www.securew2.com/blog/what-is-radsec/
https://www.cloudradius.com/radsec-vs-radius/

最新問題: **25**
お客様は、分散オーバーレイファブリックにおいて、役割がポリシーの一貫した適用を維持するのにどのように役立つかについて、もっと詳しく知りたいと考えています。この概念をどのように説明しますか？
A. デバイス認証後、グループベースのポリシーIDが出力VTEPに適用され、入力VTEPでポリシーが適用されます。

B. ロールベースのポリシーはIPアドレスに紐付けられており、IPベースのポリシーよりも優位性があり、ロール名はVTEP間で送信されます。
C. デバイス認証後、イングレスVTEPにグループベースポリシーIDが適用され、エグレスVTEPにポリシーが適用されます。
D. ロールベースのポリシーにより、キャンパスネットワーク全体でユーザーベーストンネリングが強化され、ポリシーのトラフィックはiPsecで保護されます。
Answer: C (メーッセージを残す**)**
これは、分散オーバーレイファブリックにおいて、ロールがポリシーの一貫した適用を維持するのにどのように役立つかを正しく説明したものです。ロールは、デバイスがClearPassまたはローカルデータベースで認証された後、グループベースポリシーID（GBP）をデバイスに割り当てるために使用されます。GBPは、デバイスからのトラフィックにタグを付け、イングレスVTEPに送信するために使用され、イングレスVTEPはVXLANヘッダーにGBPを適用します。その後、イグレスVTEPは、GBPと宛先デバイスに基づいてポリシーを適用します。他のオプションは、正しいイベントシーケンスを説明していないか、正しい用語を使用していないため、誤りです。参考資料：
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.htmlhttps://www.aruba

最新問題**: 26**
ある企業がCXスイッチとゲートウェイにダイナミックセグメンテーションを導入しました。ネットワークのセキュリティ監査を実施したところ、CXスイッチとHPE Aruba Networkingゲートウェイ間のトンネルが暗号化されていないことが判明しました。同社は、悪意のある攻撃者がゲートウェイに偽装メッセージを挿入して通信を妨害したり、ネットワークに関する情報を入手したりする可能性があることを懸念しています。
管理者はこの状況に対処するために、どのような行動をとるべきでしょうか？
A. セキュアモード拡張を有効にする
B. 強化されたセキュリティを有効にする
C. 拡張PAPIセキュリティを有効にする
D. GREセキュリティを有効にする
Answer: (解答を表示する**)**
PAPIは、CXスイッチとAruba Gateway間の動的セグメンテーション用のトンネルを確立するために使用されるプロトコルです。デフォルトでは、PAPIは単純なチェックサムを使用してメッセージの整合性を検証しますが、ペイロードは暗号化されません。そのため、ネットワークが悪意のある攻撃者によるなりすまし攻撃やリプレイ攻撃にさらされる可能性があります。この問題を解決するには、管理者は拡張PAPIセキュリティを有効にする必要があります。拡張PAPIセキュリティは、AES-256暗号化とHMAC-SHA1認証を使用してトンネルトラフィックを保護します。拡張PAPIセキュリティは、コマンドsystem papi enhanced-security enableを使用してCXスイッチで有効にできます。これにより、CXスイッチとAruba Gateway間で構築されるトンネルが暗号化され、認証されることが保証されます。

最新問題**: 27**
各オプションに一致するArubaスタッキングテクノロジーを選択してください（オプションは複数回使用することも、まったく使用しないことも可能です）。
Answer:



Explanation:
a) スタックあたり最大10台のデバイスをサポート -> VSF

b) スタックごとに2つのデバイスをサポート -> VSX
c) 最大400Gの個別ISLリンクをサポート -> VSX
d) 最大50Gまでの個別ISLリンクをサポート -> VSF
e) 最大200GのISL帯域幅がサポートされます -> VSF
参考文献: 1
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/GUID-2E425DAE-EC54-4313-9D

最新問題**: 28**
802.1X認証フレームワークの主要構成要素は何ですか？ 2つ選択してください。）
A. VLANトランキングプロトコル（VTP）
B. 認証器 (ネットワークデバイスE.
C. 嘆願者 (デバイスE終了)
D. スパニングツリープロトコル（STP）
Answer: B,C (メーッセージを残す**)**

最新問題**: 29**
802.11kに関して正しいのはどれですか？
A. 無線測定を拡張し、無線局の無線ネットワーク管理メカニズムを定義します。
B. クライアントがAPにローミングする前に、複数のターゲットAPでクライアントを事前認証することで、ローミング遅延を軽減します。
C. APとクライアントが利用可能な無線リソースを動的に測定するためのメカニズムを提供します。
D. クライアントを5GHz帯に誘導するかどうかを決定する前に、クライアントRSSIを含むいくつかの指標を考慮します。
Answer: A,C (メーッセージを残す**)**

最新問題**: 30**
経営情報データベース（MIS）に保存されているデータを取得するには、何を使用しますか？
A. SNMPv3
B. DSCP
C. TLV
D. CDP
Answer: (解答を表示する**)**
説明
正解はA. SNMPv3です。
SNMPv3は、ネットワーク上の管理対象オブジェクトのデータベースである管理情報ベース（MIB）に格納されたデータを取得するために使用されるプロトコルです。SNMPv3は、以前のバージョンのSNMPにはなかったセキュリティ機能とアクセス制御機能を提供します。また、SNMPv3は暗号化を使用して、不正アクセスや改ざんからデータを保護することもできます。
Aruba認定プロフェッショナル - キャンパスアクセスに関する文書1によると、この認定資格が証明するスキルの1つは次のとおりです。
一般的なネットワーク監視ツールの出力を実装および分析する
PCAPを収集するようにポートミラーリングを設定します。
NAEエージェント9.4の設定
UXIセンサーを内部テストと外部テスト用に構成する

API スキャンを使用してネットワークを構成、管理、監視、トラブルシューティングする方法を説明します。この文書では、候補者はベンダー間のさまざまなプロトコルについて優れた理解を持っている必要があるとも述べられており、これは、SNMPv3 と、それを使用して MIB データにアクセスする方法に精通している必要があることを意味します。

最新問題: **31**
HPE Arubaワイヤレスネットワークでは、マルチキャスト伝送最適化はどのように実装されていますか？
A. 「マルチキャストフレームを送信する最適なレートは、関連するすべてのクライアント間での最高ブロードキャストレートに基づいています。」
B. このオプションを有効にすると、マルチキャストトラフィックの最小デフォルトレートは5GHz帯で12Mbpsに設定されます。
C. マルチキャストフレームを送信する最適なレートは、関連するすべてのクライアントの中で最も低いブロードキャストレートに基づいています。
D. マルチキャストフレームを送信する最適なレートは、関連するすべてのクライアントの中で最も低いユニキャストレートに基づいています。
Answer: A (メーッセージを残す)
これは、HPE Aruba ワイヤレス ネットワークにおけるマルチキャスト送信最適化の正しい定義です。マルチキャスト送信最適化は、関連するすべてのクライアントにおける最高ブロードキャストレートに基づいて送信レートを動的に調整することで、マルチキャスト トラフィックのパフォーマンスと信頼性を向上させる機能です。これにより、マルチキャスト フレームが各クライアントに最適なレートで送信され、再送信とパケット損失が削減されます。他の選択肢は、異なる機能を説明しているか、不適切な用語を使用しているため、誤りです。

最新問題: **32**
あなたは、社内の小規模拠点向けに標準化されたネットワーク設計に使用する構成をCentralで構築しています。ゲートウェイとアクセスポイントにはGUI構成を、スイッチにはテンプレート構成を使用したいと考えています。Arubaのベストプラクティスに準拠する必要があります。
これらの要件を満たす行動の組み合わせはどれですか？
A. Central にスイッチ用のグループを 1 つ、AP 用のグループを 2 つ、ゲートウェイ用のグループを 3 つ作成します。各ロケーションごとに固有のサイトを作成し、デバイスを適切なサイトに割り当てます。
B. セントラルでスイッチ用のグループを1つ、APとゲートウェイ用のグループをもう1つ作成します。各拠点ごとに固有のサイトを作成し、デバイスを適切なサイトに割り当てます。
C. Centralで単一のグループを作成します。各ロケーションごとに固有のサイトを作成し、デバイスを適切なサイトに割り当てます。
D. Centralで単一のグループを作成します。デバイスの種類ごとに固有のサイトを作成し、デバイスを適切なサイトに割り当てます。
Answer: C (メーッセージを残す)
これは、オプション C で、デバイス タイプごとに異なる構成方法が定義された単一のグループを Central で作成する方法が示されているためです。たとえば、Group1 という名前のグループを作成し、このグループ内で、スイッチにはテンプレート ベースの構成方法、Instant AP およびゲートウェイには UI ベースの構成方法を有効にすることができます。Aruba Central は、これら 2 つのグループを単一の名前 (Group1) で識別します。グループ内のデバイス タイプがテンプレート ベースの構成方法用にマークされている場合、グループ名には TG がプレフィックスとして付加されます (TG Group1)。Group1 は、ユーザー管理、監視、レポート、監査証跡 2 などのワークフローのグループ ID として使用できます。
https://www.arubanetworks.com/techdocs/central/latest/content/nms/groups/abt-groups.htm 2:https://www.aruba

最新問題: **33**
ある企業は最近、キャンパスのスイッチングインフラストラクチャをAruba 6300 CXスイッチにアップグレードしました。ラップトップやIoTデバイスが通常接続されるエッジポートに802.1X認証を実装しました。管理者は、PoEデバイスの場合、PONがデバイスが実際に必要とする電力ではなく、最大ワット数を供給していることに気づきました。IoTデバイスを接続すると、デバイスは情報交換を通じて必要な特定のワット数を要求します。
A. この電力の無駄遣いを懸念して、管理者はこの問題を解決するためにどのような対策を講じるべきでしょうか？
B. AAA認証を有効にして、LLDPおよび/またはCDP情報を除外する。
C. LLDPおよび/またはCDPのQoS信頼設定をグローバルに有効にする

D. 正しい電源定義でデバイスプロファイルを作成します。
E. 正しい電力定義で分類器ポリシーを実装します。
Answer: D (メーッセージを残す**)**
説明
Arubaのドキュメントポータル1によると、Aruba 6300 CXスイッチは、デバイスプロファイルや分類ポリシーなど、特定のポート上のPoEデバイスを制御するためのさまざまな機能をサポートしています。これらの機能は、PoEデバイスの消費電力を削減し、パフォーマンスを向上させるのに役立ちます。
1:
https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/monitoring_6300-6400/Content/Chp_LEDs/fr
https://www.arubanetworks.com/products/switches/6300-series/ 3:
https://docs.samsungknox.com/admin/knox-manage/configure/profile/configure-profile-policies/configure-profil

最新問題**: 34**
VSX LAGを使用するVSXペアを備えたダウンストリームアクセススイッチに、新しいVLAN 200を許可するにはどうすればよいですか？
A. MLAG 1 で VLAN トランク 200 を許可
B. MLAG1 に vlan trunk add 100
C. LAG 1 マルチシャーシですべての VLAN トランクを許可
D. vlan trunk add 100 in LAG1 multi-chassis
Answer: A (メーッセージを残す**)**
マルチシャーシLAG（MLAG）を使用してVSXペアに接続されているダウンストリームアクセススイッチで新しいVLAN（例VLAN 200）を許可するには、正しいコマンドはvlan trunk allowed 200 in MLAG 1です。
このコマンドは、VSXペアの両方のスイッチにまたがり、下流デバイスに接続するMLAG 1インターフェイスでVLAN 200を有効にします。これにより、各物理ポートを個別に設定することなく、両方のピア間で一貫したVLANトランキングが保証されます。

最新問題**: 35**
管理者は、帯域幅制限を超過した有線ゲストユーザーが切断されていないことに気づきます。ClearPass の Access Tracker では、切断 CoA メッセージが AOS-CX スイッチに送信されていることが示されています。
管理者が以下の設定を実行しました

```
Access1(config)# ip dns host cppm.arubatraining.com 10.254.1.23 vrf mgmt
Access1(config)# radius-server host cppm.arubatraining.com key plaintext aruba123 vrf mgmt
Access1(config)# aaa group server radius cppm
Access1(config-sg)# server cppm.arubatraining.com vrf mgmt
Access1(config-sg)# exit
Access1(config)# aaa accounting port-access start-stop interim 5 group cppm
Access1(config)# radius dyn-authorization client cppm.arubatraining.com secret-key plaintext aruba123 vrf mgmt
Access1(config)# radius dyn-authorization enable
```

この問題の最も可能性の高い原因は何ですか？
A. スイッチで認証変更がグローバルに有効になっていません
B. CPPM の SSL 証明書がスイッチの信頼ポイントとして追加されていません
C. スイッチ上のRADIUSシークレットとCPPMに不一致があります。
D. スイッチとClearPass Policy Managerの間には時間差があります
Answer: (解答を表示する**)**

認証変更 (CoA) は、ClearPass Policy Manager (CPPM) がスイッチなどのネットワーク機器にメッセージを送信してユーザーセッションの認証状態を変更できるようにする機能です。CoA を使用するには、CPPM とネットワーク機器の両方がこの機能をサポートし、有効になっている必要があります。AOS-CX スイッチの場合、CoA は radius-server coa enable コマンドを使用してグローバルに有効にする必要があります。スイッチで CoA が有効になっていない場合、CPPM からの切断 CoA メッセージは無視され、ユーザーセッションは終了しません。参照:
https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/index.htm#CPPM_UserGuide/Admin/C

最新問題**: 36**
ネットワークエンジニアが最近、CXスイッチに接続された有線デバイスがネットワーク上で異常動作していることを発見しました。この問題に対処するため、このデバイスが再びネットワークに接続できないようにする新しいClearPassポリシーが導入されました。
ClearPassがCoAを実行し、この有線デバイスのアクセス権限を変更できるようにするには、どの手順を実行する必要がありますか？ 2つ選択してください。）
A. スイッチとClearPassでNTPが設定されていることを確認してください。
B. スイッチ上で動的認証を設定します。
C. スイッチポートを再起動する
D. 動的セグメンテーションを使用する。
E. スイッチポートで動的認証を設定する
Answer: (解答を表示する**)**
ClearPassがCoAを実行し、有線デバイスのアクセス権限を変更できるようにするには、以下の手順を実行する必要があります。
* スイッチと ClearPass で NTP が設定されていることを確認してください。NTP はスイッチと ClearPass 間の時刻を同期するために必要であり、CoA メッセージが正しく処理されるために不可欠です 1。
* スイッチで動的認証を設定します。動的認証とは、スイッチがRADIUSサーバーからCoAメッセージを受け取り、既存のセッションに適用できるようにする機能です。動的認証は、スイッチ全体で有効にすることも、ポートごとに有効にすることもできます。
* オプションとして、スイッチポートで動的認証を設定します。この手順は必須ではありませんが、RADIUSサーバー2からのCoAメッセージを受け入れることができるポートをより細かく制御できます。
ClearPassがCoAを実行して有線デバイスのアクセスを変更するために、スイッチポートを再起動したり、ダイナミックセグメンテーションを使用したりする必要はありません。
参考文献：
1 https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/Aruba%20Controlle
2 https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-B

最新問題**: 37**
AOS-CXスイッチで動的セグメンテーションを使用して音声トラフィックを処理する際のベストプラクティスは何ですか？
A. 音声トラフィックのスイッチ認証とローカル転送
B. 音声トラフィックのスイッチ認証とユーザーベースのトンネリング。
C. 音声トラフィックの中央認証とポートベースのトンネリング。
D. コントローラ認証と全トラフィックのポートベーストンネリング
Answer: A (メーッセージを残す**)**
これは、AOS-CX スイッチで動的セグメンテーションを使用して音声トラフィックを処理するためのベストプラクティスです。動的セグメンテーションは、AOS-CX スイッチがユーザーの役割とポリシーに基づいて、ユーザーのトラフィックをコントローラまたは別のスイッチにトンネル接続できるようにする機能です。音声トラフィックの場合、スイッチ認証とローカル転送を使用することをお勧めします。これは、音声デバイスがスイッチによって認証され、そのトラフィックがトンネル接続なしでローカルに転送されることを意味します。これにより、音声トラフィックの遅延とジッターが低減され、音声品質が向上します。他のオプションは、中央認証またはトンネル接続を使用するため、音声トラフィックには最適ではないため、適切ではありません。参照: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html
https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

最新問題**: 38**

ネットワーク管理者は、ユーザーグループと特定のサーバー間の接続問題のトラブルシューティングを試みています。管理者は、一定期間にわたってデスクトップからパケットを調査する必要がありますが、トラフィックフローに関係するAOS-CXスイッチに直接接続されていません。
AOS-CXスイッチ上で確立する必要のあるERSPANセッションに関して、正しい記述はどれですか？ 2つ選択してください）
A. 送信元AOS-CXスイッチでは、指定された宛先は管理者のデスクトップが接続されているスイッチです。
B. 使用されているカプセル化プロトコルはGREです。
C. 使用されているカプセル化プロトコルはVXLANです。
D. カプセル化プロトコルはUDPです。
E. 送信元AOS-CXスイッチで、指定された宛先は管理者のデスクトップです。
Answer: (解答を表示する**)**
説明
ネットワーク管理者がデスクトップから一定期間のパケットを検査するために、AOS-CX スイッチで確立する必要のある ERSPAN セッションに関する正しい記述は以下のとおりです。ERSPAN (Encapsulated Remote Switched Port Analyzer) は、AOS-CX スイッチが 1 つ以上の送信元ポートまたは VLAN からのトラフィックを GRE (Generic Routing Encapsulation) トンネル経由でリモート宛先 IP アドレスにミラーリングできるようにする機能です。宛先 IP アドレスは管理者のデスクトップの IP アドレスである必要があり、ミラーリングされたトラフィックを受信および分析するためにパケットキャプチャ ツールがインストールされている必要があります。ERSPAN で使用されるカプセル化プロトコルは GRE であり、送信元および宛先 IP アドレス、セッション ID などの情報を含むヘッダーがミラーリングされたパケットに追加されます。その他の記述は、正しい宛先 IP アドレスを指定していないか、ERSPAN または GRE を使用していないため、誤りです。参照:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html

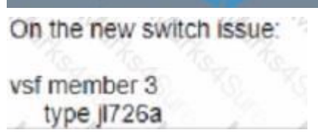
最新問題**: 39**
Aruba CX 6300で、インターフェース1/1/1のデフォルト状態において、インターフェースにIPアドレス10 10 10 1を設定するにはどうすればよいですか？
A. int 1/1/1. スイッチング、IPアドレス 10 10 10 1/24
B. インターフェース 1/1/1。スイッチングなし、IPアドレス 10 10 10.1/24
C. int 1/1/1. ip address 10.10.10.1/24
D. int 1/1/1. ルーティング、IPアドレス 10.10.10 1/24
Answer: (解答を表示する**)**
Aruba CX 6300 スイッチのインターフェース 1/1/1 のデフォルト状態において、そのインターフェースに IP アドレスを設定するには、まず no switching コマンドを使用してインターフェースのスイッチングを無効にする必要があります。その後、ip address コマンドを使用して IP アドレスを割り当てることができます。他のオプションは、スイッチングを無効にしていないか、switching や routing などの無効なキーワードを使用しているため、正しくありません。参考資料:
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch01.htmlhttps://www.arubanetworks.com

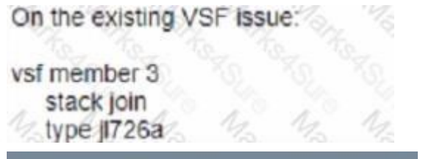
最新問題**: 40**
ポート1/45と2/45の間で、VSXペアのインタースイッチリンク256間に新しいVLAN 100を許可するにはどうすればよいですか？
A. ポート1/45および1/46に対してVLANトランク100を許可します
B. vlan trunk add 100 in LAG256
C. LAG256 で VLAN トランク 100 を許可
D. vlan trunk add 100 in MLAG256
Answer: C (メーッセージを残す**)**
ポート1/45と2/45のVSXペア間インタースイッチリンク256で新しいVLAN 100を許可するには、LAG256でvlan trunk allowed 100コマンドを使用する必要があります。これにより、VSXピア間のインタースイッチリンクの一部であるトランクポートLAG256の許可VLANリストにVLAN 100が追加されます。他のオプションは、正しいコマンドを使用していないか、正しいポートまたはVLANを指定していないため、正しくありません。
参考文献：

https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch07.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html

最新問題**: 41**
ネットワーク管理者が、ゲストユーザーがネットワークに接続および認証する際に発生するいくつかの問題のトラブルシューティングを行っています。アクセススイッチはAOS-CXスイッチです。
管理者は、ゲストユーザーに割り当てられている役割に関する情報を確認するために、どのコマンドを使用すべきでしょうか？
A. show aaa authentication port-access interface all client-status
B. ポートアクセスキャプティブポータルプロファイルを表示
C. ポートアクセスロールを表示する
D. diag-dump captiveportal client verbose
Answer: (解答を表示する**)**
show aaa authentication port-access interface all client-status コマンドは、すべてのインターフェイスでポートベースアクセス制御によって認証されたすべてのクライアントの状態を表示します。出力には、各クライアントのMAC アドレス、ユーザーロール、VLAN ID、およびセッションタイムアウトが含まれます。このコマンドを使用すると、AOS-CX スイッチによってゲストユーザーに割り当てられたロールに関する情報を調べることができます。
参考資料: https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E

最新問題**: 42**
お客様は、2台のスイッチで構成されたAruba CX 6200F VSFスタックを使用しています。3台目のメンバー（JL726A）をVSF構成に追加する必要があります。新しいデバイスをVSFに参加させるための構成は何ですか？
A.


B.


C.


D.


Answer: (解答を表示する**)**
説明
Arubaのドキュメントポータル1によると、Aruba CX 6200FのVSFスタックは、最大8つのメンバーで構成される仮想スイッチングフレームワーク（VSF）を作成し、単一の論理デバイスとして管理できる機能です。VSFスタックは、負荷分散、フェイルオーバー、冗長性、セキュリティなどのメリットを提供します。

VSFスタックに新しいデバイスを追加するには、VSFコマンドvsf memberを使用してデバイスを設定し、タイプ、リンク、およびセカンダリメンバー情報を指定する必要があります。新しいデバイスのタイプは、JL726A、JL726B、JL726C、またはJL726Dのいずれかです。リンクは、新しいデバイスを既存のVSFメンバーに接続するインターフェイスです。セカンダリメンバーは、障害発生時にバックアップとして機能するメンバーを指定するオプションのパラメーターです。
1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7726/index.html 2:
https://buy.hpe.com/us/en/networking/switches/fixed-port-l3-managed-ethernet-switches/6000-switch-products/a
https://addin.co.th/shop/switch/aruba-switch/6200f-series/jl726a/

最新問題**: 43**
AOS-CXスイッチで動的セグメンテーションを使用して音声トラフィックを処理する際のベストプラクティスは何ですか？
A. 音声トラフィックのスイッチ認証とローカル転送
B. 音声トラフィックのスイッチ認証とユーザーベースのトンネリング。
C. 音声トラフィックの中央認証とポートベースのトンネリング。
D. コントローラ認証と全トラフィックのポートベーストンネリング
Answer: A (メーッセージを残す**)**
これは、AOS-CXスイッチ上で動的セグメンテーションを使用して音声トラフィックを処理するためのベストプラクティスです。
動的セグメンテーションは、AOS-CXスイッチがユーザーの役割とポリシーに基づいて、ユーザーのトラフィックをコントローラまたは別のスイッチにトンネル接続できるようにする機能です。音声トラフィックについては、スイッチ認証とローカル転送の使用が推奨されます。これは、音声デバイスがスイッチによって認証され、そのトラフィックがトンネル接続なしでローカルに転送されることを意味します。これにより、音声トラフィックの遅延とジッターが低減され、音声品質が向上します。その他のオプションは、中央認証またはトンネル接続を使用するため、音声トラフィックには最適ではありません。
参考文献：
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html
https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

最新問題**: 44**
システムエンジニアは、遠隔オフィスに送られる複数のAruba CX 6300スイッチを事前に設定する必要があります。訓練を受けていない現地のフィールド技術者が、スイッチの展開と複数のAP-515およびAP-575Sの設置を行います。APに接続されているケーブルにはラベルが貼られていません。
VLANは既にVLAN 100（管理）、VLAN 200（クライアント）、VLAN 300（ゲスト）に事前設定されています。アクセスポイントが正しく動作するようにするには、どのような設定を行うのが適切でしょうか？
A.

```
port-access lldp-group IAP-Group
    seq 10 match sys-desc AP-515
    seq 20 match sys-desc AP-575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp vlan trunk native 100
    vlan trunk allowed 100,200,300
    enable
port-access device-profile IAP-Profile
    associate role IAP-Role
    associate lldp-group IAP-Group
```

B.

```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    associate role IAP-Role
    associate lldp-group IAP-Group
    no shutdown
```

C.

```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

D.

```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

Answer: C (メーッセージを残す)

説明

オプションCは、APが正しく動作するようにするための正しい設定です。apコマンドを使用して、ネイティブVLANとしてVLAN 100、タグ付きVLANとしてVLAN 200と300を持つAP用のポートプロファイルを設定します。また、ポートでLLDPを有効にしてAPを検出し、ポートプロファイルに自動的に割り当てます。他のオプションは、apコマンドを使用していない、LLDPを有効にしていない、またはVLANを正しく設定していないため、正しくありません。参考資料：

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch03.html

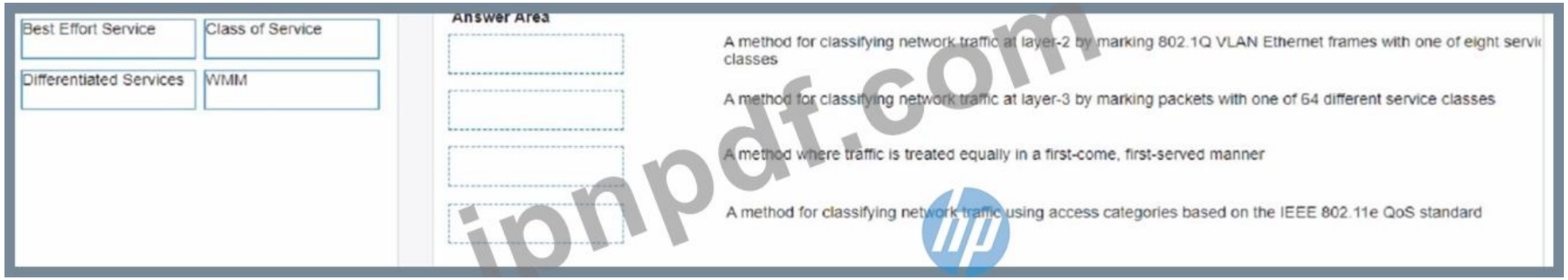
最新問題: **45**

無線デバイスがAP1からAP2へローミングする際、キー管理ワークフローにはどのような手順が含まれますか？ 2つ選択してください。）
A. キー管理サービスは、AirMatchからAP2のすべてのネイバーのリストを受け取ります。
B. キー管理サービスは、AirMatchからAP1のすべてのネイバーのリストを受け取ります。
C. キー管理サービスは、AP2のネイバー用にR1キーを生成します。
D. AP1はクライアントの情報をキャッシュし、それを鍵管理サービスに送信します。
E. クライアントはAP1からローミングした後、AP2と接続して認証を行う。
Answer: C,E (メーッセージを残す)

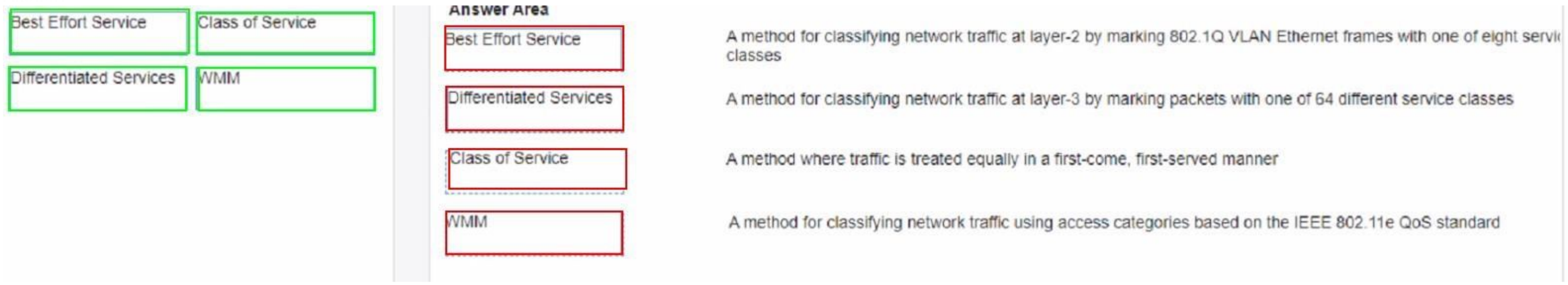
最新問題**: 46**
APとゲートウェイを使用するArubaOS 10アーキテクチャにおいて、クライアントがネットワークへの参加を試み、WLANがOWEで構成されている場合、どのようなことが起こりますか？
A. 認証情報は交換されません
B. ゲートウェイは応答しません。
C. 暗号化は適用されません。
D. RADIUSプロトコルが使用されます。
Answer: A (メーッセージを残す)
これは、クライアントがネットワークへの接続を試み、WLANがOWE（Opportunistic Wireless Encryption）で構成されている場合に何が起こるかについての正しい説明です。OWEは、クライアントまたはネットワークからの認証や資格情報を必要とせずに、オープンネットワークに暗号化を提供する標準規格です。OWEは、認証情報を交換することなく、クライアントとAP間の安全なセッションを確立するためにDiffie-Hellman鍵交換メカニズムを使用します。他の選択肢は、認証を必要とするシナリオ、またはOWEで使用されていない暗号化方式を説明しているため、誤りです。参照 :https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

最新問題**: 47**
アップリンクが1/1/51と1/1/52のCX 6000 48Gスイッチで、クライアントポートがループを検出し、tx-rx-disableパラメータが使用されている場合、スイッチはどのような動作をしますか？
A. ループが確認されたポートは無効になっています。
B. ループを送受信したポートが無効になります。
C. ループを送信したポートが無効になっています。
D. ループを受信したポートが無効になっています。
Answer: B (メーッセージを残す)
HPE Aruba Networking CX 6000スイッチのtx-rx-disableパラメータを使用すると、ループが検出されたときに、ループパケットを送信したポート（tx）と受信したポート（rx）の両方が無効になります。この動作により、ループがネットワークに影響を与えるのを防ぎ、受信ポートのみを無効にするよりも包括的な対策となります。

最新問題**: 48**
適切なQoS概念とその定義を一致させてください。（選択肢は複数回使用することも、全く使用しないことも可能です。）



Answer:



最新問題: **49**

ネットワークエンジニアが最近、CXスイッチに接続された有線デバイスがネットワーク上で異常動作していることを発見しました。この問題に対処するため、このデバイスが再びネットワークに接続できないようにする新しいClearPassポリシーが導入されました。

ClearPassがCoAを実行し、この有線デバイスのアクセス権限を変更できるようにするには、どの手順を実行する必要がありますか？ 2つ選択してください。）

A. スイッチとClearPassでNTPが設定されていることを確認してください。

B. スイッチ上で動的認証を設定します。

C. スイッチポートを再起動する

D. 動的セグメンテーションを使用する。

E. スイッチポートで動的認証を設定する

Answer: B,C (メーッセージを残す**)**

説明

CoA（Change of Authorization）は、ClearPassが認証後にデバイスの認証とアクセス権限を動的に変更できるようにする機能です1。CoAはRADIUSメッセージを使用してネットワークデバイスと通信し、デバイスの再認証、新しいVLANまたはユーザーロールの適用、デバイスの切断などのアクションを実行するように指示します2。

CXスイッチでCoAを有効にするには、ネットワークエンジニアはスイッチ上で動的認証を設定する必要があります。これは、スイッチがClearPassからのRADIUSメッセージを受け入れ、要求されたアクションを実行できるようにするグローバルコマンドです3。また、ネットワークエンジニアは、スイッチ上で動的認証クライアントとしてClearPassのIPアドレスと共有シークレットを指定する必要があります3。

特定の有線デバイスに対してCoAをトリガーするには、ネットワークエンジニアはスイッチポートを再起動する必要があります。これは、デバイスが接続されているポートを一時的に無効にしてから再度有効にする操作です。これにより、デバイスは再認証を行い、ClearPassから新しいポリシーを受信する必要があります。スイッチポートの再起動は、interface shutdownコマンドとno shutdownコマンドを使用して手動で行うことも、ClearPassをCoAサーバーとして使用し、Port-Bounce-Host AVP（属性値ペア）を含むRADIUSメッセージを送信して自動的に行うこともできます。

最新問題**: 50**
顧客がゲートウェイを導入し、SD-WANのすべての機能を活用したいと考えている場合、どのペルソナロールオプションを選択すべきでしょうか？
A. ArubaOS 10 ブランチ
B. ArubaOS 10 VPNコンセントレータ
C. ArubaOS 10 ワイヤレス
D. ArubaOS 10 Mobility
Answer: A (メーッセージを残す**)**
ゲートウェイをデプロイしてすべての SD-WAN 機能を活用するために選択する必要があるペルソナ ロール オプションは A. ArubaOS 10 ブランチです。
ArubaOS 10 Branchは、ゲートウェイがブランチネットワーク向けにLANとWANの両方の機能を提供できるようにするペルソナです。ゲートウェイは、ワイヤレスコントローラ、ルータ、ファイアウォール、およびSD-WANデバイスとして機能します。SD-WAN機能には、ルートとトンネルのオーケストレーション、動的パスステアリング、前方誤り訂正、SaaSトラフィックの最適化、SASEオーケストレーションなどが含まれます1。
他の選択肢が間違っている理由は以下のとおりです。
B) ArubaOS 10 VPN コンセントレータ: これは、ゲートウェイがリモート アクセスまたはサイト間 VPN 接続用の VPN コンセントレータとして機能できるようにするペルソナです。SD-WAN 機能は提供しません 2。
C) ArubaOS 10 Wireless: これは、ゲートウェイがキャンパスネットワークのワイヤレスコントローラとして機能できるようにするペルソナです。SD-WAN機能は提供しません3。
D) ArubaOS 10 Mobility: これは、ゲートウェイがキャンパスネットワークのモビリティコントローラとして機能することを可能にするペルソナです。SD-WAN機能は提供しません。

最新問題**: 51**
802.1X認証を使用している既存環境に新しいUXIを導入するには、どの方法を使用しますか？ センサーは携帯電話回線に接続されていません）
A. スマートフォンでUXIアプリを使用し、Bluetooth経由でUXIに接続してください。
B. スマートフォンのArubaインストーラーアプリを使用してバーコードをスキャンしてください。
C. 既にインストールされているUXIから新しいUXIを接続し、初期設定を調整します。
D. シリアルケーブル経由でCLIを使用して初期設定を調整します。
Answer: A (メーッセージを残す**)**
802.1X認証を使用している既存の環境に新しいUXIを導入するには、スマートフォンのUXIアプリを使用してBluetooth経由でUXIに接続する必要があります。UXIアプリを使用すると、UXIセンサーのQRコードをスキャンして、SSID、パスワード、IPアドレスなどのネットワーク設定を構成できます。Bluetooth接続により、ネットワークアクセスや携帯電話接続を必要とせずにUXIセンサーと通信できます。他のオプションは、UXIアプリを使用しないか、Bluetoothを使用しないため、正しくありません。参考資料 :https://www.arubanetworks.com/products/network-management-operations/analytics-monitoring/user-experience-insight-sensors/ https://help.centralon-prem.arubanetworks.com/2.5.4
/documentation/online_help/content/nms-on-prem/aos-cx/get-started/uxi-sensor.htm

最新問題**: 52**
ドラッグアンドドロップ問題
トピックとそれに対応する技術を一致させてください（選択肢は複数回使用することも、全く使用しないことも可能です）。

Answer:

最新問題**: 53**

ArubaスイッチでHTTPトラフィックをブロックし、HTTPSトラフィックを許可するACLを設定する必要があります。以下のACLルールのうち、これを実現するものはどれですか？

A. deny tcp any any eq 80; permit tcp any any eq 443

B. deny tcp any any eq 443; permit tcp any any eq 80

C. permit tcp any any eq 443; deny tcp any any eq 80

D. permit tcp any any neq 80

Answer: (解答を表示する)

最新問題**: 54**

お客様は、2台のスイッチで構成されたAruba CX 6200F VSFスタックを所有しています。VSF構成に3台目のメンバー (JL726A) を追加する必要があります。

新しいデバイスがVSFに参加できるようにする構成は何ですか？

A.

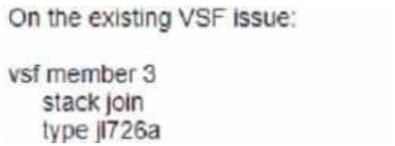
```
On the new switch issue:

vsf member 1
    link 1 1/1/50
    link 2 1/1/49
vsf renumber-to 3
```

B.

```
On the new switch issue:

vsf member 3
    type jl726a
```

C.


D.


Answer: C (メーッセージを残す)

Arubaのドキュメントポータル1によると、Aruba CX 6200FのVSFスタックは、最大8つのメンバーで構成される仮想スイッチングフレームワーク（VSF）を作成し、単一の論理デバイスとして管理できる機能です。VSFスタックは、負荷分散、フェイルオーバー、冗長性、セキュリティなどのメリットを提供します。

VSFスタックに新しいデバイスを追加するには、VSFコマンドvsf memberを使用してデバイスを設定し、タイプ、リンク、およびセカンダリメンバー情報を指定する必要があります。新しいデバイスのタイプは、JL726A、JL726B、JL726C、またはJL726Dのいずれかです。リンクは、新しいデバイスを既存のVSFメンバーに接続するインターフェイスです。セカンダリメンバーは、障害発生時にバックアップとして機能するメンバーを指定するオプションのパラメーターです。

最新問題: **55**

無線デバイスがAP1からAP2へローミングする場合、キー管理ワークフローにはどのような手順が含まれますか？
（2つ選択してください。）

A. AP1はクライアントの情報をキャッシュし、それを鍵管理サービスに送信します。

B. キー管理サービスは、AirMatchからAP2のすべてのネイバーのリストを受け取ります。

C. キー管理サービスは、AirMatchからAP1のすべてのネイバーのリストを受け取ります。

D. キー管理サービスは、AP2のネイバー用にR1キーを生成します。

E. クライアントはAP1からローミングした後、AP2と関連付け、認証を行う。

Answer: A,D (メーッセージを残す)

説明

無線デバイスがAP1からAP2へローミングする際のキー管理ワークフローに含まれる正しい手順は、AとDです。

A: AP1 はクライアントの情報をキャッシュし、それをキー管理サービスに送信します。これは、クライアントが AP1 と関連付けて認証を行うと、AP1 がクライアント用のペアワイズマスターキー (PMK) を生成し、それをキャッシュに保存するためです。AP1 はまた、PMK と MAC アドレス、VLAN、SSID などの他のクライアント情報を、Aruba Mobility Controller (MC) または Mobility Master (MM) デバイス 1 上で動作する集中型サービスであるキー管理サービスに送信します。キー管理サービスはこの情報を使用して、クライアントの高速ローミングを実現します。

D: キー管理サービスは、AP2 の近隣 AP 用に R1 キーを生成します。これは、キー管理サービスが AP1 からクライアント情報を受信すると、PMK を使用してクライアント用の R0 キーと R1 キーを導出するためです。R0 キーは R1 キーを生成するために使用され、R1 キーは暗号化用のペアワイズ一時キー (PTK) を生成するために使用されます。キー管理サービスは、R1 キーを AP2 とその近隣 AP に配布します。近隣 AP は、RF 近接度に基づいて AirMatch によって決定されます。このようにして、クライアントが AP2 またはその近隣のいずれかにローミングすると、802.1X 認証をスキップして、R1 キーを使用して新しい AP3 で PTK を迅速に生成できます。

B: キー管理サービスは、AirMatch から AP2 のすべての近隣のリストを受け取ります。これは誤りです。キー管理サービスは、AirMatch からこの情報を直接受け取るわけではありません。AirMatch は、MC または MM デバイスで実行される機能であり、機械学習アルゴリズムを使用して Aruba デバイスの RF パフォーマンスを最適化します。AirMatch は、信号強度と干渉に基づいて近くの AP に関する情報を含む近隣レポートを定期的にすべての AP に送信します。AP はこれらのレポートをキー管理サービスに送信し、キー管理サービスはこれらのレポートを使用して、特定のクライアント 2 に対して R1 キーを受け取る AP を決定します。

C :キー管理サービスは、AirMatchからAP1のすべてのネイバーのリストを受け取ります。これはBと同じ理由で誤りです。キー管理サービスは、この情報をAirMatchから直接受け取るのではなく、ネイバーレポートを送信するAPから受け取ります。

E: クライアントは AP1 からローミングした後、AP2 と関連付けて認証します。これは誤りです。クライアントは、AP1 で既に認証され、キー管理サービスから R1 キーを受け取っている場合、AP1 からローミングした後、AP2 で認証する必要はありません。クライアントは、AP2 と関連付け、R1 キーを使用して 4 ウェイ ハンドシェイクを実行して暗号化用の PTK を生成するだけで済みます 3。これは高速ローミングまたは
802.11rローミングに対応しており、完全認証によって発生する遅延や中断を軽減します。
1: ArubaOS 8.7 ユーザーガイド 2: ArubaOS 8.7 ユーザーガイド 3: ArubaOS 8.7 ユーザーガイド : ArubaOS 8.7 ユーザーガイド

最新問題: **56**
高密度環境におけるクライアントの遅延を最小限に抑えるため、新たなネットワーク設計が検討されている。この設計では、サブキャリアをクライアント専用に割り当てることで競合オーバーヘッドを排除し、遅延を最小限に抑える必要がある。
このユースケースに最適な技術はどれですか？
A. OFDMA
B. MU-MIMO
C. QWMM
D. チャネルボンディング
Answer: (解答を表示する**)**
OFDMA（直交周波数分割多重アクセス）は、サブキャリアをクライアントに割り当てることで競合オーバーヘッドを排除し、高密度環境におけるクライアントの遅延を最小限に抑えることができる技術です。
OFDMAは、複数のクライアントが同一チャネル内の異なるサブキャリアで同時に送信することを可能にし、競合を低減して効率を向上させます。MU-MIMO （マルチユーザー多入力多出力）は、複数のクライアントが同一チャネル内の異なる空間ストリームで同時に送信することを可能にする技術ですが、競合オーバーヘッドを排除するものではありません。QWMM （Quality of Service Wireless Multimedia）は、4つのアクセスカテゴリに基づいてトラフィックの優先順位付けを行う技術ですが、競合オーバーヘッドを排除するものではありません。チャネルボンディングは、隣接する2つのチャネルを1つのより広いチャネルに結合する技術で、帯域幅を増加させますが、競合オーバーヘッドを排除するものではありません。参考文献 :https://www.arubanetworks.com
/assets/ds/DS_AP510Series.pdf https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf

最新問題: **57**
Aruba Network Analytics Engine (NAE) はどのコンポーネントを使用していますか？
A. JSONベースのスクリプト
B. Lispベースのエージェント
C. Rubyベースのスクリプト
D. 現在の状態データベース
Answer: A (メーッセージを残す**)**
説明
JSON ベースのスクリプトは、Aruba Network Analytics Engine (NAE) で使用されるコンポーネントです。NAE は、エージェントと呼ばれる JSON ベースのスクリプトを使用してネットワーク監視およびトラブルシューティング機能を提供する機能です。エージェントは、スイッチの CLI コマンド、SNMP クエリ、REST API など、さまざまなソースからデータを収集し、事前定義されたルールとしきい値を使用して分析します。エージェントは、分析結果に基づいてアラート、通知、アクション、またはレポートを生成することもできます。参照:
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch07.html
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch08.html

最新問題: **58**
あなたは研究室で、以下の機器仕様を用いて実験を行っています。
* AP1は10 dBmの信号を生成する無線機を搭載しています。
* AP2は11dBmの信号を生成する無線機を搭載しています。
* AP1は9 dBiのゲインを持つアンテナを搭載しています。

* AP2は12 dBiのゲインを持つアンテナを搭載しています。
* AP1のアンテナケーブルは2dBの損失があります
* AP2のアンテナケーブルは3dBの損失があります
APTの等価等方放射電力（EIRP）はどのくらいになるでしょうか？
A. 26 dBm
B. 30 dBm
C. 17 dBm
D. -12 dBm
Answer: (解答を表示する**)**
AP1 の計算された等価等方放射電力 (EIRP) は 30 dBm です。EIRP は、送信電力 (dBm 単位) とアンテナ利得 (dBi 単位) の積からケーブル損失 (dB 単位) を差し引いたものです。AP1 の場合、EIRP = 10 dBm + 9 dBi -2 dB = 17 dBm。AP2 の場合、EIRP = 11 dBm + 12 dBi -3 dB
20 dBm。

最新問題**: 59**
お客様は現在、コアスイッチとしてMSTPが構成された5406モジュラースイッチを2台使用しています。貴社は新しいソリューションを提案しています。スパニングツリーをセットアップする必要がある場合、AOS-CX VSXスイッチペアに関してどのような説明をしますか？
A. MSTP リージョン構成で vsx-sync を使用して同期します。
B. vsx モードで vsx-sync stp-global を有効にして、設定を同期します。
C. vsx モードで vsx-peer stp-global を有効にして、設定を同期します。
D. スパニングツリーの設定は、デフォルトでVSXと同期されます。
Answer: B (メーッセージを残す**)**

最新問題**: 60**
LLDP-MEDによって何が可能になりますか？ 2つ選択してください。）
A. VoIP電話用に音声VLANを自動的に設定できます
B. APは必要に応じてPoE対応スイッチポートから電力供給を要求できます
C. iSCSLクライアントデバイスはフロー制御の有効化を要求できます。
D. GVRP VLAN情報を使用して、VLANをトランクに動的に追加できます。
E. iSCSLクライアントデバイスは、ポートに必要なMTU設定を行うことができます。
Answer: A,B (メーッセージを残す**)**
説明
これらは、LLDP-MED（リンク層検出プロトコル - メディアエンドポイント検出）によって実現される2つの利点です。
LLDP-MEDはLLDPの拡張機能であり、VoIP電話やアクセスポイントなどのネットワーク機器に追加機能を提供します。その機能の一つとして、VoIP電話の音声VLANを自動的に構成する機能があります。これにより、VoIP電話をデータ機器とは別のVLANに配置し、QoSおよびセキュリティポリシーを適用することが可能になります。
もう1つの機能は、PoE対応スイッチポートから必要に応じて電力を要求することです。これにより、APは利用可能な電力予算に基づいて消費電力とパフォーマンスを調整できます。その他のオプションは、LLDP-MEDで有効化されていないか、LLDP-MEDとは関係がないため、誤りです。参考文献：
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-qos/lldp-me
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/poe.htm

最新問題**: 61**

お客様から、新規ユーザーにスイッチ管理ロールを割り当てるよう依頼がありました。お客様の要望は、ユーザーロールがWeb UIの「システム」>「ログ」ページへのアクセス権限のみを持ち、かつREST APIの「/logs/event」リソースに対してGETメソッドのみを使用できる権限を持つことです。
これらの要件を満たすデフォルトのAOS-CXユーザーロールはどれですか？
A. 管理者
B. 監査役
C. システムオペレーター
D. 演算子
Answer: B (メーッセージを残す**)**
AOS-CX では、監査担当者の役割は、システムログとイベントへの読み取り専用アクセスを必要とするユーザー向けに設計されています。この役割では、Web UI の [システム] > [ログ] ページへのアクセスが可能になり、特に /logs/event リソースに対して、管理者権限を付与することなく、REST API の GET メソッドを使用してログを取得できます。これは、アクセス制限に関する顧客の要件を満たしています。

最新問題: **62**
貴社の製造業の顧客は、倉庫に200台の無線IPカメラと50台のヘッドレススキャナーを導入しようとしています。これらの新しいデバイスは802.1X認証をサポートしていません。
HPE Arubaは、このような環境において、これらの新しいIPカメラのセキュリティをどのように強化できるでしょうか？
A. MPSK Localを使用して、デバイスに固有の事前共有キーを自動的に提供します。
B. Aruba ClearPassは802.1X認証を実行し、証明書をインストールします。
C. MPSKは、WLAN内の各デバイスが独自の事前共有鍵を持つことを可能にします。
D. MPSKローカルでは、カメラはレイを共有し、スキャナーは別のレイを共有できます。
Answer: C (メーッセージを残す**)**
この環境における新しいIPカメラとスキャナーのセキュリティを強化するための最良の選択肢はCです。
MPSKは、WLAN内の各デバイスがそれぞれ固有の事前共有鍵を持つことを可能にする。
MPSKはMulti Pre-Shared Keyの略で、異なるデバイスが異なる事前共有キーを使用して同じSSIDに接続できるようにする機能です。これにより、各デバイスが802.1X認証や外部ポリシーエンジンを必要とせずに独自のキーと役割を持つことができるため、ネットワークのセキュリティと拡張性が向上します。MPSKは、アクセスポイント（AP）上でローカルに設定することも、Aruba Central12で一元的に設定することもできます。
他の選択肢が間違っている理由は以下のとおりです。
A) MPSK Localは、ユーザーがデバイス上でSSIDごとに24個のPSKをローカルに設定できる機能です。
これらのローカルPSKは、基本MPSK機能の拡張として機能します。しかし、MPSK Localはこのシナリオには適していません。なぜなら、SSIDごとに最大24台のデバイスしかサポートできないのに対し、クライアントには250台のデバイスがあるからです1。
B) Aruba ClearPassは、802.1X認証を実行し、デバイスに証明書をインストールできるネットワークアクセス制御ソリューションです。ただし、新しいIPカメラとスキャナは802.1X認証をサポートしていないため、このオプションはこのシナリオには適していません3。
D) MPSK Localでは、カメラが鍵を共有し、スキャナが別の鍵を共有することは許可されません。
MPSK Localは、デバイスの種類に関係なく、各デバイスに異なるキーを割り当てます。さらに、MPSK LocalはSSIDごとに最大24台のデバイスしかサポートできませんが、クライアントは最大250台のデバイスを接続できます1。

最新問題: **63**
スイッチでUBTを設定する際に、ゲートウェイの役割が指定されていない場合はどうなりますか？

A. スイッチはクライアントをアクセスVLANに接続します
B. ゲートウェイはクライアントにデフォルトの役割を割り当てます
C. スイッチはクライアントにデフォルトの拒否ロールを割り当てます。
D. ゲートウェイは拒否ロールをクライアントに返します。
Answer: A (メーッセージを残す**)**
Arubaのドキュメントポータル1によると、ユーザーベーストンネリング（UBT）は、GREを使用してスイッチインターフェイス上の受信トラフィックをゲートウェイにトンネル接続し、そこでさらに処理を行う機能です。UBTにより、スイッチはユーザーごとの認証とアクセス制御を使用して、一貫したアクセスと権限を確保し、集中型のセキュリティポリシーを提供できます。
オプションA :スイッチはクライアントをアクセスVLANに接続します
これは、オプション A が Aruba スイッチでの UBT の動作方法を示しているためです。デバイスがネットワークに接続すると、MAC 認証または 802.1X を使用して認証され、ClearPass から強制ポリシーがトリガーされます。このポリシーには、ユーザー ロール構成を含む強制プロファイルが含まれています。ユーザー ロールは、スイッチ上でローカルに割り当てることも、強制プロファイルの一部として ClearPass 上で割り当てることもできます。ユーザー ロールによって、デバイスが属する VLAN と、そのデバイスに適用されるアクセス ポリシーが決まります 23。
したがって、選択肢Aが正解です。
1: https://www.arubanetworks.com/techdocs/central/latest/content/nms/aos-cx/cfg/conf-cx-ubt.htm 2:
https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-849
https://community.arubanetworks.com/viewdocument/?DocumentKey=c740df4e-3e26-4cc5-9126-355a18709c4

最新問題**: 64**
お使いのAruba CX 6300 VSFスタックは、隣接デバイスとの間でSVI 10とLAG 1を介してOSPF隣接関係を確立しています。スイッチには以下の設定が作成されました。

```
vlan 20,30,40
!
interface vlan 20
     ip address 10.10.20.1/24
!
interface vlan 30
     ip address 10.10.30.1/24
!
interface vlan 40
     ip address 10.10.40.1/24
```


A.
```
vlan 20, 30,40
    ospf passive
```
B.
```
interface vlan 20,30,40
   ip ospf passive
```
C.
```
router ospf 1
 area 0
 passive-interface
    vlan 20,30,40
```
D.
Answer: C (メーッセージを残す**)**
説明
オプションCに、SVI 10とLAG 1を介して隣接デバイスとのOSPF隣接関係を確立するための正しい設定を示します。設定には以下の手順が含まれます。
* VLAN 10を作成し、名前とIPアドレスを割り当てます。
* LAG 1 を作成し、名前とモード（動的または静的）を割り当てます。
* LAG 1にメンバーポートを追加し、LAGインターフェースを有効にします。

* LAG 1 のタグなし VLAN として VLAN 10 を割り当てます。
* スイッチでOSPFを有効にし、ルーターIDを割り当てます。
* OSPFエリア0を作成し、そのエリアにSVI 10をインターフェースとして追加します。
オプションAは、スイッチ上でOSPFを有効にせず、OSPFエリアも作成しないため、誤りです。オプションBは、LAG 1のタグ付きVLANとしてVLAN 10を割り当てますが、これはSVI 10と互換性がないため、誤りです。
オプションDは、LAG 1にメンバーポートを追加したり、LAGインターフェースを有効にしたりしないため、誤りです。
参考文献：
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D

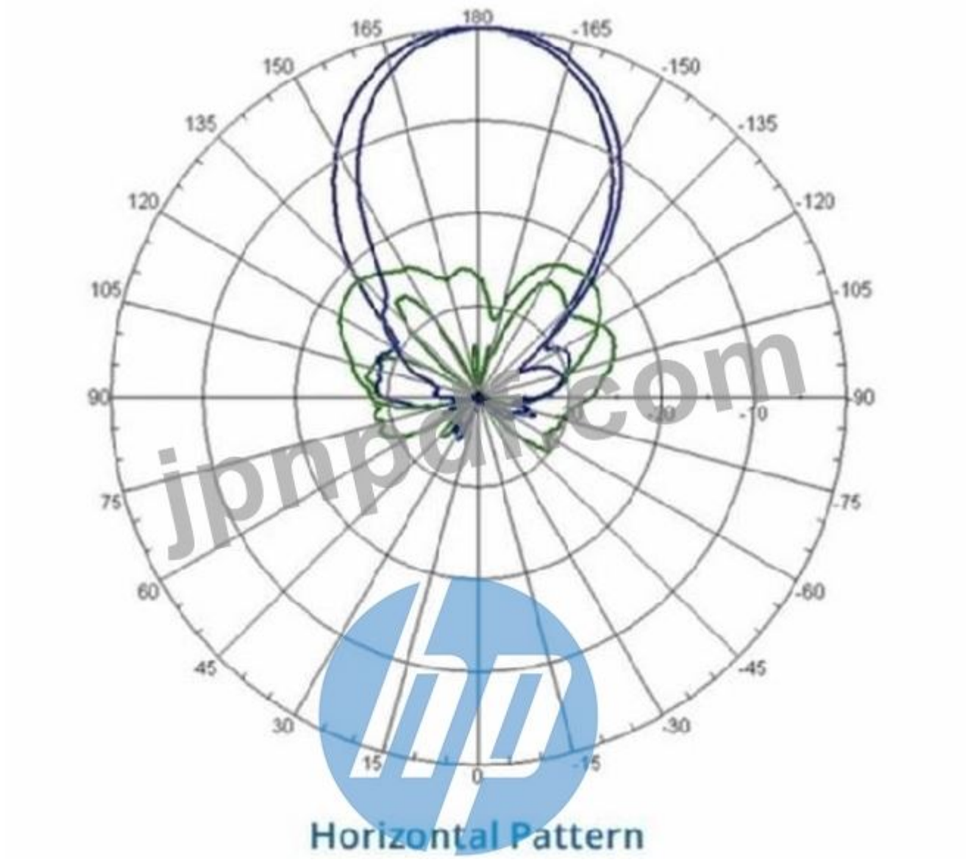
最新問題**: 65**
AP、ゲートウェイ、トラフィック転送モードが混合のAOS-10アーキテクチャにおいて、クライアントがVLAN割り当てがブリッジされるオープンな拡張SSIDに接続するとどうなりますか？
A. 認証付きディフィー ヘルマンは使用されていません
B. RADIUSプロトコルが使用されます。
C. 暗号化は適用されません。
D. ゲートウェイが応答しません。
Answer: C (メーッセージを残す**)**
AOS-10では、クライアントがオープン（暗号化されていない）拡張オープンSSIDに接続し、そのVLANがブリッジされている場合、クライアントとAP間のクライアントのトラフィックには暗号化は適用されません。
拡張オープン（OWE）は、クライアントとアクセスポイントの両方がそれをサポートしている場合にのみ暗号化を提供しますが、通常のオープンSSIDではこの保護は提供されません。

最新問題**: 66**
802.11kに関して正しいのはどれですか？
A. 無線測定を拡張し、無線局の無線ネットワーク管理のメカニズムを定義します。
B. クライアントがAPにローミングする前に、複数のターゲットAPでクライアントを事前認証することで、ローミング遅延を軽減します。
C. APとクライアントが利用可能な無線リソースを動的に測定するためのメカニズムを提供します。
D. クライアントを5GHz帯に誘導するかどうかを決定する前に、クライアントRSSIを含むいくつかの指標を考慮します。
Answer: C (メーッセージを残す**)**
802.11k は、アクセスポイント (AP) とクライアントが無線ネットワークで使用可能な無線リソースを動的に測定するためのメカニズムを提供する規格です。802.11k は、AP とクライアントが RF 環境に関する情報を交換し、より適切なローミング決定を行えるようにする、ネイバーレポート、リンク測定、ビーコンレポートなどの無線リソース管理 (RRM) 機能を定義しています。他のオプションは、802.11r、802.11v、802.11ax などの他の規格を説明しているため、誤りです。参考文献:
https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

最新問題**: 67**
Aruba CXスイッチ構成において、VSX構成で使用され、かつVSX構成に固有のアクティブゲートウェイ機能とは何ですか？
A. VLAN上ではVRRPとアクティブゲートウェイは相互に排他的です
B. VRIDはSVI VLAN IDとして自動的に設定されます
C. VRIDはVRRPと重複してはならない
D. VRRPとアクティブゲートウェイは、相互運用性のために単一のVLAN上で設定できます。
Answer: A (メーッセージを残す**)**

アクティブゲートウェイは、単一障害点を排除するファーストホップ冗長プロトコルです。アクティブゲートウェイ機能は、同じサブネット上のホストにサービスを提供するデフォルトゲートウェイの可用性を高めるために使用されます。アクティブゲートウェイは、仮想ルータをそのネットワークのデフォルトゲートウェイとして機能させることで、ホストネットワークの信頼性とパフォーマンスを向上させます。アクティブゲートウェイを有効にした場合、VRRPは不要です3。アクティブゲートウェイは、VSXノードからのルーティングトラフィックが仮想MACアドレス（VMAC）ではなくスイッチインターフェイスMACから発信されるという点でVRRPと似ています。各アクティブゲートウェイは、アクセススイッチ上のVMACのエイジングを回避するために、定期的にブロードキャストhelloパケットを送信します。スイッチは、アクティブゲートウェイIPを自己IPアドレスとして認識します3。VRRPではトラフィックがISLリンクを介してプッシュされるため、ネットワークに遅延が発生するため、アクティブゲートウェイの方がVRRPよりも推奨されます3。したがって、VLANではVRRPとアクティブゲートウェイは相互に排他的であり、回答Aが正解です。
参考文献 :1 :Aruba Campus Access のドキュメントと学習リソース 3 :VSX 上のアクティブゲートウェイ - Aruba

最新問題: **68**
画像を参照してください。お客様から、オフィス内のWi-Fi接続が弱いとの苦情が寄せられています。廊下を挟んだ反対側のオフィスでは、Wi-Fiの電波状況がはるかに良好とのことです。この問題の原因として考えられるのは何でしょうか？



A. APは無指向性アンテナを使用しています。
B. APは5GHzのみをサポートしています。
C. APはリモートアクセスポイントです。
D. APは指向性アンテナを使用しています。
Answer: D (メーッセージを残す)

極座標プロットは水平方向の放射パターンが集中していることを示しており、これはアクセスポイントが特定の方向（180°）に強い信号を発信し、その背後ではカバレッジが弱いことを示しています。この指向性集中により、廊下の反対側など、メインローブの経路から外れた場所では信号が弱くなります。

最新問題: **69**
Aruba CXスイッチ構成において、VSX構成で使用され、かつVSX構成に固有のアクティブゲートウェイ機能とは何ですか？
A. 合計16種類のVMACが共有としてサポートされています。
B. アクティブゲートウェイは、VLAN 負荷分散のために MSTP インスタンスが作成されると使用できます。
C. 各IPv4およびIPv6スタックに対して、16種類の異なるVMACSが同時にサポートされます。
D. 最適化されたパスのためにISLリンクを介してコピーされました。
Answer: C (メーッセージを残す)
アクティブゲートウェイ機能は、同一サブネット上のホストに対してアクティブ/アクティブレイヤ3デフォルトゲートウェイを提供するために使用されます。この機能により、スイッチはマルチキャストストリームを無線リンク上のユニキャストストリームに変換できるため、ストリーミングビデオの品質と信頼性が向上し、ビデオ以外のクライアントに利用可能な帯域幅が維持されます。アクティブゲートウェイ機能は、VRRPの必要性を排除し、ネットワークの遅延の原因となるISLリンクを経由したトラフィックの送信を回避するため、VSX構成に固有の機能です12。
正解はCです。IPv4スタックとIPv6スタックそれぞれで、同時に16種類のVMACがサポートされます。つまり、VSXペアでは、IPv4で最大8種類、IPv6で最大8種類のVMACを使用できます。6400スイッチシリーズ2では、15種類のVMACのみがサポートされます。
他の選択肢が間違っている理由は以下のとおりです。
A) 合計16種類のVMACは共有としてサポートされていません。これらはIPv4スタックとIPv6スタックそれぞれで個別にサポートされています。
B) アクティブゲートウェイは、MSTPインスタンスなしでも使用できます。MSTPは、同じスイッチ上で複数のスパニングツリーインスタンスが共存できるようにするプロトコルですが、アクティブゲートウェイの動作には影響しません。
D) アクティブゲートウェイは、最適化されたパスのためにISLリンクを介してトラフィックをコピーしません。ルーティングされたトラフィックにISLリンクを使用することを避け、送信元アドレス1に対して仮想MACアドレス（VMAC）の代わりにローカルスイッチインターフェイスMACを使用します。

最新問題: **70**
図を参照してください。従業員1,471名の企業が、AP-635アクセスポイントを200台導入しました。
6GHz帯を活用するため、管理者はHPE Aruba Networking Centralで新しいWPA3-OWE SSIDを設定しようと試みましたが、期待どおりに動作しません。
この問題を解決するための正しい手順は何でしょうか？

A. SSIDをWPA3-Enterprise (CNSA)に変更します。
B. SSIDをWPA3-Personalに変更します。
C. SSIDをWPA3-Enhanced Openに変更します。
D. SSIDをWPA3-Enterprise (CCM)に変更します。
Answer: (解答を表示する**)**
Aruba APでは、SSIDセキュリティ設定において、WPA3-OWEはWPA3-Enhanced Openと表記されます。6GHz帯でOpportunistic Wireless Encryption（OWE）を有効にするには、SSIDをWPA3またはWPA3-Personal/Enterpriseではなく、WPA3-Enhanced Openに設定してください。

最新問題**: 71**
システムエンジニアは、遠隔オフィスに送られる複数のAruba CX 6300スイッチを事前に設定する必要があります。訓練を受けていない現地のフィールド技術者が、スイッチの展開と複数のAP-515およびAP-575Sの設置を行います。APに接続されているケーブルにはラベルが貼られていません。
VLANは既にVLAN 100（管理）、VLAN 200（クライアント）、VLAN 300（ゲスト）に事前設定されています。アクセスポイントが正しく動作するようにするには、どのような設定を行うのが適切でしょうか？

A.
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc AP-515
    seq 20 match sys-desc AP-575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp vlan trunk native 100
    vlan trunk allowed 100,200,300
    enable
port-access device-profile IAP-Profile
    associate role IAP-Role
    associate lldp-group IAP-Group
```

B.
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    associate role IAP-Role
    associate lldp-group IAP-Group
    no shutdown
```

C.
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

D.
```
port-access lldp-group IAP-Group
    seq 10 match sys-desc 515
    seq 20 match sys-desc 575
port-access role IAP-Role
    description ARUBA AP
    poe-priority high
    trust-mode dscp
    vlan trunk native 100
    vlan trunk allowed 100,200,300
port-access device-profile IAP-Profile
    enable
    associate role IAP-Role
    associate lldp-group IAP-Group
```

Answer: C (メーッセージを残す)

オプション C は、AP が正しく動作するようにするための正しい構成です。ap コマンドを使用して、ネイティブ VLAN として VLAN 100、タグ付き VLAN として VLAN 200 と 300 を持つ AP 用のポート プロファイルを構成します。また、ポートで LLDP を有効にして AP を検出し、ポート プロファイルに自動的に割り当てます。他のオプションは、ap コマンドを使用していない、LLDP を有効にしていない、または VLAN を正しく構成していないため、正しくありません。参照: https://www.arubanetworks.com/techdocs/AOS- CX_10_08/UG/bk01-ch02.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch03.
HTML

最新問題**: 72**

クライアントは、デフォルトのAPグループ設定でトンネルモードに構成された802.1X SSIDに接続しています。

RADIUSサーバーからAccess-Acceptを受信した後、Aruba Gatewayはどのトンネルを通してアクセスポイントにAccess-Acceptを送信しますか？

A. IPsecトンネル

B. 分割トンネル

C. GREトンネル

D. PARトンネル

Answer: (解答を表示する)

Arubaのドキュメントポータル1によると、802.1Xはポートベースのネットワークアクセス制御の標準規格であり、RADIUSサーバーを使用して無線クライアントの認証と認可を行います。802.1Xは、ブリッジモード、トンネルモード、スプリットトンネルモードなど、さまざまなモードで構成できます。

オプションC :GREトンネル

これは、オプションCがArubaスイッチのデフォルトのAPグループ設定でトンネルモードでSSIDを構成する方法を示しているためです。トンネルモードでは、アクセスポイントからのすべてのクライアントトラフィックはコントローラにトンネルされ、コントローラはクライアントトラフィックをネットワーク2に転送します。GREプロトコルは、アクセスポイントとコントローラ3間のトラフィックのカプセル化とデカプセル化に使用されます。

したがって、選択肢Cが正解です。
1: https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7696/GUID-581D2976-694B-46C7-8497-F6B788AA05B2.html 2: https://community.arubanetworks.com/discussion/bridge-and-tunnel-mode 3: https://www.twingate.com/blog/ipsec-tunnel-mode

最新問題**: 73**
QoSを最も適切に説明しているのは、次のうちどれですか？
A. 指定された品質指標を満たすトラフィックを判定する
B. コンテンツの質に基づいてトラフィックをスコアリングする
C. 特別な処理が必要な特定の交通量を識別する
D. 接続品質の識別
Answer: A (メーッセージを残す**)**
QoS は Quality of Service の略で、ネットワーク デバイスがアプリケーション タイプ、送信元、宛先などの特定の基準に基づいてトラフィックの優先順位付けと区別を可能にするメカニズムです 3。QoS では、特別な処理が必要な特定のトラフィックを識別し、そのパフォーマンスを向上させたり、特定のサービス レベル契約 (SLA) を満たすためのポリシーとアクションを適用します 3。QoS は、ネットワーク デバイスがさまざまな種類のトラフィックの輻輳、遅延、ジッタ、パケット損失、帯域幅割り当てなどを管理するのに役立ちます 3。QoS は、ネットワーク スタックのさまざまなレイヤーとさまざまなネットワーク ドメインで実装できます。参照: 3 https://www.cisco.
com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mt-book/qos-overview.html

最新問題**: 74**
お使いのAruba CX 6300 VSFスタックは、隣接デバイスとの間でSVI 10、LAG 1のOSPF隣接関係を確立しています。
スイッチ上に以下の設定が作成されました。

```
interface vlan 20
     ip address 10.10.20.1/2
!
interface vlan 30
     ip address 10.10.30.1/2
!
interface vlan 40
     ip address 10.10.40.1/2
```

A.
```
vlan 20, 30,40
    ospf passive
interface vlan 20,30,40
```
B.
```
    ip ospf passive
router ospf 1
 area 0
 passive-interface
```
C.
```
    vlan 20.30.40
router ospf 1
    area 0
```
D.
```
        redistribute local
```
Answer: C (メーッセージを残す**)**
オプションCに、LAG 1を使用したSVI 10経由で隣接デバイスとのOSPF隣接関係を確立するための正しい設定を示します。
設定には以下の手順が含まれます。
* VLAN 10を作成し、名前とIPアドレスを割り当てます。

* LAG 1 を作成し、名前とモード（動的または静的）を割り当てます。
* LAG 1にメンバーポートを追加し、LAGインターフェースを有効にします。
* LAG 1 のタグなし VLAN として VLAN 10 を割り当てます。
* スイッチでOSPFを有効にし、ルーターIDを割り当てます。
* OSPFエリア0を作成し、そのエリアにSVI 10をインターフェースとして追加します。
オプションAは、スイッチ上でOSPFを有効にせず、OSPFエリアも作成しないため、誤りです。オプションBは、LAG 1のタグ付きVLANとしてVLAN 10を割り当てますが、これはSVI 10と互換性がないため、誤りです。
オプションDは、LAG 1にメンバーポートを追加したり、LAGインターフェースを有効にしたりしないため、誤りです。
参考文献：
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D

最新問題**: 75**
HPE Arubaのワイヤレスネットワークでは、動的マルチキャスト最適化（DMO）はどのように実装されていますか？
A. DMOは、ネットワークで使用されている各SSIDごとに個別に設定されます。
B. コントローラはマルチキャストストリームをユニキャストストリームに変換します。
C. APはOOSを使用してマルチキャストトラフィックに均等なエアタイムを提供します。
D. DMOは、ネットワークで使用されている各SSIDに対してグローバルに設定されます。
Answer: B (メーッセージを残す**)**

最新問題**: 76**
あなたは研究室で以下の機器仕様を用いて試験を実施しています。
* AP1は10 dBmの信号を生成する無線機を搭載しています。
* AP2は11dBmの信号を生成する無線機を搭載しています。
* AP1は9 dBiのゲインを持つアンテナを搭載しています。
* AP2は12dBiのゲインを持つアンテナを搭載しています。
* AP1のアンテナケーブルは2dBの損失があります
* AP2のアンテナケーブルは3dBの損失があります
APTの等価等方放射電力（EIRP）はどのくらいになるでしょうか？
A. 26 dBm
B. 30 dBm
C. 17 dBm
D. -12 dBm
Answer: B (メーッセージを残す**)**
説明
AP1 の計算された等価等方放射電力 (EIRP) は 30 dBm です。EIRP は、送信電力 (dBm) とアンテナ利得 (dBi) の積からケーブル損失 (dB) を差し引いたものです。AP1 の場合、EIRP = 10 dBm + 9 dBi - 2 dB = 17 dBm です。AP2 の場合、EIRP = 11 dBm + 12 dBi - 3 dB = 20 dBm です。参考文献:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/rf-fundam
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/eirp.htm

最新問題: **77**
無線デバイスがAP1からAP2へローミングする際、キー管理ワークフローにはどのような手順が含まれますか？ 2つ選択してください。）
A. AP1はクライアントの情報をキャッシュし、それを鍵管理サービスに送信します。
B. キー管理サービスは、AirMatchからAP2のすべてのネイバーのリストを受け取ります。
C. キー管理サービスは、AirMatchからAP1のすべてのネイバーのリストを受け取ります。
D. キー管理サービスは、AP2のネイバー用にR1キーを生成します。
E. クライアントはAP1からローミングした後、AP2と関連付け、認証を行う。
Answer: C,D (メーッセージを残す**)**
キー管理は、Aruba Mobility Controller（MC）またはMobility Master（MM）上で動作するサービスで、ワイヤレスクライアントのローミングパフォーマンスを最適化します。キー管理は、Aruba APの無線リソース管理を最適化するサービスであるAirMatchと連携し、クライアントがローミングする前に、近隣のAP向けにR1キーを事前生成して配布します。
無線デバイスがAP1からAP2へローミングする場合、以下の手順はキー管理ワークフローの一部となります。
* クライアントは、802.1XまたはPSK方式を使用してAP1と接続し、認証を行います。
* キー管理サービスはクライアントの情報をキャッシュし、クライアント用のR0キーを生成します。
* キー管理サービスは、AirMatchからAP1のすべての近隣ノードのリストを受け取ります。
* キー管理サービスは、R0キーを使用してAP1のネイバー用のR1キーを生成し、対応するAPに送信します。
* クライアントが AP1 の近隣の AP2 にローミングすると、再認証を必要とせずに、事前に生成された R1 キーを使用して 802.11r 高速トランジションを実行します。

最新問題: **78**
HPE Aruba Networkingスイッチにおける VXLANの実装に関して、正しい記述はどれですか？ 2つ選択してください。）
A. MTUサイズをデフォルト値より大きくする必要があります
B. VNIはVXLANトラフィックをカプセル化およびデカプセル化する
C. VTEPはVXLANトラフィックをカプセル化およびデカプセル化する。
D. データセンター用スイッチ（CX 8k、9k、10k）のみでご利用いただけます。
E. すべてのAOS-CXスイッチはVXLANをサポートしています。
Answer: A,C (メーッセージを残す**)**
VTEP（VXLANトンネルエンドポイント）は、送信元でレイヤ2フレームをVXLANパケットにカプセル化し、宛先でカプセル化を解除することで、レイヤ3ネットワーク上でレイヤ2接続を可能にする役割を担っています。
VXLANは各パケットに余分なヘッダーを追加するため、追加のカプセル化オーバーヘッドに対応し、断片化を防ぐために、MTUサイズを増やす必要があります（通常は少なくとも1550バイト以上）。

最新問題: **79**
Aruba CX 6300で、インターフェース1/1/1のデフォルト状態において、インターフェースにIPアドレス10 10 10 1を設定するにはどうすればよいですか？
A. int 1/1/1. スイッチング、IPアドレス 10 10 10 1/24
B. インターフェース 1/1/1。スイッチングなし、IPアドレス 10 10 10.1/24
C. int 1/1/1. ip address 10.10.10.1/24
D. int 1/1/1. ルーティング、IPアドレス 10.10.10 1/24
Answer: B (メーッセージを残す**)**

Aruba CX 6300 スイッチのインターフェイス 1/1/1 のデフォルト状態において、インターフェイスに IP アドレスを設定するには、まず no switching コマンドを使用してインターフェイスのスイッチングを無効にする必要があります。その後、ip address コマンドを使用して IP アドレスを割り当てることができます。他のオプションは、スイッチングを無効にしていないか、switching や routing などの無効なキーワードを使用しているため、正しくありません。参照: https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch01.html https://www.arubanetworks.com/techdocs/AOS-CX_10_08/UG/bk01-ch02.html

最新問題**: 80**
お客様は、老朽化したAruba 5406Rコアスイッチペア（スパニングツリー構成）をAruba CX 8360-32YCスイッチに置き換えるためのネットワークハードウェアの更新を必要としています。新しいソリューションでVSXクラスタリングを使用するメリットは何ですか？
A. スタック型データプレーン
B. より高速なMSTP収束処理
C. PoE冗長性のためのデュアルAruba AP LANポート接続
D. デュアル制御プレーンにより、より優れた耐障害性を実現
Answer: D (メーッセージを残す**)**
説明
VSXクラスタリングは、2台のAruba CXスイッチを単一の論理デバイスとして動作させる機能であり、高可用性、拡張性、および管理の簡素化を実現します。VSXクラスタリングは、スパニングツリー構成と比較して、次のような多くの利点があります。
デュアルコントロールプレーンにより、耐障害性が向上します。スイッチが単一のコントロールプレーンを共有するスタッキングとは異なり、VSXスイッチは独立したコントロールプレーンを備えており、スイッチ間リンク（ISL）を介して状態を同期します。つまり、一方のスイッチが故障または再起動した場合でも、もう一方のスイッチはトラフィックフローやネットワークサービスに影響を与えることなく動作を継続できます。
アクティブ/アクティブ転送方式は、より優れたパフォーマンスを提供します。ループを防ぐために一部のリンクをブロックするスパニングツリーとは異なり、VSXスイッチは利用可能なすべてのリンクを使用してトラフィックを転送するため、負荷分散と帯域幅利用率の向上を実現します。
マルチシャーシLAGは、より優れた冗長性を提供します。すべてのメンバーポートが1つのスイッチに属するシングルシャーシLAGとは異なり、VSXスイッチはダウンストリームまたはアップストリームデバイスとマルチシャーシLAGを形成でき、メンバーポートは両方のスイッチに分散されます。これにより、スイッチまたはポートの障害発生時に、リンクの冗長性とシームレスなフェイルオーバーが実現されます。
参考文献 :https://www.arubanetworks.com/assets/tg/TG_VSX.pdf

最新問題**: 81**
802.11kに関して正しいのはどれですか？
A. 無線測定を拡張し、無線局の無線ネットワーク管理のメカニズムを定義します。
B. クライアントがAPにローミングする前に、複数のターゲットAPでクライアントを事前認証することで、ローミング遅延を軽減します。
C. APとクライアントが利用可能な無線リソースを動的に測定するためのメカニズムを提供します。
D. クライアントを5GHz帯に誘導するかどうかを決定する前に、クライアントRSSIを含むいくつかの指標を考慮します。
Answer: C (メーッセージを残す**)**
説明
802.11k は、アクセスポイント (AP) とクライアントが無線ネットワークで使用可能な無線リソースを動的に測定するためのメカニズムを提供する規格です。802.11k は、AP とクライアントが RF 環境に関する情報を交換し、より適切なローミング決定を行えるようにする、ネイバーレポート、リンク測定、ビーコンレポートなどの無線リソース管理 (RRM) 機能を定義しています。他のオプションは、802.11r、802.11v、802.11ax などの他の規格を説明しているため、誤りです。参考文献:
https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

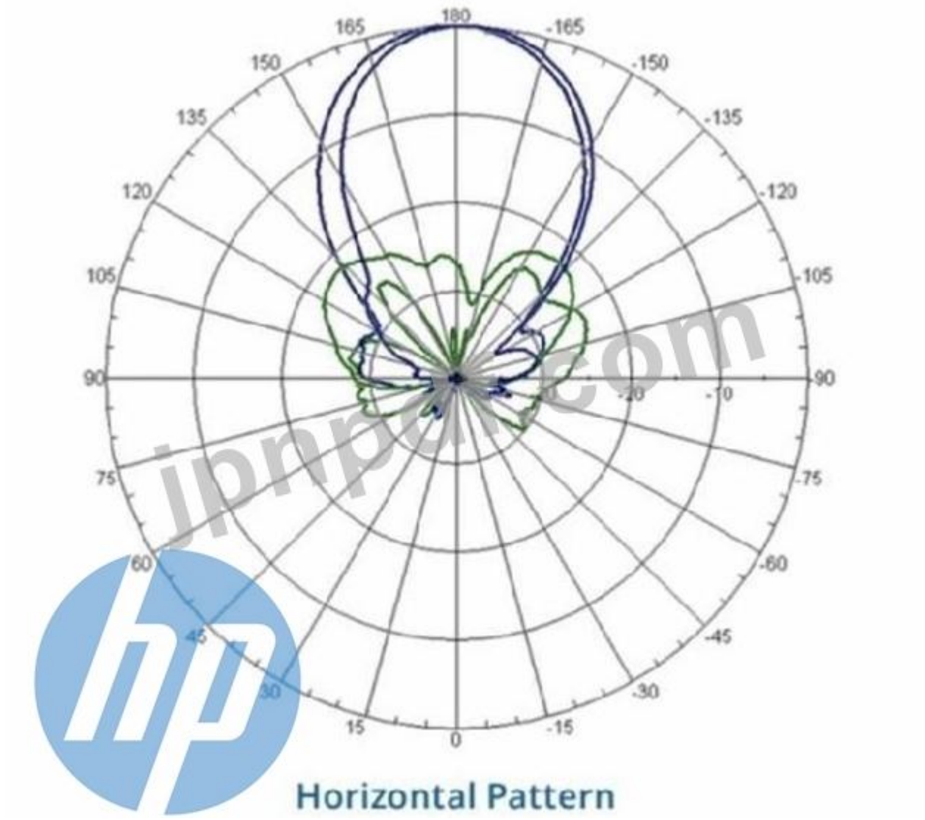
最新問題**: 82**
お客様から、新規ユーザーにスイッチ管理ロールを割り当てるよう依頼がありました。お客様は、ユーザーロールがWeb UIのSystem > Logページへのアクセスのみを持ち、/logs/eventリソースのREST APIに対してGETメソッドのみにアクセスできることを要求しています。これらの要件を満たすデフォルトのAOS-CXユーザーロールはどれですか？

A. 管理者
B. 監査役
C. システムオペレーター
D. 演算子
Answer: B (メーッセージを残す**)**
監査担当者ロールは、Web UI の [システム] > [ログ] ページへのアクセス権限と、/logs/event リソースの REST API の GET メソッドへのアクセス権限という要件を満たす、AOS-CX のデフォルトユーザーロールです。監査担当者ロールのレベルは 1 であり、セキュリティやパスワードに関連するコマンドを除くほとんどのコマンドに対して読み取り専用アクセスを許可します。また、Web UI および REST API へのアクセス権限も制限付きで許可します。他のオプションは、アクセスレベルが高すぎるか、Web UI または REST API へのアクセスを許可しないため、不適切です。
参考文献：
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch01.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch04.html

最新問題**: 83**
ある企業が最近、複数の支店に新しいArubaアクセスポイントを導入しました。無線LANの802.1X認証は、クラウド上のRADIUSサーバーに対して行われます。セキュリティチームは、アクセスポイントとRADIUSサーバー間の通信が外部に漏洩するのではないかと懸念しています。
この状況における適切な解決策は何でしょうか？
A. すべての無線機器でEAP-TLSを有効にする
B. APとAruba CentralでRadSecを設定します。
C. すべての無線デバイスでEAP-TTLSを有効にする。
D. APとRADIUSサーバーでRadSecを設定する
Answer: (解答を表示する**)**
これは、無線802.1X認証がクラウド内のRADIUSサーバーに対して行われ、セキュリティチームがAPとRADIUSサーバー間のトラフィックが漏洩することを懸念しているシナリオに適したソリューションです。RadSec（RADIUS over TLSとも呼ばれる）は、TCPおよびTLS上でRADIUSトラフィックの暗号化と認証を提供するプロトコルです。RadSecは、APとRADIUSサーバーの両方で構成でき、RADIUSパケットを交換するための安全なトンネルを確立できます。他のオプションは、RADIUSトラフィックの暗号化または認証を提供しないか、RadSecを使用していないため、不適切です。参照 :https://www.securew2.com/blog/what-is-radsec/
https://www.cloudradius.com/radsec-vs-radius/

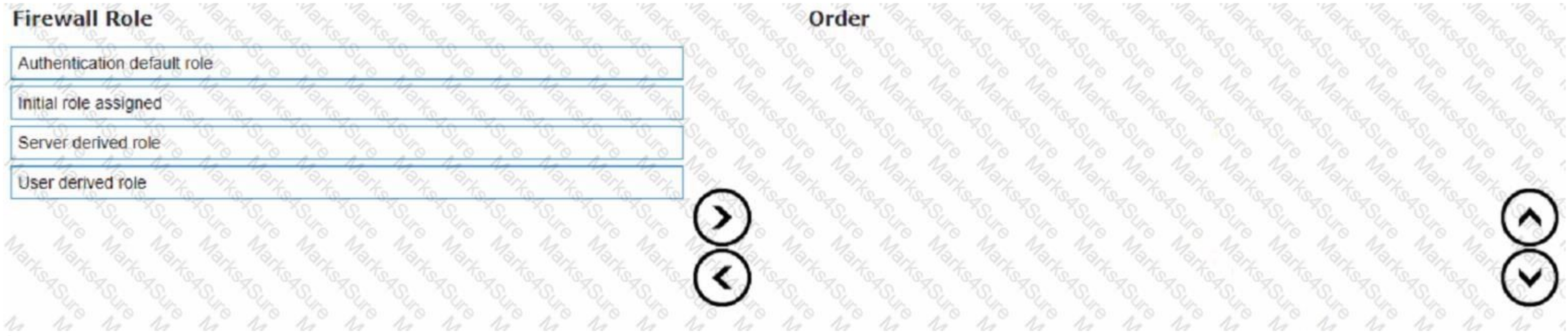
最新問題**: 84**
HPE Arubaワイヤレスネットワークでは、マルチキャスト伝送最適化はどのように実装されていますか？
A. 「マルチキャストフレームを送信する最適なレートは、関連するすべてのクライアント間での最高ブロードキャストレートに基づいています。」
B. このオプションを有効にすると、マルチキャストトラフィックの最小デフォルトレートは5GHz帯で12Mbpsに設定されます。
C. マルチキャストフレームを送信する最適なレートは、関連するすべてのクライアントの中で最も低いブロードキャストレートに基づいています。
D. マルチキャストフレームを送信する最適なレートは、関連するすべてのクライアントの中で最も低いユニキャストレートに基づいています。
Answer: D (メーッセージを残す**)**
マルチキャスト送信最適化は、IAPが関連するすべてのクライアント1におけるユニキャストレートの中で最も低いレートに基づいて、ブロードキャストフレームとマルチキャストフレームの送信に最適なレートを選択できる機能です。このオプションを有効にすると、マルチキャストトラフィックを最大24Mbpsで送信できます。2.4GHz帯のフレーム送信のデフォルトレートは1Mbps、5.0GHz帯は6Mbpsです。このオプションはデフォルトでは無効になっています1。

最新問題**: 85**
画像を参照してください。お客様から、オフィス内のWi-Fi接続が弱いとの苦情が寄せられています。廊下を挟んだ反対側のオフィスでは、はるかに良好な信号が受信できるとのことです。
この問題の考えられる原因は何ですか？

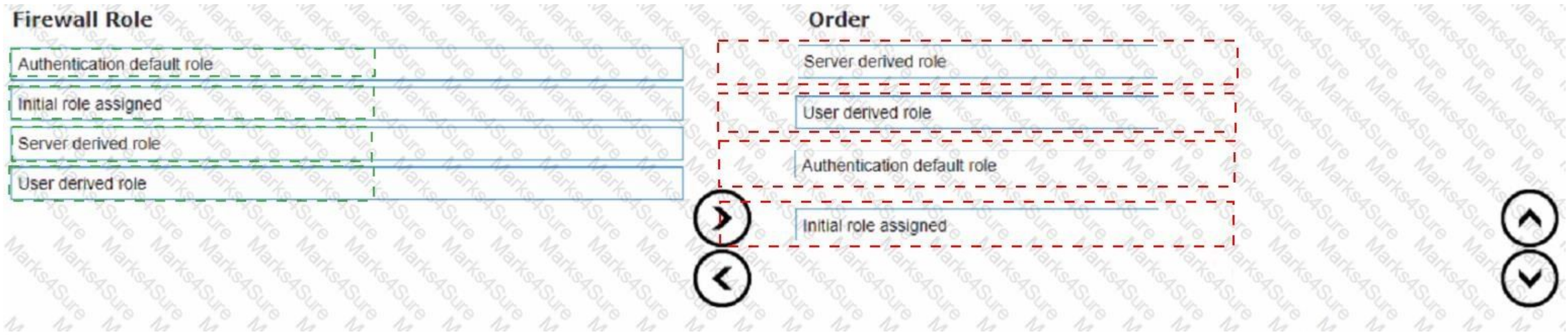


A. APはリモートアクセスポイントです。
B. APは指向性アンテナを使用しています。
C. APは屋外アクセスポイントです。
D. APはメッシュモードで設定されています。
Answer: B (メーッセージを残す**)**
オフィス内のWi-Fi接続が弱い原因として考えられるのは、アクセスポイントが指向性アンテナを使用していることです。
指向性アンテナとは、電波を特定の方向に強く放射または受信し、集中した信号ビームを生成するアンテナです。指向性アンテナは特定のエリアの通信範囲とパフォーマンスを向上させることができますが、他のエリアではデッドゾーンや弱点が生じる可能性もあります。その他の選択肢は、Wi-Fiの通信範囲に影響を与えないか、状況に合致しないため、誤りです。

最新問題**: 86**
ファイアウォールロールの派生フローを正しい順序で列挙してください。



Answer:



説明

Arubaドキュメントポータル1によると、ファイアウォールロールの導出フローは正しい順序で次のようになります。

* サーバー由来のロール
* ユーザー由来のロール
* 認証のデフォルトロール
* 開始役が割り当てられました

最新問題: **87**

Aruba OS CXスイッチにおけるSPFv2ルート再配布に関する記述のうち、正しいものはどれですか？ 2つ選択してください。）

A. 「redistribute connected」コマンドは、ローカルループバックアドレスを含む、スイッチのすべての接続済みルートを再配布します。

B. 「redistribute ospf」コマンドは、すべてのOSPF V2およびV3プロセスからのルートを再配布します。

C. 「redistribute static route-map connected-routes」コマンドは、ルートマップ 「connected-routes」内で一致する拒否がないすべての静的ルートを再配布します。

D. "redistribute connected"コマンドは、ローカルループバックアドレスを除く、スイッチのすべての接続済みルートを再配布します。

E. "redistribute static route-map connected-routes"コマンドは、ルートマップ "connected-routes-

Answer: (解答を表示する)

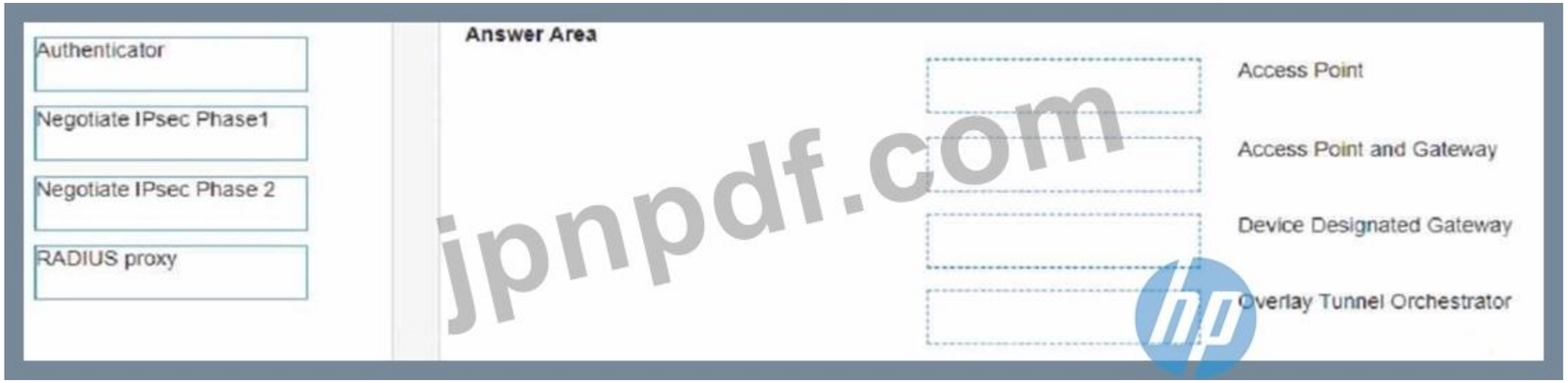
以下は、Aruba OS CX スイッチの OSPFv2 ルート再配布に関する正しい記述です。ルート再配布とは、あるルーティング プロトコルまたは送信元からのルートを別のルーティング プロトコルまたは宛先に挿入するプロセスです。OSPFv2 は、接続、スタティック、BGP など、さまざまな送信元からのルート再配布をサポートするリンク ステート ルーティング プロトコルです。"redistribute connected"コマンドは、ローカル ループバック アドレスを含む、スイッチのすべての接続ルートを OSPFv2 に再配布します。"redistribute static route-map connected-routes"コマンドは、"connected-routes"という名前のルート マップに一致する permit ステートメントを持つすべてのスタティック ルートを OSPFv2 に再配布します。その他の記述は、ルート再配布コマンドの正しい動作を反映していないか、有効なコマンドとして存在しないため、誤りです。

参考文献 :https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.htmlhttps://

最新問題**: 88**

ドラッグアンドドロップ問題

APとゲートウェイ間のAOS10トンネルモード設定のトピックを一致させてください。オプションは複数回使用することも、まったく使用しないことも可能です。)



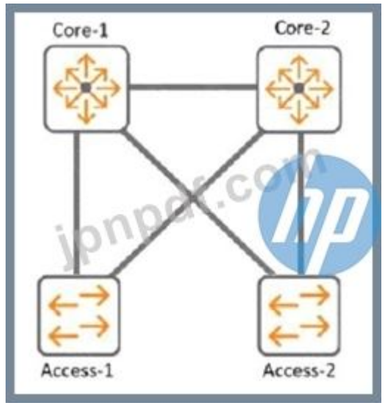
Answer:

最新問題**: 89**

顧客は、レイヤー2で通信するレガシーアプリケーションを使用しています。顧客はこのアプリケーションを、レイヤー3で接続されたリモートサイトでも引き続き動作させたいと考えています。すべてのレガシーデバイスは、各サイトに設置された専用のAruba CX 6200スイッチに接続されています。

Aruba CX 6200のどの技術を使えば、この要件を満たすことができるでしょうか？
A. インクルーシブマルチキャストイーサネットタグ（IMET）
B. イーサネット・オーバー・IP（EoIP）
C. 汎用ルーティングカプセル化 (GRE)
D. スタティックVXLAN
Answer: D (メーッセージを残す)
VXLANは、レイヤ3ネットワーク上でレイヤ2通信を行うレガシーアプリケーションを使用するという要件を満たすために利用できるテクノロジーです。スタティックVXLANは、VXLANトンネルを使用してレイヤ3アンダーレイネットワーク上にレイヤ2オーバーレイネットワークを作成できる機能です。スタティックVXLANは、制御プレーンプロトコルやVTEP検出メカニズムを必要とせず、Aruba CX 6200スイッチで手動で設定できます。その他のオプションは、レイヤ3ネットワーク上でのレイヤ2通信をサポートしていないか、Aruba CX 6200スイッチでサポートされていないため、正しくありません。

最新問題**: 90**
ポート 1/45 と VSX ペア inter-switch-link 256 間で新しい VLAN 100 を許可するにはどうすればよいですか
2/45?
A. ポート1/45および1/46に対してVLANトランク100を許可します
B. vlan trunk add 100 in LAG256
C. LAG256 で VLAN トランク 100 を許可
D. vlan trunk add 100 in MLAG256
Answer: C (メーッセージを残す)
ポート1/45と2/45のVSXペア間インタースイッチリンク256で新しいVLAN 100を許可するには、LAG256でvlan trunk allowed 100コマンドを使用する必要があります。これにより、VSXピア間のインタースイッチリンクの一部であるトランクポートLAG256の許可VLANリストにVLAN 100が追加されます。他のオプションは、正しいコマンドを使用していないか、正しいポートまたはVLANを指定していないため、正しくありません。

最新問題**: 91**
添付資料を参照してください。


Access-1を使用する場合、VLANの負荷分散を行うためにMSTPと同一に設定する必要があるものは何ですか？
A. スパニングツリー bpdu-guard 設定
B. スパニングツリーインスタンスVLANマッピング
C. スパニングツリーCistマッピング
D. 樹木根止めガード設置
Answer: B (メーッセージを残す)

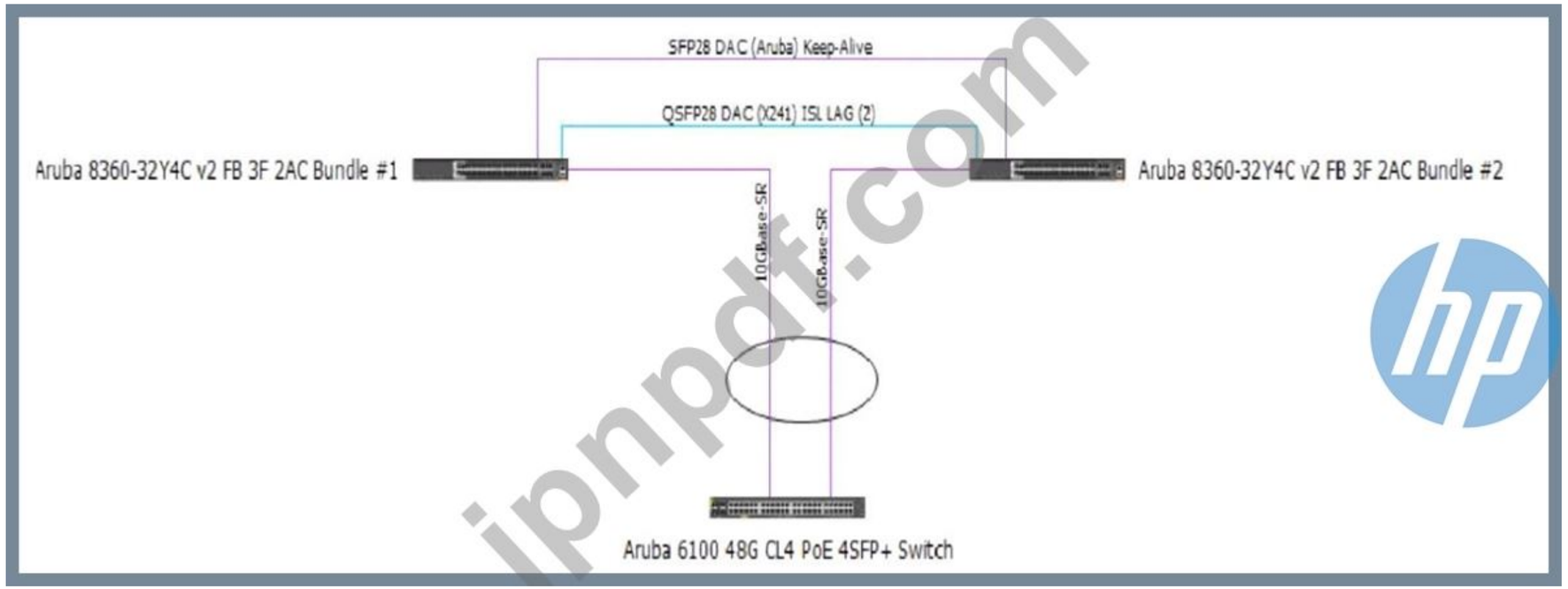
正解はBです。スパニングツリーインスタンスのVLANマッピング。
MSTPを使用してVLANの負荷分散を行うには、同じMSTリージョン内のすべてのスイッチで、同じVLANとインスタンスのマッピングを設定する必要があります。つまり、異なるMSTインスタンスに異なるVLANを割り当て、各インスタンスのスパニングツリーパラメータ（優先度、コスト、ポートロールなど）を調整して、目的の負荷分散を実現する必要があります。たとえば、1つのスイッチをインスタンス1のルート、別のスイッチをインスタンス2のルートに設定し、VLANの半分をインスタンス1に、残りの半分をインスタンス2にマッピングすることができます。
Ciscoのドキュメント「マルチプルスパニングツリープロトコル（802.1s）の理解」によると、MSTを設定する手順の1つは次のとおりです。
* VLAN のセットを複数のインスタンスに分割し、それぞれのインスタンスに対して異なる MST 設定を構成します。これを容易に実現するには、ブリッジ D1 を VLAN 501 ～ 1000 のルートに、ブリッジ D2 を VLAN 1 ～ 500 のルートに選択します。この構成では、次の記述が当てはまります。
Switch D1(config)#spanning-tree mst 設定
スイッチD1(config-mst)#instance 1 vlan 501-1000
Switch D1(config-mst)#exit
Switch D1(config)#spanning-tree mst 1 priority 0
Switch D2(config)#spanning-tree mst 設定
スイッチD2(config-mst)#instance 2 vlan 1-500
Switch D2(config-mst)#exit
Switch D2(config)#spanning-tree mst 2 priority 0
上記のコマンドは、MSTインスタンス1と2の2つを作成し、VLAN 501～1000をインスタンス1に、VLAN 1～500をインスタンス2にマッピングします。次に、スイッチD1をインスタンス1のルートに、スイッチD2をインスタンス2のルートに設定します。
他の選択肢が間違っている理由は以下のとおりです。
* A. スパニングツリーのbpdu-guard設定は、不正なデバイスからBPDUを受信した場合、ポートを無効にするセキュリティ機能です。MSTPによるロードバランシングには影響しません。
* C. スパニングツリーCISTマッピングは有効なコマンドではありません。CISTはCommon and Internal Spanning Treeの略で、MST領域内で実行され、他の領域または非MSTスイッチとやり取りするスパニングツリーインスタンスです。
* D. スパニングツリーのルートガード設定は、別のスイッチから上位のBPDUを受信したポートがルートポートになるのを防ぐセキュリティ機能です。MSTPによるロードバランシングには影響しません。

最新問題: **92**
セキュリティ担当ディレクターから、新規採用社員の職務要件に基づいてAOS-CXスイッチの管理ロールを割り当てるよう指示されました。設定完了後、監査ロールを割り当てられたユーザーにスイッチへの適切なアクセス権限がないことが判明しました。このユーザーはファームウェアのアップグレードを実行できず、ロールに特権レベル15が割り当てられていませんでした。このユーザーにはどのデフォルト管理ロールを割り当てるべきだったでしょうか？
A. システム管理者
B. システムオペレーター
C. 管理者
D. 設定
Answer: (解答を表示する)
sysopsユーザーロールは、バックアップ、復元、アップグレード、再起動など、スイッチ上でシステム操作を実行できる事前定義済みのロールです。また、sysopsユーザーロールは、スイッチ構成の変更に使用できるREST APIのPUTメソッドとPOSTメソッドにもアクセスできます。
システムオペレーターのユーザーロールには、スイッチ上で最も高いアクセス権限レベルである15の特権レベルが付与されています。

最新問題: **93**
顧客は、レイヤー2で通信するレガシーアプリケーションを使用しています。顧客はこのアプリケーションを、レイヤー3で接続されているキャンパス全体で引き続き動作させたいと考えています。レガシーデバイスは、キャンパス全体に設置されたAruba CX 6300スイッチに接続されています。
どの技術が洪水を最小限に抑え、既存アプリケーションが効率的に動作することを可能にするのでしょうか？
A. 汎用ルーティングカプセル化 (GRE)
B. EVPN-VXLAN
C. Ethernet over IP (EoIP)
D. スタティックVXLAN
Answer: B (メーッセージを残す**)**
EVPN-VXLANは、イーサネットVPN（EVPN）を制御プレーン、仮想拡張LAN（VXLAN）をデータプレーンとして使用することで、レイヤ3ネットワーク間でレイヤ2通信を可能にする技術です3。EVPN-VXLANは、レイヤ3で接続された異なるキャンパスやデータセンター間でレイヤ2通信を行うレガシーアプリケーションをサポートするために使用できます。EVPN-VXLANは、BGPを使用してホストのMACアドレスとIPアドレスを異なるVXLANセグメントに分散することで、フラッディングを最小限に抑えます3。EVPN-VXLANは、ループ防止、負荷分散、モビリティ、スケーラビリティなどのメリットも提供します3。参考文献 :3
https://www.arubanetworks.com/assets/tg/TG_EVPN_VXLAN.pdf

最新問題: **94**
VSX LAGについて正しい記述はどれですか？（2つ選択してください。）
A. 設定可能なリンクの総数は、ペアで8個、スイッチ1台で4個を超えてはなりません。
B. 送信トラフィックは、ペアのスイッチのいずれかのハッシュアルゴリズムに基づいてポートに切り替えられます。
C. スイッチペアのファームウェアをアップグレードしている間は、LAGトラフィックはVSX ISLリンクのみを介して転送されます。
D. 発信トラフィックは、LAG のローカルメンバーに優先的に切り替えられます。
E. 83xxおよび84xxモデルのスイッチでは、最大255のVSXラグを設定できます。
Answer: A,D (メーッセージを残す**)**
正解はAとDです。
ウェブ検索結果によると、VSX LAGは、1つのSSIDで複数のPSKを使用できるようにする機能であり、ヘッドレスIoTデバイスのセキュリティと展開の柔軟性を高めるために、デバイス固有またはグループ固有のパスフレーズを提供します1。VSX LAGは両方の集約スイッチにまたがり、VSXペアでLAGを形成する際に、下流または上流のデバイス、あるいはその両方と連携する1つのデバイスとして表示されます2。
VSX LAGに関する正しい記述の1つは、設定可能なリンクの総数が上限を超えてはならないということです。
ペアで 8、スイッチごとに 4 です 1。これは、ダウンストリーム スイッチをまたぐ VSX LAG には最大で合計 8 つのメンバ リンクがあり、スイッチには最大 4 つのメンバ リンクがあることを意味します。VSX LAG を作成する際には、負荷分散のために各セグメントで同数のメンバー リンクを選択することをお勧めします 1。
VSX LAGに関してもう一つ確かなことは、送信トラフィックはLAG2のローカルメンバーに優先的に切り替えられるということです。つまり、アクティブフォワーディングとアクティブゲートウェイが有効になっている場合、南北方向および南北方向のトラフィックはISLリンクをバイパスし、スイッチのローカルポートを使用します。これにより、トラフィックパスが最適化され、ISLリンク2の負荷が軽減されます。
その他の記述は誤りであるか、VSX LAG には関係ありません。送信トラフィックはハッシュアルゴリズムに基づいてポートに切り替えられるわけではなく、ペアのどちらかのスイッチになる場合もあります。これは MLAG (マルチシャーシリンクアグリゲーション) の特徴であり、VSX LAG とは異なる機能です。LAG トラフィックは、スイッチペアのファームウェアをアップグレードしている間だけ VSX ISL リンクを介して転送されません。これは、ネットワークの可用性に影響を与えずにソフトウェアを更新できる機能である無停止アップグレードを実行するときに発生する可能性のあるシナリオです。すべての 83xx および 84xx モデルのスイッチで構成できる VSX ラグの数は 255 ではなく、スイッチのモデルとファームウェアのバージョンによって異なります。たとえば、AOS-CX 10.04 では、8320 スイッチで最大 64 の VSX ラグ、8325 および 8400 スイッチで最大 128 の VSX ラグがサポートされます。

最新問題: **95**
展示内容を確認してください。



Aruba CX 8360 スイッチのペアで Tor ワイヤレス クライアントが使用する VLAN 1000 でもある 10 102.39 0/24 サブネットに関する問題のトラブルシューティングを行っています。サブネット SVI は 8360 ペアで構成されており、DHCP サーバーは IP アドレス 10 200 1.100 の Microsoft Windows Server 2022 Standard です。10.102.250.0/24 サブネットはスイッチ管理に使用されます。
多数のDHCPリクエストが失敗しています。CX 6100スイッチに接続されているクライアント全体で、DHCPの動作が断続的になっていることが確認されています。
どの対策が問題解決に役立つでしょうか？

Enter the following commands on the VSX primary switch:

```
vsx
vsx-sync dhcp-relay
exit
```

A.

Enter the following commands on the VSX secondary switch:

```
vlan 1000
ip relay-address 10.200.1.100
exit
```

B.

C. Add an SVI in the 10.102.39.0/24 subnet on the Aruba CX 6100 switch that the APs are connected to.
Enter the following commands on the Aruba CX 6100 switch:

```
interface vlan 1000
ip helper-address 10.200.1.100
exit
```

D.

Answer: C (メーッセージを残す)
説明
オプションCは、CX 8360スイッチのVLAN 1000のSVIでDHCPリレーを設定する唯一の操作です。DHCPリレーは、スイッチが1つのサブネット内のクライアントからのDHCP要求を別のサブネット内のDHCPサーバーに転送できるようにする機能です。DHCPサーバーとクライアントが同じブロードキャストドメイン1にない場合、DHCPリレーが必要です。
オプションCでは、以下のコマンドを使用します。
interface vlan 1000: このコマンドは、IPアドレスが10.102.39.1/24で、無線クライアントに使用されるVLAN 1000のSVIのインターフェース設定モードに入ります。

ip helper-address vrf default 10.200.1.100: このコマンドは、DHCP サーバーの IP アドレスを SVI のヘルパー アドレスとして設定します。つまり、スイッチは VLAN 1000 上のクライアントからの DHCP 要求をこのアドレスに転送します。vrf default パラメータは、SVI と DHCP サーバーが同じ VRF に属していることを示します。

最新問題**: 96**
経営情報データベース（MIS）に保存されているデータを取得するには、何を使用しますか？
A. SNMPv3
B. DSCP
C. TLV
D. CDP
Answer: A (メーッセージを残す**)**
正解はA. SNMPv3です。
SNMPv3は、ネットワーク上の管理対象オブジェクトのデータベースである管理情報ベース（MIB）に格納されたデータを取得するために使用されるプロトコルです。SNMPv3は、以前のバージョンのSNMPにはなかったセキュリティ機能とアクセス制御機能を提供します。また、SNMPv3は暗号化を使用して、不正アクセスや改ざんからデータを保護することもできます。
Aruba認定プロフェッショナル - キャンパスアクセスに関する文書1によると、この認定資格が証明するスキルの1つは次のとおりです。
* 一般的なネットワーク監視ツールの出力を実装および分析する
PCAPを収集するようにポートミラーリングを設定します。
* NAEエージェント9.4の設定
* UXIセンサーを内部テストと外部テスト用に構成する
* API スキャンを使用してネットワークを構成、管理、監視、トラブルシューティングする方法を説明します。この文書では、候補者はベンダー間のさまざまなプロトコルについて優れた理解を持っている必要があるとも述べられており、これは、SNMPv3 と、それを使用して MIB データにアクセスする方法に精通している必要があることを意味します。

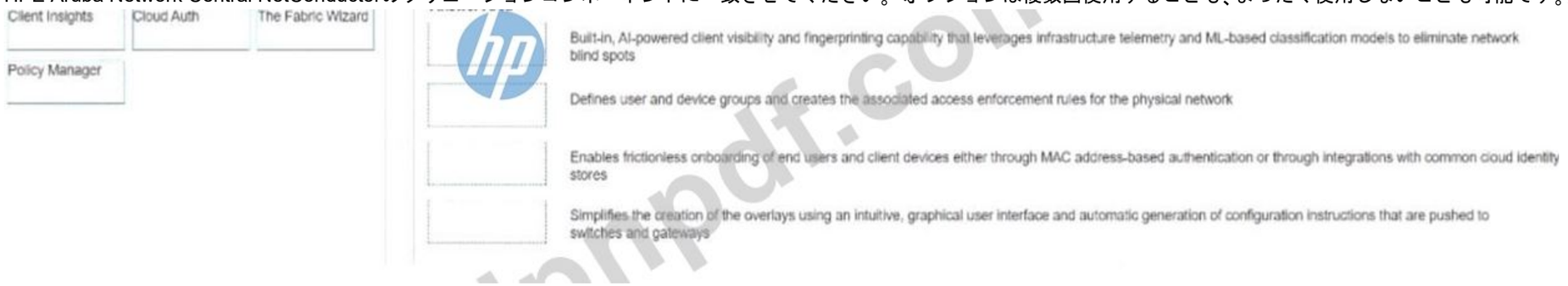
最新問題**: 97**
SNMPv3がサポートする機能のうち、SNMPv2cよりも優れている点はどれですか？
A. 交通マッピング
B. コミュニティストリングス
C. ゲットバルク
D. 暗号化
Answer: D (メーッセージを残す**)**
暗号化はSNMPv3でサポートされている機能であり、SNMPv2cよりも優れています。暗号化は、SNMPメッセージを秘密鍵で暗号化することで、メッセージの機密性と完全性を保護します。SNMPv2cは暗号化をサポートしておらず、認証と認可にコミュニティ文字列を使用しますが、これは平文で送信されるため、容易に傍受または偽装される可能性があります。トランスポートマッピング、コミュニティ文字列、およびGetBulkは、SNMPv2cとSNMPv3の両方に共通する機能です。参照 :https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmp.htm
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmpv3.htm

最新問題**: 98**
VSX LAGについて正しい記述はどれですか？ （2つ選択してください。）
A. 設定可能なリンクの総数は、ペアで8個、スイッチ1台で4個を超えてはなりません。
B. 送信トラフィックは、ペアのスイッチのいずれかのハッシュアルゴリズムに基づいてポートに切り替えられます。
C. スイッチペアのファームウェアをアップグレードしている間は、LAGトラフィックはVSX ISLリンクのみを介して転送されます。
D. 発信トラフィックは、LAG のローカルメンバーに優先的に切り替えられます。
E. 83xxおよび84xxモデルのスイッチでは、最大255のVSXラグを設定できます。

Answer: B,D (メッセージを残す)
説明
VSX LAGは、Aruba CXスイッチのペアがダウンストリームまたはアップストリームデバイスとマルチシャーシLAGを形成できる機能です。VSX LAGは、2台のスイッチ間でリンク冗長性と負荷分散を提供します。VSXペアからピアデバイスへの送信トラフィックは、送信元および宛先MACアドレス、IPアドレス、ポートなどのさまざまなパラメータを考慮したハッシュアルゴリズムに基づいてポートに切り替えられます。ハッシュアルゴリズムは、トラフィック特性に応じて、ペア内のいずれかのスイッチに属するポートを選択する場合があります1。ただし、送信トラフィックはLAGのローカルメンバーに優先的に切り替えられます。つまり、各スイッチはISLリンクを使用して他のスイッチのポートにトラフィックを送信する前に、まず自身のポートを使用しようとします2。これにより、ISLの使用率が低減され、パフォーマンスが向上します。参考文献 :1
https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7888/Content/VSX_cmds/int-lag-mul-c
2
https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7888/Content/Chp_Start/vsx-lag-10.11.

最新問題**: 99**
Aruba OS CXスイッチにおけるOSPFv2ルート再配布に関する記述のうち、正しいものはどれですか？
（2つ選択してください。）
A. ｢redistribute connected｣コマンドは、ローカルループバックアドレスを含む、スイッチのすべての接続済みルートを再配布します。
B. ｢redistribute ospf｣コマンドは、すべてのOSPF V2およびV3プロセスからのルートを再配布します。
C. ｢redistribute static route-map connected-routes｣コマンドは、ルートマップ ｢connected-routes｣内で一致する拒否がないすべての静的ルートを再配布します。
D. ｢redistribute connected｣コマンドは、ローカルループバックアドレスを除く、スイッチのすべての接続済みルートを再配布します。
E. ｢redistribute static route-map connected-routes｣コマンドは、ルートマップ ｢connected-routes-
Answer: A,E (メッセージを残す)
これらは、Aruba OS CX スイッチの OSPFv2 ルート再配布に関する 2 つの正しい記述です。ルート再配布とは、あるルーティング プロトコルまたはソースからのルートを別のルーティング プロトコルまたは宛先に注入するプロセスです。OSPFv2 は、接続、スタティック、BGP など、さまざまなソースからのルート再配布をサポートするリンク ステート ルーティング プロトコルです。
｢redistribute connected｣コマンドは、ローカルループバックアドレスを含む、スイッチのすべての接続済みルートをOSPFv2に再配布します。｢redistribute static route-map connected-routes｣コマンドは、｢connected-routes｣という名前のルートマップに一致する許可ステートメントを持つすべての静的ルートをOSPFv2に再配布します。その他の記述は、ルート再配布コマンドの正しい動作を反映していないか、有効なコマンドとして存在しないため、誤りです。

最新問題**: 100**
HPE Aruba Network Central NetConductorのソリューションコンポーネントに一致させてください。（オプションは複数回使用することも、まったく使用しないことも可能です。）



Answer:

Explanation: