

HP.HPE6-A85.v2026-08-24.q134

試験コード:	HPE6-A85
試験名称:	Aruba Certified Campus Access Associate Exam
認定資格:	HP
無料問題数:	134
バージョン:	v2026-08-24
アクセス数:	103
ページビュー数:	1340
https://www.jpnpdf.com/HP.HPE6-A85.v2026-08-24.q134-mondaishu.html	

最新問題: 1

どのArubaテクノロジーを使えば、デバイス固有のパスフレーズを使用して、ヘッドレスデバイスを安全にWLANに追加できますか？

- A. 有線等価プライバシー WEP)
- B. 複数事前共有鍵 MPSK)
- C. 機会的無線暗号化 (OWE)
- D. 一時的鍵完全性プロトコル TKIP)

Answer: B ([メッセージを残す](#))

説明

マルチプル事前共有キー (MPSK) は、デバイス固有またはグループ固有のパスフレーズを使用して、ヘッドレス デバイスを WLAN 無線ローカル エリア ネットワークに安全に追加できる機能です。WLAN は、無線通信を使用して 2 台以上のデバイスを接続し、家庭、学校、コンピュータ ラボ、キャンパス、オフィス ビルなどの限られたエリア内でローカル エリア ネットワーク (LAN) を形成する無線コンピュータ ネットワークです。MPSK は、同じ SSID (サービス セット識別子) 上の異なるデバイスに異なる PSK を許可することで、WPA2 PSK (Wi-Fi Protected Access 2 事前共有キー) モードを強化します。WPA2 PSK は、オプションの事前共有キー (PSK) 認証を使用して WPA2 を使用してネットワークを保護する方法で、エンタープライズ認証サーバーを持たない家庭ユーザー向けに設計されています。SSIDは、モバイルデバイスがIEEEの基本サービスセット BSS)に接続しようとする際にパスワードとして機能します。

802.11 WLANアーキテクチャ。MPSKパスワードは生成またはユーザー作成が可能で、ClearPass Policy Manager12によって管理されます。参考文献：

<https://blogs.arubanetworks.com/solutions/simplify-iot-authentication-with-multiple-pre-shared-keys/> 2

<https://www.arubanetworks.com/techdocs/ClearPass/6.8/Guest/Content/AdministrationTasks1/Configuring-MPS>

最新問題: 2

ノイズフロアは000000001ミリワット、受信機の信号強度は-65dBm です。信号対雑音比はいくらですか？

- A. 35 dBm
- B. 15 dBm
- C. 45 dBm
- D. 25 dBm

Answer: ([解答を表示する](#))

説明

信号対雑音比 \$NR)は、目的信号のレベルと背景雑音のレベルを比較する尺度です。SNRは信号電力と雑音電力の比として定義され、多くの場合デシベル dB)で表されます。SNRが高いということは、信号が明瞭で検出や解釈が容易であることを意味し、SNRが低いということは、信号が雑音によって劣化または不明瞭になり、識別や復元が困難になる可能性があることを意味します3。SNRをdBで計算するには、次の式を使用できます。

SNR (dB) = 信号電力dBm) − 雑音電力dBm)

この問題では、ノイズフロアが−90dBm (0.000000001ミリワット)、受信機の信号強度が−65dBm (0.000316ミリワット)であることが与えられています。したがって、これらの値を式に代入すると、次のようになります。

SNR (dB) = -65 dBm - (-90 dBm) SNR (dB) = -65 dBm + 90 dBm SNR (dB) = 25 dBm したがって、正解はSNRが25 dBmであるということです。

参考文献 :3 https://en.wikipedia.org/wiki/Signal-to-noise_ratio

最新問題: 3

どのArubaテクノロジーを使えば、デバイス固有のパスフレーズを使用して、ヘッドレスデバイスを安全にWLANに追加できますか？

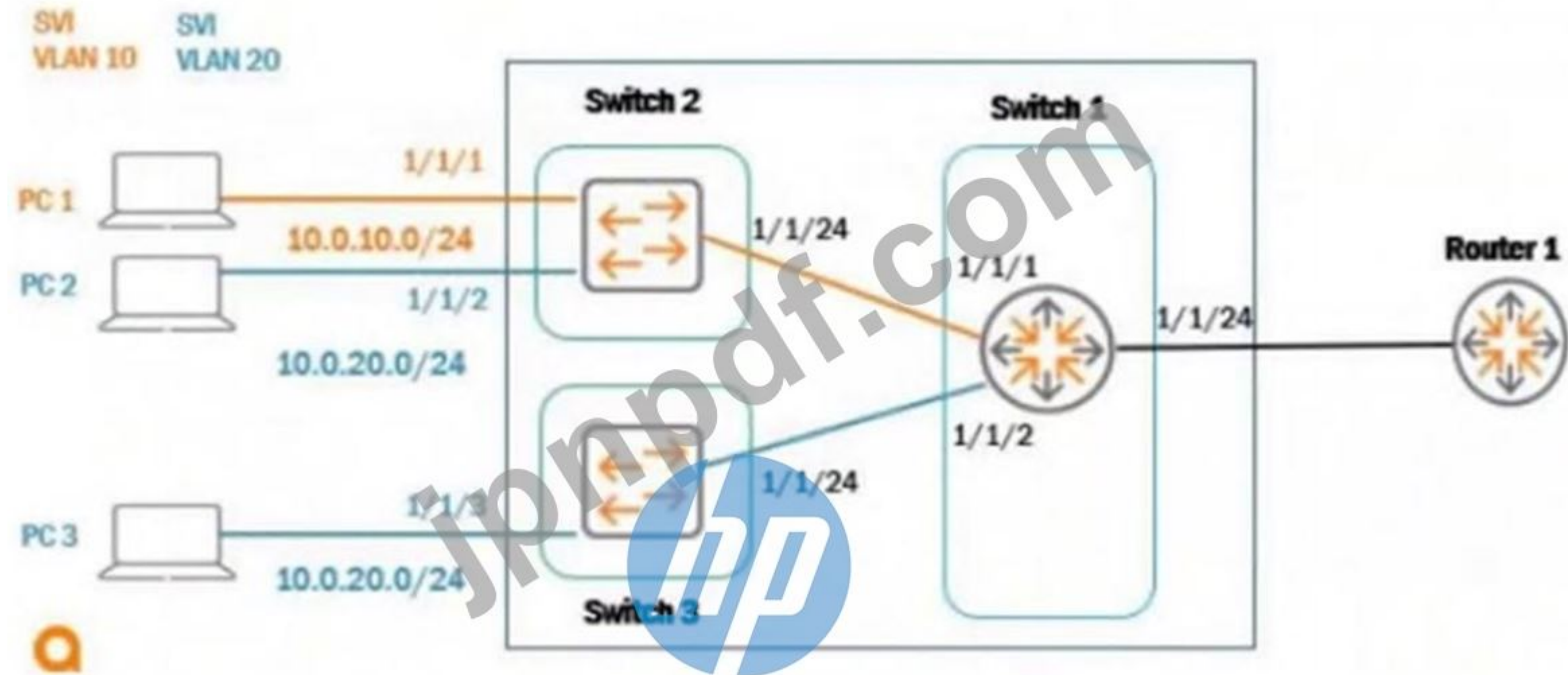
- A. 有線等価プライバシー (WEP)
- B. 複数事前共有鍵 (MPSK)
- C. 機会的無線暗号化 (OWE)
- D. 一時的鍵完全性プロトコル (TKIP)

Answer: B ([メッセージを残す](#))

マルチプル事前共有キー (MPSK) は、デバイス固有またはグループ固有のパスフレーズを使用して、ヘッドレス デバイスを WLAN 無線ローカル エリア ネットワークに安全に追加できる機能です。WLAN は、無線通信を使用して 2 台以上のデバイスを接続し、家庭、学校、コンピュータ ラボ、キャンパス、オフィス ビルなどの限られたエリア内でローカル エリア ネットワーク (LAN) を形成する無線コンピュータ ネットワークです。MPSK は、同じ SSID (サービス セット識別子) 上の異なるデバイスに異なる PSK を許可することで、WPA2 PSK (Wi-Fi Protected Access 2 事前共有キー) モードを強化します。WPA2 PSK は、オプションの事前共有キー (PSK) 認証を使用して WPA2 を使用してネットワークを保護する方法で、エンタープライズ認証サーバーを持たない家庭ユーザー向けに設計されています。SSIDは、モバイルデバイスがIEEE 802.11 WLANアーキテクチャの構成要素である基本サービスセット (BSS)に接続しようとする際にパスワードとして機能します。MPSKパスワードは生成またはユーザーが作成でき、ClearPass Policy Manager12によって管理されます。参考文献 :1 <https://blogs.arubanetworks.com/solutions/simplify-iot-authentication-with-multiple-pre-shared-keys/> 2 <https://www.arubanetworks.com/techdocs/ClearPass/6.8/Guest/Content/AdministrationTasks1/Configuring-MPSK.htm>

最新問題: 4

展示資料を参照してください。



提示されたトポロジーに基づいて、PC3とスイッチ1の間にアンマネージドスイッチが接続されている場合、PC3へのトラフィックを有効にするためのスイッチ1のポート1/1/2の有効な設定は何でしょうか？

- A. インターフェース 1/1/2、トランクはVLAN 20を許可
- B. int 1/1/2、vlanネイティブ20
- C. int 1/1/2、vlanアクセス20
- D. int 1/1/2、タグなしVLAN 20

Answer: C ([メッセージを残す](#))

アンマネージドスイッチはタグなしトラフィックを送信するため、PC3に接続されているスイッチ1のインターフェースはVLAN 20のアクセスポートとして設定する必要があります。これにより、PC3からのタグなしトラフィックがVLAN 20に送られます。

最新問題: 5

ネットワーク技術者が、支店に設置された新しいアクセスポイント (AP) がAruba Centralから設定を受信できないという問題のトラブルシューティングを行っています。支店内の他のAPIは正常に動作しています。show ap debug cloud-server command」の出力では、cloud config received」がFALSEとなっています。

新しいアクセスポイントがインターネットに接続できることを確認した後、次に何を確認しますか？

- A. 無効化と有効化をアクティブ化してプロビジョニングの更新をトリガーします
- B. arubanetworks.comでAPがデバイスにpingできることを確認します。
- C. APIにライセンスが割り当てられていることを確認します
- D. Aruba Centralを無効化してから有効化することで、設定の更新をトリガーします。

Answer: ([解答を表示する](#))

APがインターネットに接続されているにもかかわらず、Aruba Centralから設定情報を受信できない場合、考えられる原因の一つは、APIにAruba Centralでライセンスが割り当てられていないことです。Aruba Centralで管理されるAPIには、それぞれライセンスが必要です。

参考資料: https://www.arubanetworks.com/techdocs/Central/2.5.2-GA/HTML_frameset.htm#GUID-8F0E7E8

最新問題: 6

単一のAruba CX 6300Mスイッチ構成では、L3接続を使用してスイッチの仮想インターフェイス120と130間のルーティングトラフィックを確立するにはどうすればよいのでしょうか？

- A. Aruba 6300Mではルーティングはデフォルトで有効になっています。
- B. ルートリーキングはデフォルトVRFで設定する必要があります。
- C. SVIインターフェースから `no routing` を削除します。
- D. SVI 120と130の間に静的ルートを作成します。

Answer: C ([メッセージを残す](#))

Aruba CX 6300Mスイッチでは、スイッチ仮想インターフェース (SVI) 間のルーティングはデフォルトで有効になっています。

したがって、SVI 120 と 130 のような SVI 間のトラフィックは、SVI 上に `ルーティングなし` の設定がない限り、ルートリーキングやスタティックルートなどの追加設定を必要とせずに内部的にルーティングできます。

最新問題: 7

セキュリティ対策としてWPA2-Personalを使用した場合、無線LAN環境にどのような脆弱性が生じるのでしょうか？

- A. 認証局によって生成されたX509証明書を使用します
- B. ペアワイズ時間キー (PTK) はセッションごとに固有です
- C. ペアワイズマスターキー (PMK) はすべてのユーザーで共有されます
- D. WPA 4ウェイハンドシェイクは使用しません

Answer: ([解答を表示する](#))

WPA2-Personalをセキュリティに使用した場合にWLAN環境に生じる脆弱性は、PMK (ペアワイズマスターキー) がPSK (事前共有キー) から派生するキーであり、PSKは通信開始前に2者間で共有されるキーで、どちらも固定されている点です。つまり、PSKを知っているすべてのユーザーは、認証プロセスなしでPMKを生成できてしまうのです。これはまた、PSK または PMK が攻撃者によって侵害された場合、PTK で暗号化されたすべてのトラフィックを復号するために使用できることを意味します。Pairwise Temporal Key (PTK) は PMK から派生したキーです。ANonce AuthenticatorNonce (ANonce) は、認証器 (AP など、ネットワーク リソースへのアクセスを制御するデバイス) によって生成される乱数です。SNonce Supplicant Nonce (SNonce) は、サブリカント (STA など、ネットワーク リソースにアクセスしたいデバイス) によって生成される乱数です。AA Authenticator Address (AA) は認証器の MAC アドレスです。SA Supplicant Address (SA) は、擬似乱数関数 (PRF) を使用したサブリカントの MAC アドレスです。PTK は 4 つのサブキーで構成されています。KCK キー確認キー (KCK) はメッセージの完全性チェックに使用され、KEK キー暗号化キー (KEK) は暗号化キーの配布に使用され、TK 一時キー (TK) はデータの暗号化に使用され、MIC メッセージ完全性コード (MIC) キーです。

他の選択肢は弱点ではない。理由は以下のとおりである。

- 認証局によって生成された X 509 証明書を使用します: WPA2-Personal では認証に X 509 証明書や認証局を使用しないため、このオプションは false です。X 509 証明書と認証局は、802.1X と EAP を使用する WPA2-Enterprise モードで使用される拡張認証プロトコル (EAP) は、パスワード、証明書、トークン、生体認証など、複数の認証方法をサポートする認証フレームワークです。EAP は、無線ネットワークやポイントツーポイント接続で使用され、サブリカント (ネットワークにアクセスしたいデバイス) と認証サーバー (サブリカントの資格情報を検証するデバイス) の間で安全な認証を提供します。RADIUS サーバーを使用したユーザー認証に使用されます。リモート認証ダイヤルインユーザーサービス (RADIUS) は、ネットワークサービスに接続して使用するユーザーに対して、集中型の認証、認可、アカウントिंग (AAA) 管理を提供するネットワークプロトコルです。

- ペアワイズテンポラルキー (PTK) はセッションごとに固有です :このオプションは偽です。PTKがセッションごとに固有であることは、WPA2-Personalの弱点ではなく強みです。PTKがセッションごとに固有であるということは、通信中に時間または送信されるパケット数に基づいて定期的に変更されることを意味します。これにより、リプレイ攻撃が防止され、データ暗号化のセキュリティが向上します。

- WPA 4ウェイハンドシェイクを使用しない :このオプションは偽です。WPA2-PersonalはキーネゴシエーションにWPA 4ウェイハンドシェイクを使用するためです。WPA 4ウェイハンドシェイクは、ステーションとアクセスポイントがANonceとSNonceを交換し、PMKからPTKを導出するプロセスです。また、WPA 4ウェイハンドシェイクにより、ステーションとアクセスポイントは互いのPMKを検証し、PTKのインストールを確認できます。

参考文献: [https://en.wikipedia.org/wiki/Wi-](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management)

[Fi_Protected_Access#WPA_key_hierarchy_and_management https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf](https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf)

最新問題: 8

顧客は、Windows 10クライアントを使用するユーザー向けに認証ポリシーを作成する必要がある、さらに、単一のRADIUSセッション内でデバイス認証情報とユーザー認証情報の両方を認証する必要があるという要件があります。この要件に対する適切なソリューションは何でしょうか？

- A. ClearPass 6.9 (EAP-TTLS対応)
- B. ClearPass 6.9 (EAP-TLS対応)
- C. ClearPass 6.9 (PEAP対応)
- D. ClearPass 6.9 (EAP-TEAP対応)

Answer: D ([メッセージを残す](#))

EAP-TEAPは、単一のRADIUSセッション内でデバイス認証とユーザー認証の両方をサポートするトンネルベースの認証方式です。ClearPass 6.9は、Windows 10クライアントの認証方式としてEAP-TEAPをサポートしています。

最新問題: 9

WPAキー階層のどの部分がデータの暗号化および/または復号化に使用されますか？

- A. ペアワイズ時間キー (PTK)
- B. ペアワイズマスターキー (PMK)
- C. キー確認キー (KCK)
- D. 一度だけ使用される番号 (nonce)

Answer: A ([メッセージを残す](#))

データの暗号化および/または復号化に使用される WPA キー階層の部分は、ペアワイズ一時キー (PTK) です。PTK は PMK から派生したキーです。ペアワイズマスターキー (PMK) は PSK から派生したキーです。事前共有キー (PSK) は、通信開始前に 2 者間で共有されるキーです。ANonce 認証ノンス (ANonce) は、認証器 (AP など、ネットワーク リソースへのアクセスを制御するデバイス) によって生成される乱数です。SNonce サプリカントノンス (SNonce) は、サプリカント (STA など、ネットワーク リソースへのアクセスを希望するデバイス) によって生成される乱数です。AA 認証器アドレス (AA) は認証器の MAC アドレスです。SA サプリカントアドレス (SA) は、擬似乱数関数 (PRF) を使用したサプリカントの MAC アドレスです。PTK は 4 つのサブキーで構成されています。

KCK (キー確認キー)はメッセージの完全性チェックに使用されます。

KEK (キー暗号化キー)は、暗号化キーの配布に使用されます。

TKテンポラルキー (TK)はデータ暗号化に使用されます。

MICメッセージ整合性コード (MIC)キー

データ暗号化に特に使用されるサブキーは、TKテンポラルキー (TK)です。TKはペアワイズトランジェントキー (PTK)とも呼ばれます。TKは、通信中に時間または送信されるパケット数に基づいて定期的に変化します。

その他のオプションは、以下の理由によりWPAキー階層の一部ではありません。

PMK :PMKはWPAキー階層の一部ではなく、PTKを生成するための入力です。

KCK :KCKはWPAキー階層の一部ですが、データの暗号化には使用されず、メッセージの完全性チェックに使用されます。

ノンス :ノンスはWPAキー階層の一部ではなく、PTKを生成するための入力です。

最新問題: 10

スタックLEDがゆっくりとオレンジ色に点滅している場合、何を示していますか？

- A. スイッチの一つにスタッキング不良があります。
- B. ポートのスタッキングに障害が発生しました。スタッキングモードが選択されていません。
- C. スタッキングモードが選択されました
- D. スタッキングを同期中です。しばらくお待ちください。

Answer: C ([メッセージを残す](#))

ゆっくりとした琥珀色のスタックLEDが点滅している場合は、スイッチでスタッキングモードが選択されていることを示します。これは、他のスイッチが存在しない場合、スイッチがスタックに参加するか、新しいスタックを形成する準備ができていることを意味します。参照:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/stacking-leds.htm

最新問題: 11

ドラッグアンドドロップ問題

使用事例に適切な認証技術を対応させてください。

ClearPass Policy Manager		Add certificates to Android devices with the Aruba Onboard Application in the Google Play store that will be used for wireless authentication.
Cloud Authentication and Policy		Authenticate users on corporate-owned Chromebook devices using 802.1X and context gathered from the network devices that they log into.
		Leverage unbound Multi Pre-Shared Keys (MPSK) managed by Aruba Central to the end-users and client devices.
		Validate devices exist in a Mobile Device Management (MDM) database before authenticating BYOD users with corporate Active Directory using certificate

Answer:

ClearPass Policy Manager	Answer Area	
	ClearPass Policy Manager	Add certificates to Android devices with the Aruba Onboard Application in the Google Play store that will be used for wireless authentication.
Cloud Authentication and Policy	Cloud Authentication and Policy	Authenticate users on corporate-owned Chromebook devices using 802.1X and context gathered from the network devices that they log into.
	Cloud Authentication and Policy	Leverage unbound Multi Pre-Shared Keys (MPSK) managed by Aruba Central to the end-users and client devices.
	ClearPass Policy Manager	Validate devices exist in a Mobile Device Management (MDM) database before authenticating BYOD users with corporate Active Directory using certificates

最新問題: 12

Arubaアクセスポイントの設定に関して、以下の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. すべてのAruba APIは、機能するためにAruba Centralに物理的に接続されている必要があります。
- B. Aruba APIはインスタントモードではコントローラーなしでも動作します。
- C. Aruba APIは、リモートAP (RAP) 機能を標準でサポートしています。
- D. Aruba APIはクラスタリング技術をサポートしていません。

Answer: [\(解答を表示する\)](#)

最新問題: 13

ArubaOS-CXスイッチを経由して送信される音声トラフィックが、最小限の遅延で到着するようにする必要があります。
このタスクに最適なスケジューリング技術は何ですか？

- A. QoSシェーピング
- B. 律速段階
- C. 厳密なキューイング

D. DWRRキューイング

Answer: C ([メッセージを残す](#))

厳密なキューイングは、遅延に敏感な音声トラフィックを他の種類のトラフィックよりも優先させるための最適なスケジューリング技術です。この方式では、音声トラフィックが他のキューイングされたトラフィックよりも先に送信されるため、遅延の可能性を効果的に低減できます。

最新問題: 14

ワイヤレスクライアントのローミングに関する決定はどこで行われるのか？

- A.** クライアントデバイス
- B.** 仮想コントローラー
- C.** 発信元APと宛先APによる共同決定
- D.** アルバ中央

Answer: A ([メッセージを残す](#))

説明

無線クライアントのローミング決定は、信号強度、ノイズレベル、データレートなど、クライアントデバイス自身の基準に基づいて行われます。ネットワークは、近隣レポート、負荷分散、バンドステアリングなどの情報を提供することで、クライアントのローミング決定に影響を与えることができますが、最終的な決定はクライアントに委ねられます。

参考資料: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/wlan-roaming/cli

最新問題: 15

スタックLEDがゆっくりとオレンジ色に点滅している場合、何を示していますか？

- A.** スイッチの一つにスタッキング不良があります。
- B.** ポートのスタッキングに障害が発生しました。スタッキングモードが選択されていません。
- C.** スタッキングモードが選択されました
- D.** スタッキングを同期中です。しばらくお待ちください。

Answer: ([解答を表示する](#)**)**

ゆっくりとしたオレンジ色のスタックLEDの点滅は、スイッチでスタッキングモードが選択されていることを示します。これは、スイッチがスタックに参加する準備ができているか、他のスイッチが存在しない場合は新しいスタックを形成する準備ができていることを意味します。

最新問題: 16

ArubaのスタンドアロンAPを使用する場合、クライアントVLAN割り当てで「ネイティブVLAN」を選択します。クライアントIPはどのサブネットに配置されますか？

- A.** モビリティコントローラと同じサブネット
- B.** Aruba ESPゲートウェイと同じサブネット
- C.** モビリティコンダクターと同じサブネット
- D.** アクセスポイントと同じサブネット

Answer: ([解答を表示する](#)**)**

ArubaスタンドアロンAPを使用する場合、クライアントVLAN割り当てで「ネイティブVLAN」を選択すると、クライアントはアクセスポイントのIPアドレスと同じサブネットからIPアドレスを取得します。これは、このモードではアクセスポイントがクライアントのDHCPサーバーとして機能するためです。参照:https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/iap-dhcp/iap-dhcp.htm

有効な **HPE6-A85** 問題集は GoShiken.com が提供された合格しやすい HPE6-A85 試験問題集！ GoShiken.com が最新の **HPE6-A85** 試験問題集を提供しています。GoShiken.com HPE6-A85 試験問題は最新で、解答が正確でございます。最新の GoShiken.com HPE6-A85 問題集をゲットする人はこちら: <https://www.goshiken.com/HP/HPE6-A85-mondaishu.html> (**13430%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 17

病院では、患者の診断やデータ記録のために多くのモバイル機器を使用しています。単一のVSFスタックに400ポートを超える配線ラックを備えたこの大規模病院にとって、理想的なアクセススイッチは何でしょうか？

- A. CX 6300
- B. OCX 6400
- C. OCX 6200
- D. OCX 6100

Answer: A ([メッセージを残す](#))

400ポートを超える配線ラックを単一のVSFスタックに搭載する大規模病院に最適なアクセススイッチはCX 6300です。このスイッチには以下の利点があります。

CX 6300は、スイッチあたり最大48ポート、VSFスタックあたり最大10台のスイッチをサポートし、1つのスタックで合計480ポートを実現できます。これは、1つのVSFスタックで400ポート以上を必要とする要件を満たしています。

CX 6300は、最大960Gbpsのスイッチング容量と最大714Mppsの転送速度による高性能スイッチングをサポートします。これにより、モバイル機器や患者データに必要な高スループットと低遅延を実現します。

CX 6300は、動的セグメンテーション、ポリシーベースルーティング、ロールベースアクセス制御などの高度な機能をサポートしています。これらの機能は、異なる種類のデバイスやユーザーに異なるポリシーとロールを適用することで、ネットワークのセキュリティと柔軟性を向上させます。

CX 6300は、ネットワークの管理と自動化を簡素化するネットワーク構成・オーケストレーションツールであるAruba NetEditをサポートしています。これにより、ネットワークの構成と保守に伴う複雑さや人的ミスを軽減できます。

他の選択肢は理想的ではない理由は以下のとおりです。

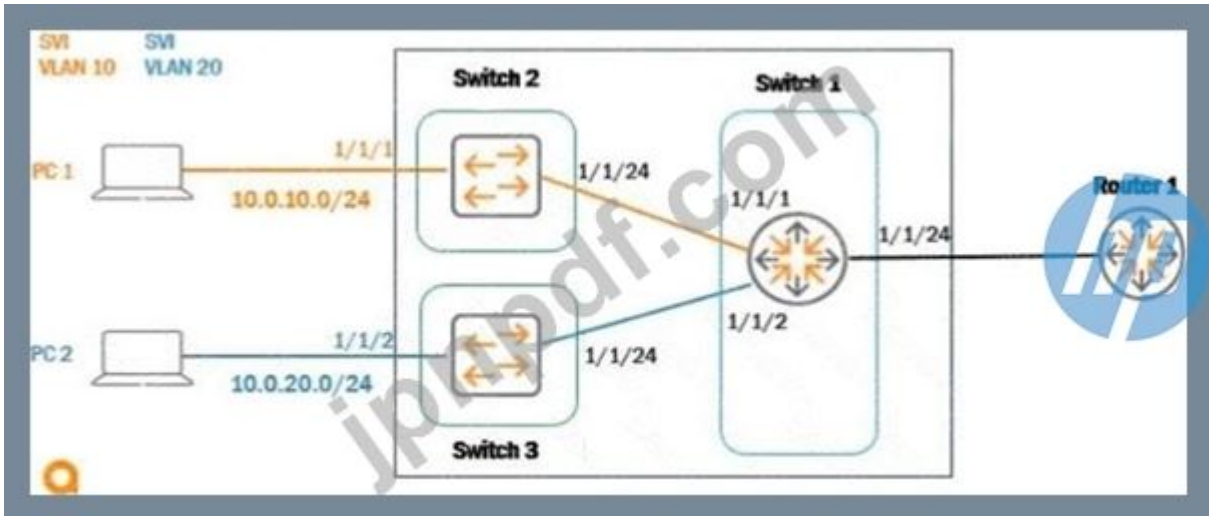
OCX 6400 :このスイッチはデータセンター向けに設計されており、VSFスタッキングには対応していません。また、ネットワークのセキュリティと柔軟性を高める上で重要な動的セグメンテーションやポリシーベースルーティングにも対応していません。

OCX 6200 :このスイッチは中小企業向けに設計されており、VSFスタッキングには対応していません。また、CX 6300よりもスイッチング容量と転送速度が低いため、ネットワークのパフォーマンスに影響を与える可能性があります。

OCX 6100 :このスイッチはエッジアプリケーション向けに設計されており、VSFスタッキングをサポートしていません。また、CX 6300よりもスイッチング容量と転送速度が低いため、ネットワークのパフォーマンスに影響を与える可能性があります。

最新問題: 18

提示されたトポロジに基づいて、スイッチ1のポート1/1/24でLLDPメッセージを受信できるようにするために、Arubaスイッチに求められる要件は何ですか。



ルーター1でLLDPが有効になっている場合？

- A. LLDPはデフォルトで有効になっています
- B. グローバル設定 lldp 有効化

- C. int 1/1/24、lldp受信
- D. int 1/1/24、cdpなし

Answer: A (メッセージを残す)

Arubaスイッチが特定のポートでLLDPメッセージを受信するには、そのポートでLLDPを有効にする必要があります。

Arubaスイッチのデフォルト設定では、通常すべてのポートでLLDPが有効になっているため、ほとんどの場合、追加の設定は必要ありません。

これは、ルーター 1 が LLDP メッセージを送信している場合、スイッチ 1 のポート 1/1/24 は、そのポートで LLDP が無効になっていない限り、追加の設定なしでそれらのメッセージを受信することを意味します。スイッチまたは特定のポートで LLDP が無効になっている場合は、有効にする必要があります。これは、オプション C (正しい Aruba OS 構文を使用) と同様の手順になります。オプション B はグローバル設定コマンドを示していますが、これは通常 Aruba スイッチで LLDP を有効にする方法ではありません。オプション D は Cisco Discovery Protocol (CDP) に関連しており、LLDP の動作とは関係ありません。

最新問題: 19

適切なQoS概念とその定義を一致させてください。

QoS concept	Definition
Best Effort Service	A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Class of Service	A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes
Differentiated Services	A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard
WMM	A method where traffic is treated equally in a first-come, first-served manner

Answer:

QoS concept	Definition
Best Effort Service	A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Class of Service	A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes
Differentiated Services	A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard
WMM	A method where traffic is treated equally in a first-come, first-served manner

説明

QoS (Quality of Service)とは、ネットワークリソースを管理し、トラフィックの種類に応じて異なるレベルのサービスを提供する技術群です。QoSは、ネットワークパフォーマンスの向上、遅延の削減、スループットの向上、輻輳の防止に役立ちます。QoSの概念とその定義について説明します。以下に私の回答を示します。

QoSの概念：

最善を尽くすサービス

サービスクラス

差別化されたサービス

WMM ===== 定義:

d) トラフィックが先着順で平等に扱われる方法 a) レイヤ 2 で 802.1Q VLAN Ethernet フレームを 8 つのサービス クラスの 1 つでマークすることによりネットワーク トラフィックを分類する方法 b) レイヤ 3 でパケットを 64 種類の異なるサービス クラスの 1 つでマークすることによりネットワーク トラフィックを分類する方法 c) IEEE 802.11e QoS 標準に基づくアクセス カテゴリを使用してネットワーク トラフィックを分類する方法 正解のみの簡潔かつ包括的な説明: QoS の概念とその定義の正しい対応は次のとおりです。

ベストエフォートサービス :これは、トラフィックを優先順位付けや差別化を行わずに、先着順で平等に処理する方式です。これは、特定のQoS要件や保証を持たないほとんどのネットワークやアプリケーションにおけるデフォルトのサービスレベルです。ベストエフォートサービスでは、帯域幅、遅延、ジッター、パケット損失について一切保証されません。

サービスクラス :これは、802.1Q VLANイーサネットフレームに8つのサービスクラス (0~7)のいずれかをマークすることで、レイヤ2でネットワークトラフィックを分類する方法です。これらのサービスクラスはIEEEとも呼ばれます。802.1p 優先度値または PCP 優先度コードポイント (PCP) は、イーサネット フレームの優先度レベルを示す 802.1Q VLAN タグの 3 ビット フィールドです。サービス クラス (Class of Service) により、ネットワーク デバイスは優先度レベルに基づいてさまざまな種類のトラフィックを識別して処理できます。サービス クラス (Class of Service) は通常、LAN で使用されます。ローカル エリア ネットワーク (LAN) は、レイヤ 2 スイッチングが主流である家庭、オフィス、建物環境など、限られた地理的範囲内でデバイスを接続するネットワークです。

差別化サービス: これは、パケットに 64 種類のサービス クラス (0 ~ 63) のいずれかを付けて、レイヤ 3 でネットワーク トラフィックを分類する方法です。これらのサービス クラスは、DiffServ コード ポイント (DSCP) とも呼ばれます。DiffServ コード ポイント (DSCP) は、IP ヘッダーの 6 ビット フィールドで、パケットのサービス クラスを示します。差別化サービスにより、ネットワーク デバイスは、サービス クラスに基づいてさまざまな種類のトラフィックを識別して処理できます。差別化サービスは通常、レイヤ 3 ルーティングが主流である WAN 環境で使用されます。WAN は、国や大陸などの広い地理的領域にわたってデバイスを接続するネットワークです。

WMM: これは、IEEE に基づくアクセスカテゴリを使用してネットワークトラフィックを分類する方法です。

802.11e QoS規格。WMMはWi-Fi Multimediaの略で、Wi-Fi Allianceが無線ネットワークのQoSを強化するために開発した認証プログラムです。WMMは、音声、ビデオ、ベストエフォート、バックグラウンドの4つのアクセスカテゴリ (AC) を定義しています。これらのアクセスカテゴリは、無線トラフィックの異なる優先度レベルと競合パラメータに対応しています。WMMにより、無線デバイスはアクセスカテゴリに基づいてさまざまな種類のトラフィックを識別して処理できます。

参考文献 https://en.wikipedia.org/wiki/Quality_of_service

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos-dfsrv/configuration/xr-16/qos-dfsrv-xr-16-book/qos-dfsrv.html>

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/81831-qos-wlan.html>

<https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm>

最新問題: 20

顧客が、会社全体のグループベースポリシー (GPO) を介してユーザー証明書とデバイス証明書を実装しました。ネットワーク認証時にクライアント証明書を必要とするEAP方式はどれですか？

A. EAP-TTLS

B. EAP-TLS

C. EAP-TEAP

D. PEAP

Answer: B ([メッセージを残す](#))

説明

EAP-TLSは、ネットワークへの認証時にクライアント証明書を必要とする認証方式です。公開鍵暗号とデジタル証明書を用いて、クライアントとサーバー間の相互認証を実現します。

参考資料 https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM_UserGuide/EAP-TLS

最新問題: 21

各要件に合わせて、最も費用対効果の高いケーブル配線オプションを選択してください。すべての長さは、パッチケーブル、サービスループなどを含むケーブルの全長を示します。)

OPTION		REQUIREMENT
Cat 5e cable		100 Gb connection with a length of 10' (3M) between two switches in the data center
Cat 6a cable		1 Gb connection with a length of 100' (30M) between an edge switch and a user desktop
Direct Attach Copper (DAC) cable		10 Gb connection with a length of 200' (60M) between the distribution switch in the main wiring closet and the edge switch in a remote wiring closet
multimode fiber		1 Gb connection with a length of 2km between two switches in different buildings
single mode fiber		

Answer:

OPTION		REQUIREMENT
Cat 5e cable	Direct Attach Copper (DAC) cable	100 Gb connection with a length of 10' (3M) between two switches in the data center
Cat 6a cable	Cat 6a cable	1 Gb connection with a length of 100' (30M) between an edge switch and a user desktop
Direct Attach Copper (DAC) cable	multimode fiber	10 Gb connection with a length of 200' (60M) between the distribution switch in the main wiring closet and the edge switch in a remote wiring closet
multimode fiber	single mode fiber	1 Gb connection with a length of 2km between two switches in different buildings
single mode fiber		

- * 100 Gbps、3M : 直接接続銅線
- * 1 Gbps、30M: Cat 6a
- * 10 Gbps、60M :マルチモードファイバー
- * 1Gbps、2km :シングルモードファイバー

最新問題: 22

AruDaCX 8400 の `show ip route`の出力に基づくと、`10.1.20.0/24, vrf default via 10.1.12.2. [1/0]`はどのようなタイプのルートですか？

- A. ローカル
- B. 静的
- C. OSPF

D. 接続済み

Answer: (解答を表示する)

スタティック ルートとは、ルーターまたはスイッチ上で手動で設定され、管理者が変更しない限り変更されないルートです。スタティック ルートは、デバイスに直接接続されていない、または動的ルーティング プロトコルでは到達できない特定の宛先にトラフィックがどのように到達するかを指定するために使用されます。Aruba CX スイッチでは、グローバル コンフィギュレーション モードで ip route コマンドを使用してスタティック ルートを設定できます。Aruba CX 8400 スイッチの show ip route」出力に基づくと、ルート 『0.1.20.0/24, vrf default via 10.1.12.2, [1/0]』は、管理距離が 1、メトリックが 0 であり、これらはスタティック ルートの一般的な値であるため、スタティック ルートです。

最新問題: 23

ネットワーク技術者が802.1X経由で従業員のSSIDに正常に接続しました。接続が成功したことを確認するために、どのRADIUSメッセージを確認すればよいですか？

A. 認可済み

B. アクセス承認

C. 成功

D. 認証済み

Answer: B (メッセージを残す)

802.1X を介した接続が成功していることを確認するために確認すべき RADIUS メッセージは Access-Accept です。このメッセージは、RADIUS サーバーがサブリカント (ネットワークへのアクセスを希望するデバイス) を認証および承認し、ネットワーク リソースへのアクセスを許可したことを示します。Access-Accept メッセージには、VLAN ID、セッション タイムアウト、フィルタ ID などの追加属性が含まれる場合があります、これらは認証装置 (スイッチなど、ネットワークへのアクセスを制御するデバイス) がサブリカントのトラフィックをどのように処理するかを指定します。

その他のオプションはRADIUSメッセージではありません。理由は以下のとおりです。

承認済み :これはRADIUSメッセージではなく、認証と認可が成功した後、認証器上のポートがサブリカントからのトラフィックを通過させることが許可されていることを示す状態です。

成功: これは RADIUS メッセージではなく、EAP 拡張認証プロトコル (EAP) は、パスワード、証明書、トークン、生体認証など、複数の認証方法をサポートする認証フレームワークです。EAP は、無線ネットワークやポイントツーポイント接続で使用され、サブリカント (ネットワークにアクセスしようとするデバイス) と認証サーバー (サブリカントの資格情報を検証するデバイス) の間で安全な認証を提供します。サブリカントと認証サーバー間の EAP 交換が正常に完了したことを示すステータスです。

認証済み :これはRADIUSメッセージではなく、認証器上のポートが、サブリカントの認証が成功した後に認証サーバーからEAP-Successメッセージを受信したことを示す状態です。

最新問題: 24

UXの利点を2つ挙げてください。2つ選択してください。)

A. AUXIIはインターネット接続なしで使用できます

B. UXIIは遠隔地で最適なWiFiチャンネルを計算するのに役立ちます

C. UXデザイナーはクライアント/ユーザーのように振る舞う

D. UX1は、指定された場所にあるすべてのAPのWi-Fiカバレッジを測定します。

E. UXI は、HTTP VOIP や Office 365 などのさまざまなアプリケーションをチェックできます。

Answer: C,E (メッセージを残す)

UXI (User Experience Insight) は、ユーザーの行動をシミュレートし、ユーザーの視点からネットワーク パフォーマンスをテストするデバイスです。HTTP、VOIP、Office 365 などのさまざまなアプリケーションをチェックし、レイテンシ、ジッター、パケット ロス、スループットなどのメトリックを測定できます。参照: https://www.arubanetworks.com/products/networking/user-experience-insight/ Aruba ネットワークで使用されているような User Experience Insight (UXI) センサーは、クライアントの行動を模倣し、ユーザーの視点からさまざまなネットワーク サービスとアプリケーションのパフォーマンスをテストするように設計されています。HTTP、VOIP、Office 365 などのクラウド サービスを含むさまざまなアプリケーションのユーザー アクティビティをシミュレートし、エクスペリエンスの品質を測定できるため、ネットワーク パフォーマンスとユーザー エクスペリエンスに関する貴重な洞察が得られます。

最新問題: 25

複数の種類のIoTデバイス (中には802.11bのみで動作するものもある)に対して無線アクセスを設定する必要があります。各デバイスクラスには固有のPSKが必要であり、役割として異なるセキュリティポリシーを適用する必要があります。デバイスクラスは15~20種類あり、パフォーマンスを最適化する必要があります。これらの要件を満たすオプションはどれですか？

A. 5GHz帯と6GHz帯を使用し、各IoTクラスごとにMPSK方式による単一のSSIDを使用

- B. 2.4GHz帯と5GHz帯を使用し、各IoTクラスごとにMPSK方式による単一SSIDを使用
- C. 5GHz帯と6GHz帯を使用し、IoTクラスごとに固有のPSKを持つ個別のSSID
- D. 2.4GHz帯と5GHz帯を使用し、各IoTクラスごとに固有のPSKを持つ個別のSSIDを使用します。

Answer: B ([メッセージを残す](#))

MPSK を使用した単一の SSID は、多くのデバイス固有またはグループ固有のパスフレーズをサポートし、各 IoT クラスを適切な役割ベースのセキュリティ ポリシーにマッピングできます。2.4 GHz の使用は、802.11bのみ対応のデバイス向けである一方、5GHz帯は対応クライアントのパフォーマンスを最適化するのに役立ちます。

最新問題: 26

複数の20MHz幅の802.11チャンネルをボンディングするのはどのような場合ですか？

- A. 信号対雑音比 \$NR\$を下げる
- B. クライアントとAP間のスループットを向上させる
- C. 高可用性APグループをプロビジョニングする
- D. 高利得無指向性アンテナを利用する

Answer: B ([メッセージを残す](#))

複数の 20MHz 幅の 802.11 チャンネルをボンディングすることは、より広い帯域幅のチャンネルを作成し、より高いデータレートの伝送をサポートする技術です。より多くのスペクトル リソースを使用し、干渉を減らすことで、クライアント と AP 間のスループットを向上させることができます。参照:<https://ieeexplore.ieee.org/document/9288995> 複数の 20MHz 幅の 802.11 チャンネルをボンディングすることは、クライアント デバイスとアクセス ポイント (AP) 間のスループットを向上させるために使用される技術です。2 つ以上の 20MHz チャンネルを、より広いチャンネル (e.

例えば、40MHz、80MHz、あるいは160MHzといった周波数帯域を用いることで、データ伝送容量、ひいては無線接続全体の処理能力が向上します。この方法は、高帯域幅を必要とするアプリケーションや、より高いデータレートが求められる環境で特に有効です。

最新問題: 27

単一のAruba CX 6300Mスイッチ構成では、L3接続を使用してスイッチの仮想インターフェイス120と130間のルーティングトラフィックを確立するにはどうすればよいのでしょうか？

- A. SVIインターフェースから `no routing` を削除します。
- B. ルートリーキングはデフォルトVRFで設定する必要があります。
- C. Aruba 6300Mではルーティングはデフォルトで有効になっています。
- D. SVI 120と130の間に静的ルートを作成します。

Answer: C ([メッセージを残す](#))

最新問題: 28

Arubaのキャプティブポータルは、どの認証方式を使用していますか？

- A. レイヤー3認証
- B. MAC認証
- C. 802.1x認証
- D. レイヤー2認証

Answer: A ([メッセージを残す](#))

Arubaのキャプティブポータルはレイヤー3認証を使用します。つまり、クライアントのHTTPリクエストを傍受し、クライアントが認証情報を入力できるWebページにリダイレクトします。その後、RADIUSサーバーまたはローカルデータベースによって認証情報が検証され、ネットワークアクセスが許可されます。

参考資料: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/captive-portal/ca

最新問題: 29

Centralのネットワークチェックページを使用する場合、スイッチに対してどのようなテストを実行できますか？ 2つ選択してください。）

- A. スピードテスト (iperf)
- B. ピングテスト
- C. ハードウェアの完全なチェック (メモリの徹底的なチェックを含む)
- D. LEDチェック。
- E. PoEチェック

Answer: (解答を表示する)

Aruba Centralのネットワークチェックページでは、スイッチに対して複数の診断テストを実行できます。pingテストは、IPネットワーク上のホストへの到達可能性を確認するための一般的なユーティリティです。Power over Ethernet (PoE) チェックは、PoE対応デバイスへの電力供給状態を確認するのに役立ちます。これらのテストは、ネットワークデバイスへの接続性と電力供給を確保するために不可欠です。

最新問題: 30

機能をAruba OSのバージョンと照合してください（一致する項目は複数回使用できます）。

Aruba OS 8

Aruba OS 10

Answer Area

Clustered Instant Access Points

Dynamic Radius Proxy

Scales to more than 10,000 devices

Unifies wired and wireless management

Wireless controllers

Answer:

Aruba OS 8

Aruba OS 10

Answer Area

Aruba OS 8

Aruba OS 8

Aruba OS 10

Aruba OS 8

Aruba OS 8

Clustered Instant Access Points

Dynamic Radius Proxy

Scales to more than 10,000 devices

Unifies wired and wireless managemen

Wireless controllers

Explanation:

機能: 1) クラスタ化されたインスタント アクセス ポイント Aruba OS バージョン: a) Aruba OS 8 機能: 2) ダイナミック Radius プロキシ Aruba OS バージョン: a) Aruba OS 8 機能: 3) 10,000 台以上のデバイスに拡張可能 Aruba OS バージョン: b) Aruba OS 10 機能: 4) 有線と無線の管理を統合 Aruba OS バージョン: a) Aruba OS 8 機能: 5) ワイヤレス コントローラ Aruba OS バージョン: a) Aruba OS 8 ArubaOS は、すべての Aruba Mobility Controller (MC) およびコントローラ管理のワイヤレス アクセス ポイント (AP) のオペレーティングシステムです。ArubaOS 8 は、統合された有線および無線アクセス、シームレスなローミング、エンタープライズ グレードのセキュリティ、高密度環境をサポートするために必要な信頼性を備えた高可用性ネットワークを提供します 1。

ArubaOS 8の主な機能は以下のとおりです。

- クラスタ化されたInstant Access Point :この機能により、複数のInstant APがクラスタを形成し、設定情報と状態情報を共有できます。これにより、クライアントのシームレスなローミング、負荷分散、および高速フェイルオーバーが可能になります2。

- 動的RADIUSプロキシ :この機能により、MCはクライアントまたはAPからのRADIUS認証要求のプロキシとして機能できます。これにより、RADIUSサーバーの設定と管理が簡素化され、MCとRADIUSサーバー間のネットワークトラフィックが削減されます3。

- ワイヤレスコントローラ Arubaのワイヤレスコントローラは、ワイヤレスネットワークを一元的に管理 制御するデバイスです。アクセスポイントのプロビジョニング、設定、セキュリティ、ポリシーの適用、ネットワークの最適化などの機能を提供します。

ArubaOS 10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あるAruba Centralと連携する次世代オペレーティングシステムです。ArubaOS 10は、大規模なキャンパス、支店、リモートワーク環境において、拡張性、セキュリティ、AIによる最適化を向上させます。ArubaOS 10の主な機能は以下のとおりです。

- 10,000台以上のデバイスに対応 ArubaOS 10は、クラスタあたり最大10,000台のデバイスをサポートできます。これはArubaOS 8の10倍です。これにより、お客様はパフォーマンスや信頼性を損なうことなくネットワークを拡張できます。

-有線と無線の管理を統合 ArubaOS 10は、ネットワーク上の有線デバイスと無線デバイスの両方を管理するための単一プラットフォームを提供します。お客様はAruba Centralを使用して、どこからでもデバイスの設定、監視、トラブルシューティング、およびアップデートを行うことができます。

ArubaOS 8とArubaOS 10には、以下のような共通機能がいくつかあります。

- 有線と無線の管理を統合：両方のオペレーティングシステムは、ArubaスイッチとAPを使用する顧客向けに、有線と無線の統合アクセスを提供します。顧客は単一のインターフェイスを使用して、ネットワークインフラストラクチャ全体を管理できます1。

参考文献：

1 <https://www.arubanetworks.com/resource/arubaos-8-fundamental-guide/>

2 https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/iap-maintenance/clus

3 https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overvie

<https://www.arubanetworks.com/products/networking/controllers/>

<https://www.arubanetworks.com/products/network-management-operations/arubaos/>

<https://blogs.arubanetworks.com/solutions/making-the-switch/>

<https://www.arubanetworks.com/products/network-management-operations/aruba-central/>

最新問題: 31

ドラッグ&ドロップ

Aruba Centralテクノロジーを適切な機能と一致させてください。（同じ項目を複数回使用しても構いません。）

この VLAN に関連付けるサブネットのルーティング可能なインターフェイスを正しく構成するには、SVI を作成します。スイッチド仮想インターフェイス (SVI) は、スイッチ上の仮想インターフェイスで、VLAN を表し、その VLAN のレイヤ 3 ルーティング機能を提供します。SVI は、VLAN 間ルーティングを有効にしたり、VLAN 内のホストにゲートウェイ アドレスを提供したり、VLAN に ACL や QoS ポリシーを適用したりするために使用されます。SVI には、インターフェイス ポートの節約、ケーブル コストの削減、ネットワーク設計の簡素化など、物理的なルーティング インターフェイスよりもいくつかの利点があります。SVI は通常、VLAN ID (例: vlan 10) に従って番号が付けられ、VLAN のサブネット内で IP アドレスが割り当てられます。SVI は、interface vlan、ip address、no shutdown などのコマンドを使用して作成および構成できます。SVI は、6300M スタックのサブネットに show ip interface brief、show vlan、show ip route などのコマンドを使用して確認できます。SVIは、スイッチ上の仮想インターフェースであり、VLANを表し、そのVLANに対してレイヤ3ルーティング機能を提供します。6300MスタックのサブネットにSVIを作成することで、スイッチはそのVLAN内のユーザーのゲートウェイとして機能し、異なるサブネット間のVLAN間ルーティングが可能になります。また、6300MスタックのサブネットにSVIを作成することで、ルーティングに必要な物理インターフェースとケーブルの数を減らすことができ、ネットワーク設計と管理が簡素化されます。

他のオプションは、このVLANに関連付けるサブネットのルーティング可能なインターフェースを設定する正しい方法ではありません。理由は以下のとおりです。

- 6300M スタック上のサブネットに、ダウストリーム スイッチごとに物理的にルーティングされたインターフェイスを作成する: このオプションは、ダウストリーム スイッチごとに 1 つの物理ポートとケーブルを使用する必要があるため、インターフェイス リソースを消費し、ケーブル コストが増加するため、適切ではありません。また、6300M スタック上のサブネットに、ダウストリーム スイッチごとに物理的にルーティングされたインターフェイスを作成すると、インターフェイスごとに個別のルーティング構成とポリシーが必要になるため、ネットワークの設計と管理が複雑になります。

- 各ダウストリームスイッチのサブネットにSVIを作成する :このオプションは誤りです。各ダウストリームスイッチのサブネットにSVIを作成しても、各ダウストリームスイッチは自身のVLANのゲートウェイとしてのみ機能するため、異なるサブネット間のVLAN間ルーティングは有効になりません。また、各ダウストリームスイッチのサブネットにSVIを作成すると、同じサブネット内に重複したIPアドレスが作成され、IPアドレスの競合やルーティングエラーが発生します。

- 6300M スタックのサブネットに SVI を作成し、各ダウストリーム スイッチ スタックの管理アドレスを同じサブネット内の異なる IP アドレスに割り当てる: このオプションは誤りです。6300M スタックのサブネットに SVI を作成し、各ダウストリーム スイッチ スタックの管理アドレスを同じサブネット内の異なる IP アドレスに割り当てても、各ダウストリーム スイッチは自身の VLAN のゲートウェイとしてのみ機能するため、異なるサブネット間の VLAN 間ルーティングは有効になりません。また、6300M スタックのサブネットに SVI を作成し、各ダウストリーム スイッチ スタックの管理アドレスを同じサブネット内の異なる IP アドレスに割り当てても、同じサブネット内に不要な IP アドレスが作成され、IP スペースが無駄になり、ネットワーク管理が複雑になります。

参考文献：

<https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/index.html>

<https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-ov>

<https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-co>

最新問題: 33

Aruba CXスイッチでOSPFダイナミックルーティングプロトコルを使用する場合、ルートを交換するために隣接デバイス間で一致させる必要がある設定は何ですか？

A. こんにちはタイマー

B. DR構成

C. ECMP法

D. BDR構成

Answer: A ([メッセージを残す](#))

OSPF は Open Shortest Path First の略です。OSPF は、階層構造を使用して IP ネットワークのルーティング トポロジを作成するリンク ステート ルーティング プロトコルです。OSPF ルータは、各インターフェイスで定期的送信される Hello パケットを使用して、ネイバーとルーティング情報を交換します。隣接関係 (隣接関係とは、ルーティング情報を交換するために選択されたネイバー ルータ間で形成される関係です) を確立するには、OSPF ルータは、インターフェイスで Hello パケットが送信される頻度を指定する Hello タイマーなど、いくつかのパラメータについて合意する必要があります。ネイバー ルータ間で Hello タイマーが一致しない場合、隣接関係は形成されず、ルートも交換されません。

参考資料: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/osfp/

最新問題: 34

以下の設定を確認してください。

```
Core-1(config)# interface loopback 0
Core-1(config-if)# ip address 10.1.200.1/32
Core-1(config)# router ospf 1
Core-1(config-ospf-1)# router-id 10.1.200.1
Core-1(config-ospf-1)# area 0
Core-1(config-ospf-1)# exit
```

OSPFでルーターIDとしてIPアドレス10.1.200.1を使用するように設定するのはなぜですか？

- A. ループバックインターフェースに関連付けられたIPアドレスはルーティング不可であり、ループを防止します。
- B. ループバックインターフェースの状態は管理インターフェースの状態に依存し、ルーティングの更新を減らします。
- C. ループバックインターフェースに関連付けられたIPアドレスはルーティング可能であり、ループを防止します。
- D. ループバックインターフェースの状態は、物理インターフェースとは独立しており、ルーティングの更新を削減します。

Answer: ([解答を表示する](#))

説明

OSPF を設定する理由は、Open Shortest Path First (OSPF) は、IP ネットワーク内でのデータ伝送に最適なルートを動的に計算するリンクステートルーティングプロトコルです。OSPF は、ネットワークをエリアに分割し、各ルータにルータ ID (RID) と呼ばれる識別子を割り当てる階層構造を使用します。OSPF は、ハロー パケットを使用してネイバーを検出し、ルーティング情報を交換します。OSPF は、リンク コストに基づいて最短パス ツリー (SPT) を計算し、SPT に基づいてルーティング テーブルを構築するために、ダイクストラ アルゴリズムを使用します。OSPF は、複数の等コスト パス、ロード バランシング、認証、およびブロードキャスト、ポイント ツー ポイント、ポイント ツー マルチポイント、非ブロードキャスト マルチ アクセス (NBMA) などのさまざまなネットワーク タイプをサポートします。OSPF は、IPv4 の場合は RFC 2328、IPv6 の場合は RFC 5340 で定義されています。IP アドレスを使用するには、インターネット プロトコル (IP) アドレスは、インターネット プロトコルを使用して通信するコンピュータ ネットワークに接続された各デバイスに割り当てられる数値ラベルです。IP アドレスは、ホストまたはネットワーク インターフェイスの識別と場所のアドレス指定という 2 つの主要な機能を果たします。IP アドレスには、IPv4 と IPv6 の 2 つのバージョンがあります。IPv4 アドレスは 32 ビット長で、192.168.1.1 のようにドット付き 10 進数表記で記述されます。IPv6 アドレスは 128 ビット長で、2001:db8::1 のように 16 進数表記で記述されます。IP アドレスは、静的 (固定) または動的 (DHCP サーバーによって割り当てられる) のいずれかになります。ルーター ID として 10.1.200.1 ルーター ID (RID) ルーター ID (RID) は、ルーティング ドメインまたはプロトコル内の各ルーターに割り当てられる一意の識別子です。RID は、OSPF、IS-IS、EIGRP、BGP などのルーティング プロトコルによって、ネイバーの識別、ルーティング情報の交換、指定ルーター (DR) の選出などに使用されます。

RID は通常、ルータのインターフェイスまたはループバックに設定されている IP アドレスのいずれかから派生するか、ネットワーク管理者が手動で指定します。RID は、ルーティング ドメインまたはプロトコル インスタンス内で一意である必要があります。ループバック インターフェイスの状態は、ループバック インターフェイスです。ループバック インターフェイスは、物理ポートや接続に対応しないルータ上の仮想インターフェイスです。ループバック インターフェイスは、ネットワーク接続のテスト、ルーティング プロトコル用の安定したルータ ID の提供、ルータへの管理アクセスの提供など、さまざまな目的で使用されます。ループバック インターフェイスには、管理上シャットダウンされない限り常に稼働している、ハードウェア障害やリンク障害の影響を受けない、サブネットの制約に関係なく任意の IP アドレスを割り当てることができるなど、物理インターフェイスよりもいくつかの利点があります。ループバック インターフェイスは通常、ルータ上でゼロ (例: loopback0) から番号が付けられます。ループバック インターフェイスは、ループバック テスト用に予約されている特別な IP アドレス (IPv4 の場合は 127.xxx、IPv6 の場合は ::1) を使用して、テストまたは構成の目的で PC またはサーバ上に作成することもできます。ループバック インターフェイスは、仮想インターフェイスまたはダミー インターフェイスとも呼ばれます。ループバックインターフェイスの状態 ループバック インターフェイスの状態とは、ルータ上のループバックインターフェイスがアップ状態かダウン状態かを指します。ループバックインターフェイスの状態は、管理者が制御するか (no shutdown や shutdown などのコマンドを使用する) するか、ルーティング プロトコルによって自動的に決定されます (passive-interface や ip ospf network point-to-point などのコマンドを使用する)。ループバックインターフェイスの状態は、ルーティング プロトコルがループバックインターフェイスに割り当てられた IP アドレスをネイバー検出、ルータ ID の選択、ルートのアドバタイズメントなどに使用方法に影響します。ループバックインターフェイスの状態は、他のデバイスがループバックインターフェイスにアクセスしたり ping を実行したりする方法にも影響します。ループバックインターフェイスの状態は、show ip interfacebrief や show ip ospf neighbor などのコマンドを使用して確認できます。

ループバックインターフェースの状態は、ハードウェアやリンクの状態に依存しないため、物理インターフェースとは独立しています。つまり、管理者が手動でシャットダウンしない限り、ループバックインターフェースの状態は常に「アップ」になります。また、ルーター上の他のインターフェースに影響を与える可能性のある物理障害やリンク障害によって、ループバックインターフェースの状態が変化することはありません。

ループバックインターフェイスの状態は、ルーター上の他のインターフェイスに影響を与える可能性のある物理的障害やリンク障害によって変更されない安定したルーター ID を OSPF に提供するため、ルーティングの更新を削減します。これは、OSPF が DR を再選出する必要がないことを意味します。指定ルーター (DR) 指定ルーター (DR) は、ブロードキャストまたは非ブロードキャストマルチアクセス (NBMA) ネットワークで OSPF ルーターによって選出され、そのネットワークでの OSPF 操作のリーダーおよびコーディネーターとして機能するルーターです。DR は、ネットワークセグメント全体のリンク状態広告 (LSA) を生成し、セグメント内の他のすべてのルーターとの隣接関係を維持し、バックアップ指定ルーター (BDR) を介して異なるセグメントの他の DR とルーティング情報を交換する責任があります。DR は、ルーター優先度値とルーター ID に基づいて選出されます。優先度が最も高いルーターが DR になり、2 番目に優先度が高いルーターが BDR になります。優先度値が同点の場合は、ルーター ID が最も高いルーターが選ばれます。DR は、特定のインターフェイスでルータ優先度値を 0 (不適格) または 255 (常に適格) に設定することにより、手動で構成できます。DR は、ip ospf priority、ip ospf dr-delay、ip ospf network point-to-multipoint などのコマンドを使用しても影響を受けることがあります。DR は、show ip ospf neighbor、show ip ospf interface、show ip ospf database など

のコマンドを使用して検証できます。最短パスツリー (SPT) 最短パスツリー (SPT) は、グラフまたはネットワーク内のソースノードから他のすべてのノードへの最短パスを表すデータ構造です。SPT は、OSPF や IS-IS などのリンクステートルーティングプロトコルによって、リンクコストに基づいて最適なルートを計算するために使用されます。SPT は、ソース ノードから開始し、すべてのノードが含まれるまで最小コスト パスを持つノードをツリーに反復的に追加する Dijkstra アルゴリズムを使用して構築されます。SPT は、ツリー内の各ノードから親ノードへのポインタのセット、またはネットワーク内の各ノードから宛先ノードへのネクスト ホップ アドレスのセットで表すことができます。SPT は、ノードまたはリンクを追加または削除するか、リンク コストを変更することによって更新できます。SPT は、show ip route、show ip ospf database、show clns route、show clns database などのコマンドを使用して検証するか、LSA を送信することによって検証できます。リンク ステート 広告 (LSA) リンク ステート 広告 (LSA) は、ネットワーク セグメント内のリンクの状態とコストに関する情報を含むパケットです。LSA は、OSPF や IS-IS などのリンクステートルーティングプロトコルによって生成され、同じエリアまたはレベルの他のルータとルーティング情報を交換するためにフラッディングされます。LSA は、各ルータ上でリンク状態データベース (LSDB) を構築するために使用されます。LSDB には、ネットワーク セグメントの完全なトポロジが格納されます。LSA はまた、各ルータ上で最短経路木 (SPT) を計算するためにも使用されます。SPT は、ネットワーク内のすべての宛先への最適な経路を決定します。LSA には、その発生源と範囲に応じてさまざまな種類があります。ルーター LSA、ネットワーク LSA、サマリー LSA、外部 LSA など。LSA は、そのタイプとプロトコルバージョンによってフォーマットが異なりますが、通常は LSA ヘッダー、LSA タイプ、LSA 長、LSA 経過時間、LSA シーケンス番号、LSA チェックサム、LSA ボディなどのフィールドが含まれます。ルーター ID の変更により、LSA は show ip ospf database、show clns database、debug ip ospf hello、debug clns hello などのコマンドを使用して検証できます。

他の選択肢は理由として適切ではありません。理由は以下のとおりです。

ループバックインターフェイスに関連付けられた IP アドレスはルーティング不可であり、ループを防止します: このオプションは false です。ループバックインターフェイスに関連付けられた IP アドレスはルーティング可能であり、ループを防止しません。ループバックインターフェイスに関連付けられた IP アドレスは、既存のサブネットまたはループバック専用で作成された新しいサブネットに属する有効な IP アドレスであればどれも構いません。ループは IP アドレスではなく、ルーティング プロトコルまたはデバイスの設定ミスや障害によって発生するため、ループバックインターフェイスに関連付けられた IP アドレスはループを防止しません。ループバック インターフェイスの状態は管理インターフェイスの状態に依存し、ルーティングの更新を減らします。このオプションは、ループバック インターフェイスの状態が管理インターフェイスの状態を含む物理インターフェイスの状態とは独立しているため、false です。管理インターフェイス 管理インターフェイスは、構成、監視、トラブルシューティングなどの管理機能へのアクセスを提供するデバイス上のインターフェイスです。管理インターフェイスは、コンソール ポート、イーサネット ポート、USB ポートなどの物理ポート、または Telnet セッション、SSH セッション、Web セッションなどの仮想ポートにすることができます。管理インターフェイスは、CLI などのさまざまなプロトコルを使用できます。コマンドライン インターフェイス (CLI) コマンドライン インターフェイス (CLI) は、ユーザーがキーボードで入力したコマンドを使用してデバイスと通信できるようにする対話型のテキスト ベースのユーザー インターフェイスです。CLI は、ルーター、スイッチ、ファイアウォール、サーバーなどのデバイスの管理機能にアクセスする方法の 1 つです。CLI は、コンソール ポートなどのさまざまなプロトコルを使用できます。シリアル通信プロトコルシリアル通信プロトコルは、シリアル ポートとケーブルを使用してデバイス間でデータを送信する方法です。シリアル通信プロトコルは、ビット 0と1)を表すバイナリ信号を使用し、それらを1本のワイヤで順番に送信します。シリアル通信プロトコルには、シンプルさ、低コスト、長寿命などの利点があります。

最新問題: 35

複数のクラスのIoTデバイスに対して無線アクセスを設定する必要があります。これらのデバイスの中には、802.11bのみで動作するものもあります。各クラスには固有のPSKが必要であり、役割として異なるセキュリティポリシーを適用する必要があります。デバイスクラスは15〜20種類あり、パフォーマンスを最適化する必要があります。これらの要件を満たすオプションはどれですか？

- A. 5GHz帯と6GHz帯を使用し、各IoTクラスごとにMPSK方式による単一のSSIDを使用
- B. 2.4GHz帯と5GHz帯を使用し、各IoTクラスごとにMPSK方式による単一SSIDを使用
- C. 5GHz帯と6GHz帯を使用し、IoTクラスごとに固有のPSKを持つ個別のSSIDを使用する
- D. 2.4GHz帯と5GHz帯を使用し、各IoTクラスごとに固有のPSKを持つ個別のSSIDを使用します。

Answer: B (メッセージを残す)

セキュリティ要件が異なる複数のクラスの IoT デバイスに対してワイヤレス アクセスを構成するには、単一の SSID とマルチプル プリシェアード キー (MPSK) を使用するのが効率的なソリューションです。MPSK を使用すると、異なるデバイスまたはデバイス グループが同じ SSID に接続できますが、PSK はそれぞれ異なるため、クラスごとに独自のセキュリティ ポリシーを設定できます。一部の IoT デバイスは 2.4GHz 帯域で動作する 802.11b のみをサポートしているため、構成に 2.4GHz 帯域を含めることが不可欠です。5GHz 帯域も、その帯域で動作可能なデバイスをサポートし、ネットワーク パフォーマンスを最適化するために含める必要があります。6GHz 帯域 (オプション A) は、802.11b デバイスと互換性がないため適していません。IoT クラスごとに個別の SSID (オプション C および D) を使用すると、ネットワーク管理と SSID のオーバーヘッドが不必要に複雑になります。

最新問題: 36

ドラッグアンドドロップ問題

既存のIAP-315アクセスポイントを運用しているネットワーク管理者がAruba Centralに関心を持っており、特定の機能に必要なライセンスを知りたいと考えています。機能ごとに必要なライセンスを一致させてください（一致したライセンスは複数回使用できます）。

Advanced

Foundation

Answer Area

Alerts on config changes via email

Group-based firmware compliance

Heat maps of deployed APs

Live upgrades of an AOS10 cluster

Answer:

Advanced

Foundation

Answer Area

Foundation

Alerts on config changes via email

Foundation

Group-based firmware compliance

Advanced

Heat maps of deployed APs

Advanced

Live upgrades of an AOS10 cluste

Explanation:

Aruba Centralのライセンスガイドによると、Foundationライセンスは、構成、監視、アラート、レポート、ファームウェア管理などの基本的なデバイス管理機能を提供します。Advancedライセンスは、AIによる分析、WLANサービス、NetConductor Fabric、ヒートマップ、ライブアップグレードなどの追加機能を提供します。

最新問題: 37

AOS-CXにおいて、ゲートウェイ172.16.1.1を経由してクラスCネットワーク10.2.10.0への静的ルートを追加するための正しいコマンドは何ですか？

A. ip-route 10.2.10.0/24 172.16.1.1

B. ip route 10.2.10.0 255.255.255.0 172.16.1.1 description aruba

C. ip route 10.2.10.0/24 172.16.1.1

D. ip route-static 10.2.10.0 255.255.255.0 172.16.1.1

Answer: (解答を表示する)

AOS-CXでは、静的ルート構文はip routeに続いて宛先プレフィックスとネクストホップゲートウェイを使用し、これはオプションCに一致します。

最新問題: 38

AruDaCX 8400 の show ip route出力に基づくと、10.1.20.0/24、vrf default via 10.1.12.2 [1/0]”?

A. ローカル

B. 静的

C. OSPF

D. 接続済み

Answer: B ([メッセージを残す](#))

スタティック ルートとは、ルーターまたはスイッチで手動で設定され、管理者が変更しない限り変更されないルートです。スタティック ルートは、デバイスに直接接続されていない、または動的ルーティング プロトコルでは到達できない特定の宛先にトラフィックがどのように到達するかを指定するために使用されます。Aruba CX スイッチでは、グローバル コンフィギュレーション モードで ip route コマンドを使用してスタティック ルートを設定できます。Aruba CX 8400 スイッチの `show ip route` 出力に基づく、ルート `10.1.20.0/24`, `vrf default` via `10.1.12.2`, `[1/0]` は、管理距離が1、メトリックが0という、静的ルートの典型的な値を持つため、静的ルートです。参考資料 https://en.wikipedia.org/wiki/Static_routing https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htmhttps://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/show-ip-route.htm

最新問題: 39

チャンネル幅が同じ5GHz帯と6GHz帯のチャンネルを比較する場合、正しい記述はどれですか？

- A. 5GHzチャンネルは、6GHzチャンネルと比較して、伝送距離は同じですが、クライアントに提供するスループットが異なります。
- B. 5GHzチャンネルは、6GHzチャンネルと比較して伝送距離が異なり、クライアントに提供するスループットも異なります。
- C. 5GHzチャンネルは、6GHzチャンネルと比較して、伝送距離が同じで、クライアントに同じスループットを提供します。
- D. 5GHzチャンネルは6GHzチャンネルと比較して伝送距離が異なりますが、クライアントに提供するスループットは同じです。

Answer: ([解答を表示する](#))

5GHz帯と6GHz帯はどちらも同様のスループットを提供できますが、6GHz帯は周波数が高いため、5GHz帯の信号に比べて信号の到達距離が短く、障害物による減衰も大きくなります。この結果、一般的に5GHz帯のチャンネルは、同様の条件下では6GHz帯のチャンネルよりも長距離を伝送できるが、どちらも接続されたクライアントに対して高いデータレートをサポートできる。

最新問題: 40

レイヤー2 MAC認証を使用する利点は何ですか？

- A. ユーザー名とMACアドレスを照合します
- B. クライアント側での設定は不要です
- C. MAC許可リストは長期にわたって容易に維持管理できます。
- D. MAC識別子は偽装が難しい

Answer: ([解答を表示する](#))

レイヤ2 MAC認証は、クライアント側の設定や認証情報を必要とせずに、MACアドレスに基づいてデバイスを認証する方法です。スイッチはデバイスのMACアドレスをClearPassやRADIUSなどの認証サーバーに送信し、認証サーバーはそのMACアドレスがネットワークへのアクセスを許可されているかどうかを確認します。許可されている場合は、スイッチは割り当てられた役割とポリシーに基づいてデバイスへのアクセスを許可します。許可されていない場合は、スイッチはアクセスを拒否するか、デバイスをキャプティブポータルにリダイレクトして、さらなる認証を行います。参考資料 https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-ov

最新問題: 41

スパニングツリー (STP) 設定が適用された2台の独立したArubaOS-CX 6300スイッチが、ポート1/1/1と1/1/2間を2本のケーブルで相互接続されています。4つのポートすべてに `no shutdown` コマンドと `no routing` コマンドが設定されています。STPはこれらのポートでトラフィックをどのように転送または破棄するのでしょうか？

- A. MACアドレスが小さい方のスイッチは両方のポートで転送を行い、MACアドレスが大きい方のスイッチは両方のポートで転送を行います。
- B. MACアドレスが小さい方のスイッチは両方のポートで転送を行い、MACアドレスが大きい方のスイッチは一方のポートで破棄を行います。
- C. MACアドレスが小さいスイッチは1つのポートでパケットを破棄し、MACアドレスが大きいスイッチは両方のポートでパケットを転送します。
- D. MACアドレスが小さい方のスイッチは1つのポートでパケットを破棄し、MACアドレスが大きい方のスイッチは1つのポートでパケットを破棄します。

Answer: D ([メッセージを残す](#))

STP（スパニングツリープロトコル）は、スイッチ間またはブリッジ間の冗長パスがループを作成してブロードキャストストーム、複数フレーム送信、およびMACテーブルの不安定性を引き起こすのを防ぐことで、ブリッジされたイーサネットローカルエリアネットワークのループのないトポロジを保証するネットワークプロトコルです。STPは、拡張ネットワーク内のすべてのスイッチにまたがる論理ツリー構造を作成し、ツリーの一部ではない冗長リンクがデータパケットを転送するのをブロックします³。これらのポートでトラフィックを転送または破棄する方法は次のとおりです。

STPは、優先度値とMACアドレスで構成されるブリッジIDに基づいて、2台のスイッチからルートブリッジを選出します。ブリッジIDが小さい方のスイッチがルートブリッジとなり、そのスイッチのすべてのポートでトラフィックを転送します。

STPは、優先度値とポート番号で構成されるポートIDに基づいて、両方のスイッチの各ポートに役割と状態を割り当てます。ポートIDが小さい方のポートは指定ポートとなり、トラフィックを転送します。一方、ポートIDが大きい方のポートは代替ポートとなり、トラフィックを破棄します。

このシナリオでは、両方のスイッチのポート1/1/1と1/1/2の間に2本のケーブルが接続されているため、スイッチ間には2つの経路が存在し、ループが発生します。このループを防ぐため、STPは各スイッチのいずれかのポートでトラフィックを破棄することで、これらの経路の1つをブロックします。

両方のスイッチの優先度値が同じ（デフォルトは32768）と仮定すると、MACアドレスが小さい方のスイッチがブリッジIDが小さくなり、ルートブリッジになります。ルートブリッジは、ポート1/1/1と1/1/2の両方でトラフィックを転送します。

両方のポートの優先度値が同じ（デフォルトは128）と仮定すると、ポート番号が小さいため、両方のスイッチでポート1/1/1のポートIDはポート1/1/2よりも小さくなります。ポート1/1/1は指定ポートとなり、トラフィックを転送しますが、ポート1/1/2は代替ポートとなり、トラフィックを破棄します。

したがって、MACアドレスが小さい方のスイッチは1つのポート（ポート1/1/2）のトラフィックを破棄し、MACアドレスが大きい方のスイッチも1つのポート（ポート1/1/2）のトラフィックを破棄します。

最新問題: 42

ArubaOSファイアウォールロールを設定する際に、クライアントのブロードキャストドメインはどこで設定できますか？

- A. 無線LAN設定
- B. 帯域幅制御
- C. アクセス制御ルール
- D. ロールベースのVLANオーバーライド

Answer: D ([メッセージを残す](#))

ArubaOSにおけるクライアントのブロードキャストドメインは、ファイアウォールロール設定内のロールベースのVLANオーバーライドによって設定できます。これにより、ユーザーの役割に基づいてVLANを動的に割り当てることが可能になり、ブロードキャストドメインを含むネットワークアクセスレベルが決定されます。

最新問題: 43

正しく起動しない Aruba CX 6200 4 ノード VSF スタック スイッチのトラブルシューティングを行う必要があります。スイッチにアクセスして、OS イメージと ServiceOS で使用可能な起動オプションを表示できるオプションを選択してください。

- A. メンバー2スイッチ管理ポート
- B. USB-Cコンソールポート
- C. SSHを使用したコンダクター管理ポート
- D. メンバー2 RJ-45コンソールポート

Answer: B ([メッセージを残す](#))

最新問題: 44

AOS-CXスイッチでOSFPダイナミックルーティングプロトコルを使用する場合、経路を交換するために隣接デバイス間で一致させる必要があるのはどのような設定ですか？

- A. OSPFパッシブ設定
- B. OSPFエリア
- C. ルーターID
- D. ループバック設定

Answer: B (メッセージを残す)

OSPFネイバーは、隣接関係を確立し、ルーティング情報を交換するためには、同じエリア内に存在する必要があります。

最新問題: 45

Aruba Centralでグループを作成する際に、ユーザーはどのデバイス構成グループタイプを定義できますか？

2つ選択してください。）

A. セキュリティグループ

B. テンプレートグループ

C. デフォルトグループ

D. UIグループ

E. ESPグループ

Answer: B,C (メッセージを残す)

Aruba Centralでは、デバイス構成グループを作成し、各グループ内のデバイスに共通の設定を定義することができます。ネットワーク要件や管理上の好みに応じて、さまざまな種類のグループを作成できます。

Aruba Centralでグループを作成する際に定義できるグループの種類は2つあります。

テンプレートグループ :テンプレートグループを使用すると、変数と式を用いて構成テンプレートを作成し、複数のデバイスまたはデバイスグループに適用できます。テンプレートグループは、類似した構成を持つ大規模な展開を管理するための柔軟性と拡張性を提供します。

- デフォルトグループ :Aruba Centralにデバイスを初めて追加すると、デフォルトグループが自動的に作成されます。デフォルトグループには、他のグループに割り当てられていないすべてのデバイスに適用される基本的な構成設定が含まれています。必要に応じて、デフォルトグループを変更または削除できます。

参考文献：

<https://www.arubanetworks.com/techdocs/Central/latest/content/nms/device-groups.htm>

<https://www.arubanetworks.com/techdocs/Central/latest/content/nms/template-groups.htm>

<https://www.arubanetworks.com/techdocs/Central/latest/content/nms/default-group.htm>

最新問題: 46

1つのディストリビューションラックあたり200～380台のクライアント、プリンター、アクセスポイントを費用対効果の高い方法で接続するための、理想的なArubaアクセススイッチは何ですか？

A. Aruba CX 6400

B. Aruba CX 6200

C. Aruba CX 6300

D. Aruba CX 6000

Answer: C (メッセージを残す)

Aruba CX 6300シリーズは、中～高密度のクライアント環境に最適なアクセススイッチで、さまざまなポート密度とタイプに対応できる幅広いモデルを提供しています。ディストリビューションラックをサポートするCX 6300は、200～380台のクライアント、プリンター、アクセスポイントに対応し、高速アップリンク、クラス4 PoE (PoE+)サポート、スタッキング機能など、必要なポート密度とパフォーマンス機能を提供します。このシリーズはコスト効率に優れ、信頼性の高い接続性と安定したパフォーマンスを必要とする企業向けに設計されています。CX 6400、CX 6200、CX 6000などの他のオプションは、仕様が過剰で高価 (CX 6400)、必要なポート密度を提供できない (CX 6200)、または製品ラインに存在しない (CX 6000) 可能性があります。

有効な **HPE6-A85** 問題集は GoShiken.com が提供された合格しやすい HPE6-A85 試験問題集！ GoShiken.com が最新の **HPE6-A85** 試験問題集を提供しています。GoShiken.com HPE6-A85 試験問題は最新で、解答が正確でございます。最新の GoShiken.com HPE6-A85 問題集をゲットする人はこちら: <https://www.goshiken.com/HP/HPE6-A85-mondaishu.html> (134**30%OFF**問題集溶と正解付きで 30%w 特別割引コード: **Freepdfumps**)

最新問題: 47

エッジスイッチのアップリンクを要求どおりに設定した後、同僚からコアスイッチへのpingに失敗したと言われました。同僚に、接続が正しく接続されているか、スイッチの電源が入っているかを確認するように依頼します。同僚は両方とも正しいと確認します。コアスイッチへのpingを試み、pingが失敗していることを確認します。

この展開の性質を踏まえて、この問題のトラブルシューティングにはどのようなコマンドが使えるでしょうか？

A. Ping 10.11 1 - コアにpingを実行して接続性を確認します Show trunk - LAGインターフェイスがスイッチに正しく追加されたかどうかを確認します Show spanning tree - スパニングツリーのブロック状態を確認します Show port-access clients interface all - すべてのインターフェイスでポートアクセスのブロック状態または認証失敗を表示します Show run interface vlan20 - レイヤ3接続のレイヤ3 SVI構成が正しいことを再確認します Show lldp neighbors - コアをL2ネイバーとして認識できるかどうかを確認します 正しいリンクが正しいポートに接続されているかどうかを確認します

B. diagnostic diag cable-diag 1/1/51 diag cable-diag 1/1/52 - 物理リンクの診断情報を表示し、レイヤ 1 接続の中断に関するステータスを取得します。show ip route - デフォルト ゲートウェイがルーティング テーブルに存在することを確認します。show ip ospf - レイヤ 3 ルーティング プロトコルが有効になっているかどうかを確認します。show ip dns - 有効な DNS ソースがあるかどうかを確認します。

C. Ping 10.1.1.1 - コアにpingを実行して接続性を確認します show lacp agg - 現在どのリンクアグリゲーションがどの物理ポートを使用して構成されているかを確認します show lacp int - LACPステータスとトポロジ内でリンクがブロックされているかどうかを確認します show lldp neighbors - コアをL2ネイバーとして認識できるかどうかを確認します 正しいリンクが正しいポートに接続されているかどうかを確認します show run interface 1/1/51.1/1/52 - 物理インターフェイスがno-shutでlagのメンバーであることを確認します show run interface lag 1 - 論理インターフェイスに正しいvlanトランキング構成が適用されていることを確認します show run int vlan 20 - L3 SVIがno-shutで正しいサブネットに構成されていることを確認します

D. show run - スwitchの実行中の設定を表示します。Show run | begin 20 "vlan 20" - VLAN 20 がデータベースに正しく追加されたことを確認します。show run | begin 20 'interface vlan 20' - L3 SVI の設定を表示します。Show run interface 1/1/51.1/1/52 - 物理インターフェイスが no shut であり、LAG 1 のメンバーとして追加されたことを確認します。Show run int lag 1 - LACP ブロッキング状態を解消するために LACP モードが active に設定されていることを確認します。

Answer: ([解答を表示する](#))

これらのコマンドは、レイヤ3到達可能性、レイヤ2隣接性、LACP構成とステータス、VLANトランキング構成、インターフェイスステータスなど、エッジスイッチとコアスイッチ間の接続のさまざまな側面をチェックするため、この問題のトラブルシューティングに役立つ可能性があります。

参考資料: https://www.arubanetworks.com/techdocs/AOS-CX_10_04/CLI/GUID-8F0E7E8B-0F4B-4A3C-AE

最新問題: 48

Aruba Centralテクノロジーを適切な機能と一致させてください。(同じ項目を複数回使用しても構いません。)

AirMatch	ClientMatch
----------	-------------



Answer Area

	Calculates channel and power settings for all AP radios based on data from the last 24 hours of usage
	Load balancing across APs
	Makes changes once per day
	Minimizes co-channel interference between radios.
	Steers clients to different radio bands

Answer:

AirMatch	ClientMatch
----------	-------------



Answer Area

AirMatch	Calculates channel and power settings for all AP radios based on data from the last 24 hours of usage
ClientMatch	Load balancing across APs
AirMatch	Makes changes once per day
AirMatch	Minimizes co-channel interference between radios.
ClientMatch	Steers clients to different radio bands

最新問題: 49
ノイズフロアは000000001ミリワット、受信機の信号強度は-65dBm です。信号対雑音比はいくらですか？
A. 35 dBm
B. 15 dBm

C. 45 dBm

D. 25 dBm

Answer: D ([メッセージを残す](#))

信号対雑音比 \$NR)は、目的信号のレベルと背景雑音のレベルを比較する尺度です。SNRは信号電力と雑音電力の比として定義され、多くの場合デシベル (dB)で表されます。SNRが高いということは、信号が明瞭で検出や解釈が容易であることを意味し、SNRが低いということは、信号が雑音によって劣化または不明瞭になり、識別や復元が困難になる可能性があることを意味します3。SNRをdBで計算するには、次の式を使用できます。

SNR (dB) = 信号電力dBm) − 雑音電力dBm)

この問題では、ノイズフロアが−90dBm 0.000000001ミリワット)、受信機の信号強度が−65dBm 0.000316ミリワット)であることが与えられています。したがって、これらの値を式に代入すると、次のようになります。

SNR (dB) = -65 dBm - (-90 dBm) SNR (dB) = -65 dBm + 90 dBm SNR (dB) = 25 dBm したがって、正解はSNRが25 dBmであるということです。

参考文献 :3 https://en.wikipedia.org/wiki/Signal-to-noise_ratio

最新問題: 50

ネットワーク技術者が802.1X経由で従業員のSSIDに正常に接続しました。接続が成功したことを確認するために、どのRADIUSメッセージを確認すればよいですか？

A. 認可済み

B. アクセス承認

C. 成功

D. 認証済み

Answer: ([解答を表示する](#))

説明

802.1X を介した接続が成功していることを確認するために確認すべき RADIUS メッセージは Access-Accept です。このメッセージは、RADIUS サーバーがサブリカント (ネットワークへのアクセスを希望するデバイス) を認証および承認し、ネットワーク リソースへのアクセスを許可したことを示します。Access-Accept メッセージには、VLAN ID、セッション タイムアウト、フィルタ ID などの追加属性が含まれる場合もあり、これらは認証装置 (スイッチなど、ネットワークへのアクセスを制御するデバイス) がサブリカントのトラフィックをどのように処理するかを指定します。

その他のオプションはRADIUSメッセージではありません。理由は以下のとおりです。

承認済み :これはRADIUSメッセージではなく、認証と認可が成功した後、認証器上のポートがサブリカントからのトラフィックを通過させることが許可されていることを示す状態です。

成功: これは RADIUS メッセージではなく、EAP 拡張認証プロトコル (EAP) は、パスワード、証明書、トークン、生体認証など、複数の認証方法をサポートする認証フレームワークです。EAP は、無線ネットワークやポイントツーポイント接続で使用され、サブリカント (ネットワークにアクセスしようとするデバイス) と認証サーバー (サブリカントの資格情報を検証するデバイス) の間で安全な認証を提供します。サブリカントと認証サーバー間の EAP 交換が正常に完了したことを示すステータスです。

認証済み :これはRADIUSメッセージではなく、認証器上のポートが、サブリカントの認証が成功した後に認証サーバーからEAP-Successメッセージを受信したことを示す状態です。

参考文献 <https://en.wikipedia.org/wiki/RADIUS#Access-Accept>

<https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-1>

https://en.wikipedia.org/wiki/IEEE_802.1X#Port-based_network_access_control

https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_exchange

最新問題: 51

ArubaOS-CXスイッチへの入力時に過剰なブロードキャストトラフィックをドロップする必要があります。このタスクに最適なテクノロジーは何ですか？

A. 律速段階

B. DWRRキューイング

C. QoSシェーピング

D. 厳密なキューイング

Answer: A ([メッセージを残す](#))

ArubaOS-CX スイッチへの入力時に過剰なブロードキャスト トラフィックを破棄する最適な技術は、レート制限です。レート制限とは、ネットワーク管理者が帯域幅のしきい値または制限を設定することで、スイッチのポートまたは VLAN に入出力するトラフィック量を制御できる機能です。レート制限は、ネットワークの輻輳を防止したり、ネットワーク パフォーマンスを向上させたり、サービス レベル契約 (SLA) を遵守させたり、サービス拒否 (DoS) 攻撃を軽減したりするために使用できます。レート制限は、インターフェイス設定モードで storm-control コマンドを使用することで、ArubaOS-CX スイッチへの入力時のブロードキャスト トラフィックに適用できます。このコマンドを使用すると、ネットワーク管理者は、入力ポートでブロードキャスト トラフィックが使用できる帯域幅の割合または 1 秒あたりのパケット数を指定できます。ブロードキャスト トラフィックが指定されたしきい値を超えると、スイッチは超過分のパケットを破棄します。

他の選択肢は、受信時に過剰なブロードキャストトラフィックを破棄する技術ではありません。理由は以下のとおりです。

DWRRキューイング :DWRRはDeficit Weighted Round Robinの略で、出力ポート上の異なるトラフィッククラスまたはキューに異なる重みまたは優先度を割り当てるキューイングアルゴリズムです。DWRRは、各キューがその重みに基づいて公平な帯域幅を確保しつつ、優先度の低いキューがリソース不足に陥るのを防ぎます。DWRRは入力時に過剰なブロードキャストトラフィックを破棄するのではなく、出力時に送信トラフィックをスケジュールします。

QoSシェーピング :QoSとはQuality of Serviceの略で、ネットワークリソースを管理し、トラフィックの種類に応じて異なるレベルのサービスを提供する一連の技術です。QoSシェーピングは、利用可能な帯域幅やレート制限に合わせて、出力ポートで送信トラフィックを遅延またはバッファリングする技術です。QoSシェーピングは、入力時に過剰なブロードキャストトラフィックを破棄するのではなく、出力時に送信トラフィックを平滑化します。

厳密キューイング：厳密キューイングは、出力ポート上の異なるトラフィッククラスまたはキューに異なる優先順位を割り当てる別のキューイングアルゴリズムです。厳密キューイングでは、帯域幅要件や重みに関係なく、優先順位の高いキューが常に優先順位の低いキューよりも先に処理されることが保証されます。厳密キューイングは、入力時に過剰なブロードキャストトラフィックを破棄するのではなく、出力時に送信トラフィックをスケジュールします。

最新問題: 52
顧客環境への新しいAruba 6300Mの導入を依頼されました。オンサイトではなくリモートで作業しています。同僚がスイッチをインストールしています。同僚からエッジスイッチを設定するためのリモートコンソールセッションが提供されました。インターフェース1/1/51と1/1/52を使用してコアに戻るリンクアグリゲーションを設定するよう依頼されました。プロジェクトのシニアエンジニアから、以下のガイドラインに従ってスイッチと1Qアップリンクを設定するよう依頼されました。

- 1. VLAN 20をローカルVLANデータベースにMgmtという名前で追加します。
- 2. 10.1.10/24サブネットのアドレス10を使用して、VLAN 20に管理用のL3 SVIを追加します。
- 3. アップリンク用にLACPモードをアクティブにしてLAG 1を追加します。
- 4. LAG のネイティブ VLAN として VLAN 20 を使用します。
- 5. すべてのインターフェースが ON になっていることを確認します。

どの設定スクリプトを使えば目的を達成できますか？

A. Edge1# conf t vlan 20 name Mgmt interface vlan 20 ip address 10.1.1.10/24 no shut interface lag 1 shut vlan access 20 lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut

B. Edge1# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1.1 10/24 no shut interface 1/1/51.1/1

/52 シャットダウン VLAN トランク ネイティブ 20 VLAN トランク 許可 すべて ラグ 1 lacp

モード アクティブ インターフェース 1/1/51.1/1/52 シャットダウンなし

C. Edge1# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1 1 10/24 no shut interface lag 1 shut vlan trunk native 20 vlan trunk allowed all lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut interface 1/1/51.1/1/52 no shut

D. conf t vlan 20 name Mgmt ip address 10 1 1.10/24 no shut interface lag 1 shut vlan trunk native 1 vlan trunk allowed all lacp mode active int 1/1/51.1/1/52 shut no routing interface lag 1 no shut interface 1/1

/51.1/1/52 シャットダウンなし

Answer: C (メッセージを残す)

この設定スクリプトは、シニアエンジニアから提供されたガイドラインに従ってタスクを実行します。具体的には、Mgmt という名前の VLAN 20 を作成し、IP アドレス 10.1.1.10/24 を持つ L3 SVI を VLAN 20 に追加し、アップリンク用に LACP モードが有効な LAG 1 を作成し、LAG 上で VLAN 20 をネイティブ VLAN として使用し、すべてのインターフェースが ON であることを確認します。参考資料: [https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790](https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html)

/GUID-8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

Edge1# conf t

VLAN 20

名前管理

インターフェース VLAN 20

IPアドレス 10.1.1.10/24

閉めない

インターフェース遅延 1
 閉めない
 VLANトランクネイティブ20
 VLANトランクはすべて許可されています
 LACPモード有効
 インターフェース 1/1/51
 閉めない
 グループ1
 インターフェース 1/1/52
 閉めない
 グループ1
 出口

このスクリプトは、VLAN 20を「Mgmt」という名前で正しく作成し、指定されたIPアドレスを使用して管理用のL3 SVIを追加し、アクティブモードを使用してリンクアグリゲーション（LAG 1）用のLACPを設定します。また、VLAN 20をLAGのネイティブVLANとして設定し、すべてのインターフェイスが有効になっていることを確認します（no shutは、インターフェイスが管理上シャットダウンされている場合に、そのインターフェイスを起動するコマンドです）。

最新問題: 53
 適切なQoS概念とその定義を一致させてください。

QoS concept		Definition
Best Effort Service		A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Class of Service		A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes
Differentiated Services		A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard
WMM		A method where traffic is treated equally in a first-come, first-served manner

Answer:

QoS concept		Definition
Best Effort Service	Class of Service	A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Class of Service	Differentiated Services	A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes
Differentiated Services	WMM	A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard
WMM	Best Effort Service	A method where traffic is treated equally in a first-come, first-served manner

最新問題: 54

ネットワーク技術者が、Aruba Central から設定を受信しない支店の新しい AP のトラブルシューティングを行っています。支店の他の AP は期待どおりに動作しています。\$show ap debug cloud-server command」の出力では、cloud config received」が FALSE であることが示されています。

新しいアクセスポイントがインターネットに接続できることを確認した後、次に何を確認しますか？

- A.** 無効化と有効化をアクティブ化してプロビジョニングの更新をトリガーします
- B.** arubanetworks.comでAPがデバイスにpingできることを確認します。
- C.** APIにライセンスが割り当てられていることを確認します
- D.** Aruba Centralを無効化してから有効化することで、設定の更新をトリガーします。

Answer: A (メッセージを残す)

Aruba APがAruba Centralから設定を受信できず、同じ場所にある他のAPが正常に動作している場合、一般的なトラブルシューティング手順として、APのアクティベーションプロセスを無効にしてから再度有効にする方法があります。この操作によりプロビジョニングの更新がトリガーされ、APIはAruba Centralから設定を再度取得しようとします。この手順は、APと管理プラットフォーム間の通信またはプロビジョニングの問題を解決するのに効果的な場合が多くあります。

最新問題: 55

Aruba APでライブファームウェアアップグレードを実行する場合。

どの技術が、RF近隣データに基づいてすべてのアクセスポイントを分割し、クライアントへの影響を最小限に抑えますか？

- A.** HPE Aruba Networking ClientMatch
- B.** HPE Aruba Networking AI Insights
- C.** HPE Aruba Networking AirMatch
- D.** HPE Aruba Networking ESP

Answer: (解答を表示する)

Aruba AirMatch は、RF 無線周波数を最適化する機能です。RF は、電波伝搬に関連する電磁スペクトル内の任意の周波数です。アンテナに RF 電流が供給されると、電磁場が生成され、空間を伝搬できるようになります。機械学習アルゴリズムと履歴データを使用して AP の電力レベル、チャネル割り当て、チャネル幅を動的に調整することで、パフォーマンスとユーザー エクスペリエンスを向上させます。AirMatch は、RF 近隣データに基づいてすべての AP をパーティション分割し、クライアントへの影響を最小限に抑えることで、Aruba AP のライブ ファームウェア アップグレードを実行します。AirMatch は、隣接するパーティションが同時にアップグレードされないようにしながら、一度に 1 つのパーティションをアップグレードするローリング アップグレード プロセスを使用します。

最新問題: 56

HPE Aruba Networkingのキャプティブポータルは、どの認証方式を使用していますか？

- A.** レイヤー3認証
- B.** MAC認証
- C.** 802.1x認証
- D.** レイヤー2認証

Answer: (解答を表示する)

Arubaのキャプティブポータルはレイヤー3認証を使用します。つまり、クライアントのHTTPリクエストを傍受し、クライアントが認証情報を入力できるWebページにリダイレクトします。その後、RADIUSサーバーまたはローカルデータベースによって認証情報が検証され、ネットワークアクセスが許可されます。

最新問題: 57

信号強度を測定する際には、一般的にdBmが用いられ、0dBmは1mWの電力に相当する。

-20 dBmは何に相当しますか？

- A.** -1 mW
- B.** 0.01 mw

- C. 10 mW
- D. 1mW

Answer: B (メッセージを残す)

dBm は、特定の電力レベルと 1 mW の比率を測定する電力の単位です。dBm を mW に変換する式は、 $P(mW) = 1mW * 10^{(P(dBm)/10)}$ です。したがって、-20 dBm は、次のように 0.01 mW に相当します。 $P(mW) = 1mW * 10^{(-20/10)} = 0.01 mW$ 参考: https://www.rapidtables.com/convert/power/dBm_to_mW.html dBm は、1 ミリワット (mW) に対する電力の対数単位です。-20 dBm は、信号強度が 1 mW より 20 デシベル低いことを意味します。mW で表すと、これは 0.01 mW です。10 dB の減少ごとに、電力は 10 分の 1 になります。したがって、-20 dBm は $10^{-20/10} = 0.01$ mW または 0.01 mW です。

最新問題: 58

アクセスポイントからの信号が物体を通過する際に吸収されて弱まると、何が起こるのでしょうか？

- A. APIはボンディングチャネルを使用してクライアントへの遅延を低減します。
- B. 信号対雑音比 (SNR)が増加する
- C. 信号対雑音比 (SNR)が低下する
- D. Aruba Centralは、クライアントを動的に近隣のアクセスポイントに移動します。

Answer: C (メッセージを残す)

信号対雑音比 (SNR) は、目的の信号レベルと背景雑音レベルを比較する尺度です。SNR は、信号電力と雑音電力の比として定義され、多くの場合デシベル (dB) で表されます。SNR が高いということは、信号が明瞭で検出や解釈が容易であることを意味しますが、SNR が低いということは、信号が雑音によって破損または不明瞭になり、識別や回復が困難になる可能性があることを意味します 1。アクセス ポイント (AP) からの信号が壁や家具などの物体を通過する際に吸収されて弱まると、信号電力は低下します。これにより SNR が低下し、無線接続の品質に影響します。雑音電力は、他の AP や同じ周波数帯域で動作するデバイスなどの他のソースからの干渉によって増加することもあります 2。したがって、AP からの信号が物体を通過する際に吸収されて弱まると SNR が低下するというのが正解です。

最新問題: 59

各AAAサービスを正しい定義と一致させてください（一致した項目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）。

Definition	AAA Service
A list of rules that specifies which entities are permitted or denied access	Accounting
Control users access on the network	Authentication
Tracking user activity on the network	Authorization

Answer:

Definition	AAA Service
A list of rules that specifies which entities are permitted or denied access	Accounting
Control users access on the network	Authentication
Tracking user activity on the network	Authorization
Who can access the network based on credentials/certificates	

Explanation:

以下に、各AAA（認証 認可、アカウントिंग）サービスとその定義に対応する正しい項目を示します。

会計 :ネットワーク上でのユーザーアクティビティの追跡

認証: 資格情報/証明書に基づいて誰がネットワークにアクセスできるか。認可: どのエンティティがアクセスを許可または拒否されるかを指定するルールの一覧。アカウントINGはユーザーアクティビティの記録を保持することに関係し、認証はIDを確認するプロセスであり、認可は認証されたユーザーがネットワーク上で何を実行できるかを決定します。

最新問題: 60

HPE Aruba Networkingのどのテクノロジーが、無線帯域とAP無線間で負荷分散を提供しますか？

- A. HPE Aruba Networking ESP
- B. HPE Aruba Networking ClientMatch
- C. HPE Aruba Networking AirWave
- D. HPE Aruba Networking Central

Answer: B (メッセージを残す)

HPE Aruba Networking ClientMatchは、クライアントの接続状況とネットワーク状態を継続的に分析し、アクセスポイント (AP) と無線帯域間でクライアントをインテリジェントに振り分けます。これにより、利用可能な無線機器と帯域間で負荷分散が実現され、パフォーマンス、容量、およびユーザーエクスペリエンスの最適化に役立ちます。

最新問題: 61

データリンク層のPDUを表すプロトコルデータユニット (PDU) はどれですか？

- A. PDU1 - 信号
- B. PDU2 - フレーム
- C. PDU3 - パケット
- D. PDU4 - セグメント

Answer: B (メッセージを残す)

フレームは、送信元および宛先MACアドレス、フレームタイプ、エラー検出などの情報を含むヘッダーとトレーラーでネットワーク層PDU (パケット) をカプセル化したデータリンク層PDUです。フレームは、イーサネット、Wi-Fiなどの物理媒体を介して送信されます。参照: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/networking-basics.htm

有効な **HPE6-A85** 問題集は GoShiken.com が提供された合格しやすい HPE6-A85 試験問題集！ GoShiken.com が最新の **HPE6-A85** 試験問題集を提供しています。GoShiken.com HPE6-A85 試験問題は最新で、解答が正確でございます。最新の GoShiken.com HPE6-A85 問題集をゲットする人はこちら: <https://www.goshiken.com/HP/HPE6-A85-mondaishu.html> (134**30%OFF**問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 62

セキュリティで保護された有線イーサネットネットワークに接続する場合、802.1x認証プロセスはいつ開始されますか？

- A. ファイアウォールポリシーが適用された後
- B. 接続が確立されたとき
- C. キャプティブポータル認証後
- D. ペアワイズマスターキーを受け取ったとき

Answer: B (メッセージを残す)

有線802.1X環境では、物理的なイーサネット接続が確立されるとすぐに認証プロセスが開始されます。サブリカントとオーセンティケーターはEAPOLメッセージを交換し、デバイスは正常なネットワークアクセスが許可される前に認証に成功する必要があります。

最新問題: 63

最も安全な鍵管理オプションは何ですか？

A. ダイナミックWEP

B. WPA

C. WPA3

D. WPA2

Answer: (解答を表示する)

WPA3は、SAE（同時認証を使用することで最も安全な鍵管理を提供し、オフラインパスワード攻撃から保護するとともに、以前のWPAおよびWPA2方式と比較して暗号化を強化します。

最新問題: 64

WLANにおいて、新しいアクセスポイントへのローミングを最終的に決定する責任を負っているのは、どのデバイスですか？

A. クライアントデバイス

B. ネットワークゲートウェイ

C. ワイヤレスコントローラー

D. アクセスポイント

Answer: A (メッセージを残す)

WLANにおけるローミングの決定は、最終的にはクライアントデバイスが行います。アクセスポイント、コントローラ、ClientMatchなどの技術は情報や推奨事項を提供できますが、現在のアクセスポイントから離脱して新しいアクセスポイントに接続するタイミングを決定するのはクライアント自身です。

最新問題: 65

6GHz帯の主な特徴は何ですか？

A. 6GHz WLANでは、物体によるRF信号の吸収が少なくなります。

B. 北米では、6GHz帯には5GHz帯の40MHzチャンネルよりも多くの80MHzチャンネルが用意されています。

C. 6GHz帯は既存の帯域と完全な下位互換性があります。

D. 低電力機器は屋内および屋外での使用が許可されています。

Answer: (解答を表示する)

提示されたオプションの中で 6 GHz 帯域の主な特徴は、北米では 6 GHz 帯域が 5 GHz 帯域の 40 MHz チャンネルよりも多くの 80 MHz チャンネルを提供していることです。この特徴により、Wi-Fi 6E をサポートするワイヤレス デバイスに対して、より多くのスペクトル利用可能性、干渉の減少、およびより高いスループットが提供されます。Wi-Fi Enhanced (Wi-Fi 6E) は、Wi-Fi 6 (802.11ax) 規格の拡張であり、既存の帯域よりも低い帯域に加えて、新たに利用可能になった 6 GHz 付近の非免許周波数スペクトルで動作します。

この特性に関するいくつかの事実は以下のとおりです。

北米では、新しい周波数帯域（5925～7125MHz）の免許不要帯域全体において、3つのチャンネル幅（20MHz、40MHz、80MHz）それぞれに、最大7つの重複しないチャンネルが利用可能です。つまり、Wi-Fi機器で利用できる重複しないチャンネルは合計で最大21個となります。

一方、北米では、既存の周波数帯域（2400～2483MHzおよび5150～5825MHz）の免許不要帯域全体において、2つのチャンネル幅（20MHzと40MHz）それぞれで、重複しないチャンネルはわずか9つしか利用できません。つまり、Wi-Fi機器で利用できる重複しないチャンネルは合計で最大9つしかないということです。

したがって、北米では、新しい周波数帯域では、既存の周波数帯域に比べて、各チャンネル幅において重複しないチャンネルが2倍以上利用可能となる。

具体的には、既存の周波数帯域において、80MHz幅で利用可能な重複しないチャンネル数（7つ）は、40MHz幅で利用可能なチャンネル数（3つ）の2倍以上である。

他の選択肢は正しくありません。理由は以下のとおりです。

- 6 GHz WLAN では、RF 信号が物体に吸収されにくい: この選択肢は誤りです。高周波信号は、減衰が大きいため、低周波信号よりも物体に吸収されやすい傾向があります。減衰とは、伝送距離や物体または媒体を通過する際に信号強度が低下することを指す一般的な用語です。したがって、6 GHz WLAN の RF 信号は、低周波 WLAN の RF 信号よりも物体に吸収されやすくなります。

- 6GHz帯は既存の帯域と完全な下位互換性があります :このオプションは誤りです。Wi-Fiデバイスが6GHz付近の新しい周波数帯域で動作するには、Wi-Fi 6E規格をサポートしている必要があります。Wi-Fi 6E規格をサポートしていない既存のWi-Fiデバイスは、この周波数帯域を使用できず、それより低い既存の帯域でのみ動作します。

- 低電力デバイスは屋内と屋外での使用が許可されています: このオプションは誤りです。低電力屋内デバイス (LPI) は、特定の電力制限と登録要件の下で屋内での使用のみが許可されています。LPI デバイスの屋外での使用は、FCC などの規制当局によって禁止されています。連邦通信委員会 (FCC) は、米国全土のラジオ、テレビ、有線、衛星、ケーブルによる通信を規制する米国政府の独立機関です。ただし、超低電力デバイス (VLP) の屋外での使用は、特定の電力制限の下で登録要件なしで許可される場合があります。

参考文献：

<https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e>

<https://www.wi-fi.org/file/wi-fi-alliance-spectrum-needs-study>

https://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert-wi-fi/prod_white_paper0900aecd80

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-power-levels.html>

<https://www.wi-fi.org/file/wi-fi-alliance-unlicensed-spectrum-in-the-us>

最新問題: 66

クライアントが無線LAN内で1つのアクセスポイントから別のアクセスポイントへローミングする場合、どのような変更が発生しますか？

- A.** 802.11フレームの宛先MACアドレスを変更します。
- B.** SSIDを新しいアクセスポイントのSSIDと一致するように変更します。
- C.** デフォルトゲートウェイを新しいアクセスポイントのIPアドレスに変更します。
- D.** 新しいワイヤレス コントローラーの SSID との関連付けを変更します。

Answer: ([解答を表示する](#))

クライアントがアクセスポイント間をローミングする場合、802.11フレームの宛先MACアドレスを、接続先の新しいアクセスポイントに合わせて変更する必要があります。SSIDは通常、無線LAN全体で一貫しているため変更されず、クライアントが同じIPサブネット内に留まっている限り、デフォルトゲートウェイも同じままです。新しいアクセスポイントへの接続には、クライアントが送信するフレームの宛先MACアドレスの更新が必要です。

最新問題: 67

Aruba Centralを使用する際に、ネットワークの健全性に関する問題を解決するための推奨手順を特定し、サポート担当者と詳細情報を共有できる機能は何ですか？

- A.** 概要ダッシュボード
- B.** OAIOps
- C.** アラートとイベント
- D.** 監査証跡

Answer: B ([メッセージを残す](#))

OAIOpsは、Aruba Centralの機能の一つで、人工知能と機械学習を用いてネットワークの状態に関する問題を解決するための推奨手順を特定し、サポート担当者と詳細な情報を共有できるようにします。OAIOpsは、ネットワークパフォーマンス、根本原因分析、異常検知、プロアクティブなアラート、および自動修復アクションに関する洞察を提供します。また、OAIOpsはAruba User Experience Insight (UXI) センサーと統合され、有線および無線ネットワーク全体でユーザーエクスペリエンスを測定および改善します。

参考資料 https://www.arubanetworks.com/assets/ds/DS_ArubaCentral.pdf

最新問題: 68

チャネル幅が同じ5GHz帯と6GHz帯のチャネルを比較する場合、正しい記述はどれですか？

- A.** 5GHzチャネルは、6GHzチャネルと比較して、伝送距離は同じですが、クライアントに提供するスループットが異なります。
- B.** 5GHzチャネルは、6GHzチャネルと比較して伝送距離が異なり、クライアントに提供するスループットも異なります。
- C.** 5GHzチャネルは、6GHzチャネルと比較して、伝送距離が同じで、クライアントに同じスループットを提供します。
- D.** 5GHzチャネルは6GHzチャネルと比較して伝送距離が異なりますが、クライアントに提供するスループットは同じです。

Answer: B ([メッセージを残す](#))

説明

チャンネル幅が同じ5GHzチャンネルと6GHzチャンネルを比較する場合、正しい記述は、5GHzチャンネルは6GHzチャンネルと比較して伝送距離が異なり、クライアントに提供するスループットも異なる、というものである。

この記述は、高周波信号は減衰が大きい傾向があるという事実を反映しています。減衰とは、伝送距離や物体または媒体を通過する際に信号強度が減少する現象を指す一般的な用語です。減衰が大きいということは、高周波信号は低周波信号よりも伝送距離が短く、スループットが低いことを意味します。この記述に関するいくつかの事実は次のとおりです。

5GHz帯のチャンネルは6GHz帯のチャンネルよりも周波数が低いため、6GHz帯のチャンネルよりも減衰が少ない。

減衰が少ないということは、5GHz帯のチャンネルは、同じチャンネル幅の6GHz帯のチャンネルよりも、より長い距離を伝送でき、クライアントに対してより高いスループットを提供できることを意味します。

しかし、屋内環境では、信号伝搬に影響を与える障害物や反射が多いため、5GHz帯と6GHz帯のチャンネル間の距離とスループットの差はそれほど大きくない可能性がある。

5GHzチャンネルと比較して6GHzチャンネルを使用する利点は、5GHzチャンネルよりも利用可能なスペクトルが多く、干渉が少なく、重複しないチャンネルが多いことです。

他の選択肢が正しくない理由は以下のとおりです。

5 GHz チャンネルは 6 GHz チャンネルと同じ距離を伝送し、クライアントに異なるスループットを提供します。このオプションは誤りです。高周波信号は減衰が大きいため、5 GHz チャンネルは 6 GHz チャンネルと同じ距離を伝送しません。

5 GHz チャンネルは 6 GHz チャンネルと同じ距離を伝送し、クライアントに同じスループットを提供します。このオプションは誤りです。高周波信号は減衰が大きいため、5 GHz チャンネルは 6 GHz チャンネルと同じ距離を伝送したり、同じスループットを提供したりすることはありません。

5 GHz チャンネルは、6 GHz チャンネルと比較して伝送距離が異なり、クライアントに同じスループットを提供します。このオプションは、5 GHz チャンネルが 6 GHz チャンネルと同じスループットを提供しないため、誤りです。

高周波信号は減衰が大きいため、6GHz帯のチャンネルが使用される。

参考文献 <https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e>

<https://www.wi-fi.org/file/wi-fi-alliance-spectrum-needs-study>

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-power-levels.html>

https://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert-wi-fi/prod_white_paper0900aecd80

最新問題: 69

Aruba CX 8325 の `show ip route` 出力に基づくと、`0.20.0.0/22, vrf default via 10.1.1.1, [110/200]` はどのようなタイプのルートですか？

- A. 接続済み
- B. ローカル
- C. OSPF
- D. 静的

Answer: C ([メッセージを残す](#))

ルート `0.20.0.0/22, vrf default via 10.1.1.1, [110/200]` は、OSPFルートであることを示しています。これは、管理距離とメトリック `[110/200]` によって証明されます。ここで、110はOSPFルートのデフォルトの管理距離です。

最新問題: 70

Aruba CX 8325 の `show ip route` 出力に基づくと、`0.20.0.0/22, vrf default via 10.1.1.1, [110/200]` はどのようなタイプのルートですか？

- A. 接続済み
- B. ローカル
- C. OSPF
- D. 静的

Answer: C ([メッセージを残す](#))

ルート `0.20.0.0/22, vrf default via 10.1.1.1, [110/200]` は、OSPF ルートであることを示しています。

これは、管理距離とメトリック `110/200` によって証明されます。ここで、110はOSPFルートのデフォルトの管理距離です。

最新問題: 71

複数の種類のIoTデバイスに対して無線アクセスを設定する必要がありますが、その中には802.112のみで動作するものもあります。

11b. 各クラスは固有のPSKを持ち、役割に応じて異なるセキュリティポリシーを適用する必要があります。デバイスには15～20種類の異なるクラスがあり、パフォーマンスを最適化する必要があります。これらの要件を満たすオプションはどれですか？

- A. 5GHz帯と6GHz帯を使用し、各IoTクラスごとにMPSK方式による単一のSSIDを使用
- B. 2.4GHz帯と5GHz帯を使用し、各IoTクラスごとにMPSK方式による単一SSIDを使用
- C. 5GHz帯と6GHz帯を使用し、IoTクラスごとに固有のPSKを持つ個別のSSIDを使用する
- D. 2.4GHz帯と5GHz帯を使用し、各IoTクラスごとに固有のPSKを持つ個別のSSIDを使用します。

Answer: (解答を表示する)

説明

要件を満たすオプションは、2.4GHz帯と5GHz帯を使用して、IoTクラスごとに固有のPSKを持つ個別のSSIDを作成することです。このオプションには、以下の利点があります。

各IoTクラスには固有のPSK（事前共有鍵があり、これを用いて役割に応じて異なるセキュリティポリシーを適用できます。これにより、WLANネットワークのセキュリティと柔軟性が向上します。

個別のSSIDを使用することで、異なるIoT機器クラスの分離と管理が向上します。これにより、無線LANネットワークのパフォーマンスと拡張性が向上します。

2.4 GHz 帯と 5 GHz 帯の両方を使用することで、2.4 GHz 帯を使用する 802.11b のみで動作する IoT デバイスとの下位互換性が確保されます。また、5 GHz 帯を使用する 802.11a、802.11g、802.11n、または 802.11ac をサポートする IoT デバイスに対して、より高いスループットと干渉の低減が実現します。

他の選択肢は要件を満たしていません。理由は以下のとおりです。

5GHz帯と6GHz帯を使用する各IoT機器クラスごとに、MPSK方式の単一SSIDを使用する方法 :このオプションは、2.4GHz帯を使用する802.11bのみで動作するIoT機器をサポートしていません。また、単一SSIDでは異なるIoT機器クラス間で同一チャネル干渉や輻輳が発生する可能性があるため、WLANネットワークのパフォーマンスも最適化されません。

2.4 GHz 帯と 5 GHz 帯を使用して、各 IoT クラスごとに MPSK を使用した単一の SSID: このオプションでは、単一の SSID が異なる IoT クラス間で同一チャネル干渉や輻輳を引き起こす可能性があるため、WLAN ネットワークのパフォーマンスが最適化されません。

各IoTクラスごとに固有のPSKを持つ個別のSSIDを使用し、5GHz帯と6GHz帯を使用します。このオプションは、2.4GHz帯を使用する802.11bのみで動作するIoTデバイスをサポートしていません。

参考文献: 1 https://en.wikipedia.org/wiki/IEEE_802.11b-1999 2

<https://www.lifewire.com/wireless-standards-802-11a-802-11b-gn-and-802-11ac-816553>

最新問題: 72

ネットワーク技術者がHPE Aruba Networking Centralを使用してネットワークの問題をトラブルシューティングしています。

トラブルシューティングを開始する際に、問題を確認 認識するために使用できるダッシュボードはどれですか？

- A. アラートとイベントのダッシュボード
- B. 監査証跡ダッシュボード
- C. レポートダッシュボード
- D. ツールダッシュボード

Answer: (解答を表示する)

アラートとイベントのダッシュボードには、デバイスのプロビジョニング、構成、およびユーザー管理に関連するイベントに対して生成されたすべての種類のアラートとイベントが表示されます。設定アイコンを使用して、アラートのカテゴリと重要度に応じてアラートと通知を設定できます。アラートとイベントは、リストビューと概要ビューで表示することもできます。

最新問題: 73

Aruba Centralでグループを作成する際に、ユーザーはどのデバイス構成グループタイプを定義できますか？

(2つ選択してください。)

- A. ESPグループ
- B. セキュリティグループ

- C. ウル基
- D. デフォルトグループ
- E. テンプレートグループ

Answer: D,E ([メッセージを残す](#))

Aruba Centralでは、グループ作成時に、複数のデバイスの設定を管理するためのさまざまな構成グループを定義できます。セキュリティグループを使用すると、デバイス全体に一貫したセキュリティ設定を適用でき、テンプレートグループを使用すると、定義済みの構成をデバイスに適用できます。これらのグループは、Aruba Centralにおけるネットワークデバイスの展開と管理を効率化するのに役立ちます。

最新問題: 74

WPA 4ウェイハンドシェイクの機能を正しい順序で列挙してください。

Function

Distributes an encrypted GTK to the client

Exchanges messages for generating PTK

Proves knowledge of the PMK

Sets first initialization vector (IV)

Order

>

<

Answer:

Function

Distributes an encrypted GTK to the client

Exchanges messages for generating PTK

Proves knowledge of the PMK

Sets first initialization vector (IV)

Order

>

<

- PMKに関する知識を証明する
- PTK生成のためのメッセージ交換
- 暗号化されたGTKをクライアントに配布します
- 最初の初期化ベクトル (IV)を設定します。

最新問題: 75

HPE Aruba Networking Centralを使用すると、ネットワークの健全性に関する問題を解決するための推奨手順を特定し、サポート担当者と詳細情報を共有できます。

- A. 概要ダッシュボード
- B. AIOps
- C. アラートとイベント
- D. 監査証跡

Answer: B ([メッセージを残す](#))

Aruba CentralのAIOpsは、ネットワークデータを分析して問題を特定し、推奨される修復手順を提供するとともに、トラブルシューティングのために詳細な診断情報をサポートチームと共有できるようにします。

最新問題: 76

Aruba APの無線ステータスLEDがオレンジ色に点灯している場合、何を示していますか？

- A. スイッチから供給されるPoE電力が不足しているため、APの2つの無線機器両方に電力を供給できません。
- B. 無線機はメッシュモードで動作しています
- C. この無線機は5GHz帯のみで動作します。
- D. 無線機はモニターモードまたはスペクトル分析モードで有効になっています。

Answer: D ([メッセージを残す](#))

説明

Aruba AP アクセス ポイント (AP) の無線ステータス LED がオレンジ色に点灯している場合、無線がモニター モードまたはスペクトル分析モードで有効になっていることを示します。アクセス ポイント (AP) は、Wi-Fi またはその他の無線規格を使用して無線デバイスを有線ネットワークに接続するデバイスです。AP は無線信号の送信機および受信機として機能し、特定のエリアに無線カバレッジを提供します。AP は、ルート、リピーター、ブリッジ、メッシュなどのさまざまなモードで動作できます。AP は、セキュリティ、QoS、ローミング、ロード バランシングなどのさまざまな機能もサポートできます。AP はスタンドアロン デバイスとして動作することも、コントローラまたはクラウド サービスによって管理することもできます。AP は、show ap active、show ap database、show ap bss-table などのコマンドを使用して確認できます。モニターモードは、AP がすべてのチャネルをスキャンして、無線トラフィック、干渉、不正デバイスなどに関する情報を収集できるモードです。スペクトラム分析モードは、AP がすべてのチャネルをスキャンして、RF 環境、ノイズ源、チャネル利用率などに関する情報を収集できるモードです。無線周波数 (RF) 無線周波数 (RF) は、3 kHz から 300 GHz までの周波数を持つ電磁波を指す用語です。RF 波は、通信、放送、レーダー、ナビゲーション、リモートコントロールなど、さまざまな目的で使用されます。RF 波は、振幅、周波数、または位相を変更して変調し、情報をエンコードできます。RF 波は、減衰、反射、屈折、回折、散乱、干渉、ノイズなど、さまざまな要因の影響を受けることもあります。RF 波は、スペクトラムアナライザ、パワーメータ、アンテナなどのデバイスを使用して測定できます。どちらのモードも、無線パフォーマンスのトラブルシューティングと最適化に役立ちますが、無線での通常のデータ送信と受信を無効にします。

Aruba APの無線ステータスLEDがオレンジ色に点灯しない理由は以下のとおりです。

スイッチから AP の両方の無線に電力を供給するのに十分な PoE が供給されていません: このオプションは、PoE が不足しているため偽です。Power over Ethernet (PoE) Power over Ethernet (PoE) は、ネットワーク デバイスが同じ Ethernet ケーブルを介して電力とデータを受信できるようにする技術です。PoE により、IP 電話、カメラ、アクセス ポイントなどのデバイスに個別の電源とケーブルが不要になります。

PoE は IEEE 802.3af および IEEE 802.3at 規格で定義されており、さまざまな電力クラスとモードをサポートしています。PoE は、電源供給機器 (PSE) として機能するスイッチまたはインジェクタによって供給され、受電機器 (PD) として機能するデバイスによって受信されます。PoE は、show power inline、show power-over-ethernet、debug ip device tracking などのコマンドを使用して確認できます。Aruba AP の電源ステータス LED は、オレンジ色の点滅で示され、オレンジ色の無線ステータス LED は点灯しません。オレンジ色の電源ステータス LED が点滅している場合は、AP がスイッチまたはインジェクタから十分な電力を受信しておらず、正常に動作できないことを意味します。緑色の電源ステータス LED が点灯している場合は、AP がスイッチまたはインジェクタから十分な電力を受信しており、正常に動作できることを意味します。

無線がメッシュモードで動作しています: このオプションは偽です。Aruba AP では、無線がメッシュモードで動作している場合は、無線ステータス LED が緑色に点灯し、オレンジ色の点灯では示されません。無線ステータス LED が緑色に点灯している場合は、無線が通常モードまたはメッシュモードで動作しており、割り当てられたチャネルでデータを送受信できることを意味します。メッシュモードは、有線接続を必要とせずに、AP が他の AP とワイヤレスで接続してメッシュネットワークを形成できるモードです。

無線機は 5 GHz 帯域のみで動作しています: このオプションは誤りです。5 GHz 帯域のみで動作する無線機は、Aruba AP の無線ステータス LED が青色に点灯することで示され、オレンジ色の点灯では示されません。青色の無線ステータス LED が点灯している場合は、無線機がデュアルバンドモードで動作しており、2.4 GHz 帯域と 5 GHz 帯域の両方でデータの送受信が可能であることを意味します。

参考文献：

https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/ap-led-behavior.htm

https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/troubleshooting/ap-monitor-m

https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/troubleshooting/ap-spectrum

有効な **HPE6-A85** 問題集は GoShiken.com が提供された合格しやすい HPE6-A85 試験問題集！ GoShiken.com が最新の **HPE6-A85** 試験問題集を提供しています。GoShiken.com HPE6-A85 試験問題は最新で、解答が正確でございます。最新の GoShiken.com HPE6-A85 問題集をゲットする人はこちら: <https://www.goshiken.com/HP/HPE6-A85-mondaishu.html> (134**30%OFF**問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 77

Aruba CXスイッチでOSPFダイナミックルーティングプロトコルを使用する場合、ルートを交換するために隣接デバイス間で一致させる必要がある設定は何ですか？

- A. こんにちはタイマー
- B. DR構成
- C. ECMP法
- D. BDR構成

Answer: (解答を表示する)

OSPF (Open Shortest Path First)は、IPネットワークのルーティングトポロジを作成するために階層構造を使用するリンクステートルーティングプロトコルです。OSPFルータは、各インターフェイスで定期的送信されるHelloパケットを使用して、ネイバーとルーティング情報を交換します。隣接関係（隣接関係とは、ルーティング情報を交換するために選択されたネイバールータ間で形成される関係です）を確立するには、OSPFルータは、インターフェイスでHelloパケットが送信される頻度を指定するHelloタイマーなど、いくつかのパラメータについて合意する必要があります。ネイバールータ間でHelloタイマーが一致しない場合、隣接関係は形成されず、ルートも交換されません。参照：

<https://www.arubanetworks.com/techdocs>

/ArubaOS_86_Web_Help/Content/arubaos-solutions/osfp/osfp.htm

最新問題: 78

複数の20MHz幅の802.11チャンネルをバインドするのはどのような場合ですか？

- A. 信号対雑音比 (SNR)を下げる
- B. クライアントとAP間のスループットを向上させる
- C. 高可用性APグループをプロビジョニングする
- D. 高利得無指向性アンテナを利用する

Answer: B (メッセージを残す)

複数の20MHz幅の802.11チャンネルを結合する技術は、より広い帯域幅のチャンネルを作成し、より高いデータレートの伝送をサポートするものです。これにより、より多くのスペクトルリソースを活用し、干渉を低減することで、クライアントとアクセスポイント間のスループットを向上させることができます。

最新問題: 79

ClearPassのセルフサービス登録ページを使用して、ヘッドレスデバイス用の複数事前共有キー (MPSK)を生成する際に必要な情報は何か？

- A. デバイスの型番
- B. デバイスのMACアドレス
- C. デバイスのIPアドレス
- D. デバイスのOSタイプ

Answer: B (メッセージを残す)

ClearPassのセルフサービス登録ページを使用してヘッドレスデバイス用のマルチプル事前共有キー (MPSK)を生成する場合、デバイスのMACアドレスが必要です。MPSKは、デバイスのMACアドレスに固有のPSKを関連付けることで、ユーザーインターフェースを持たないデバイスでも認証を行う方法を提供します。

最新問題: 80

セキュリティで保護されたエンタープライズモードの無線LANに接続する場合、802.1x認証プロセスはいつ開始されますか？

- A. ファイアウォールポリシーがセッションに適用された後
- B. クライアントが802.11アソシエーションを完了した後
- C. キャプティブポータル認証が完了した後
- D. WPA 4ウェイハンドシェイクが完了した後

Answer: B (メッセージを残す)

802.1x認証プロセスは、クライアントデバイスがアクセスポイントとの802.11接続を完了した後、WPA 4ウェイハンドシェイクの前に開始されます。これはEAP（拡張認証プロトコル）プロセスの一部であり、ネットワークへの完全なアクセスを許可する前にデバイスを認証します。

最新問題: 81

既存のIAP-315アクセスポイントを運用しているネットワーク管理者がAruba Centralに関心を持っており、特定の機能に必要なライセンスを知りたいと考えています。機能ごとに必要なライセンスを一致させてください（一致したライセンスは複数回使用できます）。

AdvancedFoundation

Answer Area

Alerts on config changes via email

Group-based firmware compliance

Heat maps of deployed APs

Live upgrades of an AOS10 cluster

Answer:

AdvancedFoundation

Answer Area

Foundation

Alerts on config changes via email

Foundation

Group-based firmware compliance

Advanced

Heat maps of deployed APs

Advanced

Live upgrades of an AOS10 cluster

Explanation:

a) 電子メールによる構成変更のアラート - Foundation b) グループベースのファームウェア準拠 - Foundation c) 展開された AP のヒート マップ - Advanced d) AOS10 クラスタのライブ アップグレード - Advanced Aruba Central ライセンス ガイド 1 によると、Foundation ライセンスは、構成、監視、アラート、レポート、ファームウェア管理などの基本的なデバイス管理機能を提供します。Advanced ライセンスは、AI インサイト、WLAN サービス、NetConductor Fabric、ヒート マップ、ライブ アップグレードなどの追加機能を提供します。

<https://www.arubanetworks.com/techdocs/central/2.5.3/content/pdfs/licensing-guide.pdf>

最新問題: 82

適切な使用事例に合わせてスイッチング技術を選択する。

TECHNOLOGY	USE CASE
802.1Q	Controls the dynamic addition and removal of ports to groups
802.1X	Tags Ethernet frames with an additional VLAN header
LACP	Used to authenticate EAP-capable clients on a switch port
LLDP	Used to identify a voice VLAN to an IP phone

Answer:

TECHNOLOGY	USE CASE
802.1Q	Controls the dynamic addition and removal of ports to groups
802.1X	Tags Ethernet frames with an additional VLAN header
LACP	Used to authenticate EAP-capable clients on a switch port
LLDP	Used to identify a voice VLAN to an IP phone

Explanation:

ユースケース: a) ポートのグループへの動的な追加と削除を制御します テクノロジー: 3) LACP ユースケース: b) イーサネット フレームに追加の VLAN ヘッダーをタグ付けします テクノロジー: 1) 802.1Q ユースケース: c) スイッチポート上の EAP 対応クライアントの認証に使用します テクノロジー: 2) 802.1X ユースケース: d) IP 電話に音声 VLAN を識別するために使用します テクノロジー: 4) LLDP 次の表は、スイッチング テクノロジーとそのユースケースをまとめたものです。

テクノロジー

使用事例

1) 802.1Q

802.1Q は、ネットワーク上で仮想 LAN (VLAN) を作成および管理する方法を定義する標準規格です。VLAN を使用すると、ネットワーク管理者はネットワークを論理的に異なるブロードキャスト ドメインに分割でき、セキュリティ、パフォーマンス、および管理性が向上します。802.1Q では、イーサネット フレームに VLAN 識別子 (VID) を含む追加の VLAN ヘッダーを付加します。この VID は、フレームがどの VLAN に属するかを示します 1。

2) 802.1X

802.1Xは、ネットワーク上でポートベースのネットワークアクセス制御 (PNAC)を提供する方法を定義する規格です。

PNAC を使用すると、ネットワーク管理者はデバイスにネットワーク リソースへのアクセスを許可する前に、デバイスを認証および認可できます。802.1X は、拡張認証プロトコル (EAP) を使用して、サブリカント (ネットワークにアクセスしたいデバイス)、オーセンティケータ (スイッチなど、ネットワークへのアクセスを制御するデバイス)、および認証サーバー (RADIUS サーバーなど、サブリカントの資格情報を検証するデバイス) の間で認証メッセージを交換します 2。

3) LACP

LACPIはLink Aggregation Control Protocolの略で、IEEE 802.3ad規格の一部であり、複数の物理リンクを単一の論理リンク (リンクアグリゲーショングループ (LAG)またはEtherChannelとも呼ばれる)にまとめる方法を定義します。LAG は、ネットワーク接続の帯域幅の拡大、負荷分散、冗長性を提供します。LACPは、グループへのポートの動的な追加と削除を制御し、互換性のある構成を持つポートのみがLAGを形成できるようにします。

4) LLDP

LLDPはLink Layer Discovery Protocolの略で、ネットワーク上の隣接デバイスに関する情報を検出して通知する方法を定義するIEEE 802.1AB規格の一部です。LLDPはOSIモデルのレイヤ2で動作し、TLV (タイプ長さ値)を使用して、デバイス名、ポート番号、VLAN ID、機能、電力要件などの情報を交換します。LLDPを使用すると、音声VLAN IDと優先度を含むTLVを送信することで、IP電話に音声VLANを識別させることができます。

参考文献: 1 https://en.wikipedia.org/wiki/IEEE_802.1Q 2 https://en.wikipedia.org/wiki/IEEE_802.1X 3 https://en.wikipedia.org/wiki/Link_aggregation https://en.wikipedia.org/wiki/Link_layer_discovery_protocol

- 最新問題: 83
- 推奨されるVSFトポロジはどれですか？ (2つ選択してください。)
- A. スター
 - B. デイジーチェーン+MAD
 - C. フルメッシュ
 - D. フルメッシュ+MAD
 - E. リング

Answer: (解答を表示する)

ただし、Arubaスイッチで推奨されるVSFトポロジは、デイジーチェーン+MADとリングのみです。

これらはVSFスタックに高い可用性と冗長性を提供します。MAD (Multiple Active Detection)は、VSFスタックにおけるスプリットブレイン状態を検出し、解決するためのメカニズムです。

- 最新問題: 84
- WPA 4ウェイハンドシェイクの機能を正しい順序で列挙してください。

Function	Order
Distributes an encrypted GTK to the client	Exchanges messages for generating PTK
Exchanges messages for generating PTK	Proves knowledge of the PMK
Proves knowledge of the PMK	Distributes an encrypted GTK to the client
Sets first initialization vector (IV)	Sets first initialization vector (IV)

Answer:

Function	Order
Distributes an encrypted GTK to the client	Exchanges messages for generating PTK
Exchanges messages for generating PTK	Proves knowledge of the PMK
Proves knowledge of the PMK	Distributes an encrypted GTK to the client
Sets first initialization vector (IV)	Sets first initialization vector (IV)

Explanation:

WPA 4ウェイハンドシェイクの正しい順序は以下のとおりです。

PTK生成のためのメッセージ交換

PMKに関する知識を証明する

暗号化されたGTKをクライアントに配布します

最初の初期化ベクトル (IV)を設定します。

このプロセスは、クライアントとアクセスポイントの両方が正しい認証情報（PMKなど）を持っていることを確認し、データの暗号化と復号に使用される一時的な鍵を確立し、ハンドシェイクの時点でクライアントが実際に稼働して存在していることを確認するように設計されています。

最新問題: 85

レイヤ3のIPv4パケットヘッダーで、レイヤ3のルートループを軽減するために使用されるのはどれですか？

- A. チェックサム
- B. 生きる時間
- C. プロトコル
- D. 宛先IPアドレス

Answer: B ([メッセージを残す](#))

レイヤ 3 のルートループを軽減するために使用されるレイヤ 3 IPv4 パケット ヘッダーのフィールドは、Time To Live (TTL) です。TTL は 8 ビットのフィールドで、パケットが破棄される前に通過できる最大ホップ数を示します。TTL は送信元デバイスによって設定され、パケットを転送する各ルータによって 1 ずつ減らされます。TTL がゼロになると、パケットは破棄され、ICMP メッセージが送信元デバイスに返送されます。ICMP は、IP ネットワークのエラー報告および診断機能を提供するネットワーク プロトコルです。ICMP は、エコー要求と応答 (ping)、宛先到達不能、時間超過、パラメータの問題、送信元クエンチ、リダイレクトなどのメッセージを送信するために使用されます。ICMP メッセージは IP データ グラムにカプセル化され、タイプ、コード、チェックサム、識別子、シーケンス番号、データなどのフィールドを含む特定の形式になっています。ICMP メッセージは、ping、traceroute、debug ip icmp などのコマンドを使用して検証できます。TTLはレイヤーを軽減するために使用されます

3つのルートループは、ループ状のネットワークポロジでパケットが無限に循環するのを防ぐためです。TTLは、ネットワークリソースの節約と、ループしたパケットによって引き起こされる輻輳の回避にも役立ちます。

その他のオプションは、レイヤ3 IPv4パケットヘッダーのフィールドではありません。理由は以下のとおりです。

- チェックサム :チェックサムは、IPヘッダーの整合性を検証するために使用される16ビットのフィールドです。チェックサムは送信元デバイスによって計算され、宛先デバイスによってIPヘッダー内のすべてのフィールドの値に基づいて検証されます。チェックサムはパケットが通過できるホップ数を制限しないため、レイヤ3のルーティングループを軽減する効果はありません。
- プロトコル: プロトコルは、IP データグラムによって運ばれるペイロードの種類を示す 8 ビットのフィールドです。プロトコルは、TCP など、データ伝送に IP を使用する上位層プロトコルを識別します。伝送制御プロトコル (TCP) は、異なるデバイス上のアプリケーション間でデータの信頼性が高く、順序が付けられ、エラーチェックされた配信を提供する接続指向のトランスポート層プロトコルです。TCP は、3 ウェイ ハンドシェイクを使用して 2 つのエンドポイント間の接続を確立し、シーケンス番号、確認応答、ウィンドウイングを使用してデータの配信とフロー制御を保証します。TCP はまた、パケット損失と輻輳を処理するために、再送信、輻輳回避、高速回復などのメカニズムを使用します。TCPはデータをセグメントと呼ばれるより小さな単位に分割し、セグメントはIPデータグラムにカプセル化され、送信元ポート、宛先ポート、シーケンス番号、確認応答番号、ヘッダー長、フラグ、ウィンドウサイズ、チェックサム、緊急ポインタ、オプション、データなどのフィールドを含む特定のフォーマットを持ちます。TCPセグメントは、telnet、ftp、ssh、debug ip tcp transactionsなどのコマンドを使用して検証できます。UDPユーザーデータグラムプロトコル (UDP) ユーザーデータグラムプロトコル (UDP)は、コネクションレスのトランスポート層プロトコルであり、

最新問題: 86

アクセスポイントからの信号が物体を通過する際に吸収されて弱まると、何が起こるのでしょうか？

- A. APIはボンディングチャネルを使用してクライアントへの遅延を低減します。
- B. 信号対雑音比 (SNR)が増加する
- C. 信号対雑音比 (SNR)が低下する
- D. Aruba Centralは、クライアントを動的に近隣のアクセスポイントに移動します。

Answer: C ([メッセージを残す](#))

説明

信号対雑音比 (SNR)は、目的信号のレベルと背景雑音のレベルを比較する指標です。SNRは信号電力と雑音電力の比として定義され、多くの場合デシベル (dB) で表されます。SNRが高いほど信号は明瞭で検出や解釈が容易ですが、SNRが低いほど信号は雑音によって劣化または不明瞭になり、識別や回復が困難になる可能性があります1。アクセスポイント (AP)からの信号が壁や家具などの物体を通過する際に吸収されて弱まると、信号電力は低下します。これによりSNRが低下し、無線接続の品質に影響します。雑音電力は、他のAPや同じ周波数帯域で動作するデバイスなどの他のソースからの干渉によって増加することもあります2。したがって、APからの信号が物体を通過する際に吸収されて弱まるとSNRが低下するというのが正解です。参考文献 :1

https://en.wikipedia.org/wiki/Signal-to-noise_ratio 2

https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_%28SNR%29

最新問題: 87

IPカメラ、アクセスポイント、その他のPoEデバイスを導入する際に、スイッチポートのPoE優先度を動的に設定するにはどうすればよいでしょうか？

- A. デバイスプロビジョニングのプロファイリングを有効にする
- B. PoE電源管理をダイナミックモードに設定する
- C. スイッチモジュールでクイックPoEを有効にする
- D. PoE電源管理をクラスベースモードに設定する

Answer: D ([メッセージを残す](#))

最新問題: 88

ディストリビューションおよびレイヤ 3 サービスに使用される 6300M スイッチのスタック ペアでネットワークを構成しています。ディストリビューション スタックの下流に接続された CX6200 スイッチのマルチ アクセス スタックで使用されるユーザー用の新しい VLAN を作成します。これと同様の VLAN/サブネットを複数作成し、マルチ アクセス スタックで使用します。この VLAN に関連付けられるサブネットのルーティング可能なインターフェイスを正しく構成する方法はどれですか？

- A. ダウンストリームスイッチごとに、6300Mスタック上のサブネット内に物理的にルーティングされたインターフェースを作成します。
- B. 各ダウンストリームスイッチのサブネット内にSVIを作成する
- C. 6300Mスタック上のサブネットにSVIを作成し、各ダウンストリームスイッチスタックの管理アドレスを同じサブネット内の異なるIPアドレスに割り当てます。
- D. 6300Mスタック上のサブネットにSVIを作成します。

Answer: D ([メッセージを残す](#))

説明

この VLAN に関連付けるサブネットのルーティング可能なインターフェイスを正しく構成するには、SVI を作成します。スイッチド仮想インターフェイス (SVI) は、スイッチ上の仮想インターフェイスで、VLAN を表し、その VLAN のレイヤ 3 ルーティング機能を提供します。SVI は、VLAN 間ルーティングを有効にしたり、VLAN 内のホストにゲートウェイ アドレスを提供したり、VLAN に ACL または QoS ポリシーを適用したりするために使用されます。

SVI は、インターフェース ポートの節約、ケーブル コストの削減、ネットワーク設計の簡素化など、物理的なルーティング インターフェイスに比べていくつかの利点があります。SVI は通常、VLAN ID (例: vlan 10) に従って番号が付けられ、VLAN のサブネット内で IP アドレスが割り当てられます。SVI は、interface vlan、ip address、no shutdown などのコマンドを使用して作成および構成できます。SVI は、6300M スタックのサブネットに show ip interface brief、show vlan、show ip route などのコマンドを使用して確認できます。

SVIは、スイッチ上の仮想インターフェースであり、VLANを表し、そのVLANに対してレイヤ3ルーティング機能を提供します。6300MスタックのサブネットにSVIを作成することで、スイッチはそのVLAN内のユーザーのゲートウェイとして機能し、異なるサブネット間のVLAN間ルーティングが可能になります。また、6300MスタックのサブネットにSVIを作成することで、ルーティングに必要な物理インターフェースとケーブルの数を減らすことができ、ネットワーク設計と管理が簡素化されます。

他のオプションは、このVLANIに関連付けるサブネットのルーティング可能なインターフェースを設定する正しい方法ではありません。理由は以下のとおりです。

6300Mスタック上のサブネットに、ダウンストリームスイッチごとに物理的にルーティングされたインターフェースを作成する :このオプションは誤りです。6300Mスタック上のサブネットに、ダウンストリームスイッチごとに物理的にルーティングされたインターフェースを作成すると、ダウンストリームスイッチごとに1つの物理ポートとケーブルを使用する必要があり、インターフェイスリソースを消費し、ケーブルコストが増加します。また、6300Mスタック上のサブネットに、ダウンストリームスイッチごとに物理的にルーティングされたインターフェースを作成すると、インターフェイスごとに個別のルーティング構成とポリシーが必要になるため、ネットワークの設計と管理が複雑になります。各ダウンストリームスイッチのサブネットにSVIを作成する :このオプションは誤りです。各ダウンストリームスイッチのサブネットにSVIを作成しても、各ダウンストリームスイッチは自身のVLANのゲートウェイとしてのみ機能するため、異なるサブネット間のVLAN間ルーティングは有効になりません。また、各ダウンストリームスイッチのサブネットにSVIを作成すると、同じサブネット内に重複したIPアドレスが作成され、IPアドレスの競合やルーティングエラーが発生します。

6300M スタックのサブネットに SVI を作成し、各ダウンストリーム スイッチ スタックの管理アドレスを同じサブネット内の異なる IP アドレスに割り当てます。このオプションは正しくありません。6300M スタックのサブネットに SVI を作成し、各ダウンストリーム スイッチ スタックの管理アドレスを同じサブネット内の異なる IP アドレスに割り当てても、各ダウンストリーム スイッチは自身の VLAN のゲートウェイとしてのみ機能するため、異なるサブネット間の VLAN 間ルーティングは有効になりません。また、6300M スタックのサブネットに SVI を作成し、各ダウンストリーム スイッチ スタックの管理アドレスを同じサブネット内の異なる IP アドレスに割り当てても、同じサブネット内に不要な IP アドレスが作成され、IP スペースが無駄になり、ネットワーク管理が複雑になります。

参考資料 <https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/index.html>

<https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscfg/l3-routing/l3-routing-ove>

最新問題: 89

ドラッグ&ドロップ

各要件に合わせて、最も費用対効果の高いケーブル配線オプションを選択してください。すべての長さは、パッチケーブル、サービスループなどを含むケーブルの全長を示します。)

OPTION		REQUIREMENT
Cat 5e cable		100 Gb connection with a length of 10' (3M) between two switches in the data center
Cat 6a cable		1 Gb connection with a length of 100' (30M) between an edge switch and a user desktop
Direct Attach Copper (DAC) cable		10 Gb connection with a length of 200' (60M) between the distribution switch in the main wiring closet and the edge switch in a remote wiring closet
multimode fiber		1 Gb connection with a length of 2km between two switches in different buildings
single mode fiber		

Answer:

OPTION		REQUIREMENT
Cat 5e cable	single mode fiber	100 Gb connection with a length of 10' (3M) between two switches in the data center
Cat 6a cable	Cat 6a cable	1 Gb connection with a length of 100' (30M) between an edge switch and a user desktop
Direct Attach Copper (DAC) cable	Direct Attach Copper (DAC) cable	10 Gb connection with a length of 200' (60M) between the distribution switch in the main wiring closet and the edge switch in a remote wiring closet
multimode fiber	multimode fiber	1 Gb connection with a length of 2km between two switches in different buildings
single mode fiber		

最新問題: 90

顧客環境への新しいAruba 6300Mの導入を依頼されました。オンサイトではなくリモートで作業しています。スイッチのインストールは同僚が行っています。同僚はエッジスイッチを設定するためのリモートコンソールセッションを提供してくれました。インターフェース1/1/51と1/1/52を使用してコアに戻るリンクアグリゲーションを設定するよう依頼されました。プロジェクトのシニアエンジニアは、以下のガイドラインに従ってスイッチと1Qアップリンクを設定するよう依頼しました。

1. VLAN 20をローカルVLANデータベースにMgmtという名前で追加します。
2. 10.1.10/24サブネットのアドレス10を使用して、VLAN 20に管理用のL3 SVIを追加します。
3. アップリンクにLACPモードをアクティブにしてLAG 1を追加します。
4. LAG上でネイティブVLANとしてVLAN 20を使用する
5. すべてのインターフェースがオンになっていることを確認してください。

どの設定スクリプトを使えば目的を達成できますか？

A. Edge1# conf t vlan 20 name Mgmt interface vlan 20 ip address 10.1.1.10/24 no shut interface lag 1 shut vlan access 20 lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut

B. Edgel# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1.1 10/24 no shut interface

1/1/51.1/1/52 shut vlan trunk native 20 vlan trunk allowed all lag 1 lacp mode active interface

1/1/51.1/1/52 閉鎖なし

C. Edge1# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1 1 10/24 no shut interface lag 1 shut vlan trunk native 20 vlan trunk allowed all lacp mode active int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut interface 1/1/51.1/1/52 no shut

D. conf t vlan 20 name Mgmt ip address 10 1 1.10/24 no shut interface lag 1 shut vlan trunk native 1 vlan trunk allowed all lacp mode active int 1/1/51.1/1/52 shut no routing interface lag 1 no shut interface 1/1/51.1/1/52 閉鎖なし

Answer: ([解答を表示する](#))

この設定スクリプトは、シニアエンジニアから提供されたガイドラインに従ってタスクを実行します。具体的には、Mgmt という名前の VLAN 20 を作成し、IP アドレス 10.1.1.10/24 を持つ L3 SVI を VLAN 20 に追加し、LAG を作成します。

1 アップリンクで LACP モードがアクティブになっている場合、LAG のネイティブ VLAN として VLAN 20 を使用し、すべてのインターフェイスが ONであることを保証します。

参考資料: <https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-8F0E7E8B-0F4>

最新問題: 91

Aruba Centralを使用した手動スイッチプロビジョニングに関する記述として正しいのはどれですか？

- A.** 手動プロビジョニングではDHCPは不要で、DNSが必要です
- B.** 手動プロビジョニングではDHCPもDNSも必要ありません
- C.** 手動プロビジョニングにはDHCPが必要で、DNSは不要です
- D.** 手動プロビジョニングにはDHCPとDNSが必要です

Answer: ([解答を表示する](#))

説明

手動プロビジョニングは、DHCPやDNSを使用せずにスイッチをAruba Centralに追加する方法です。この方法では、ユーザーはAruba Centralにスイッチのシリアル番号、MACアドレス、アクティベーションコードを入力し、その後、同じアクティベーションコードとAruba CentralのIPアドレスを使用してスイッチを設定する必要があります。

参考資料: https://help.central.arubanetworks.com/latest/documentation/online_help/content/devices/switches/pr

有効な **HPE6-A85** 問題集は GoShiken.com が提供された合格しやすい HPE6-A85 試験問題集！ GoShiken.com が最新の **HPE6-A85** 試験問題集を提供しています。GoShiken.com HPE6-A85 試験問題は最新で、解答が正確でございます。最新の GoShiken.com HPE6-A85 問題集をゲットする人はこちら: <https://www.goshiken.com/HP/HPE6-A85-mondaishu.html> (**13430%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 92

支店のネットワーク技術者が、新しく設定されたAOS-CXスイッチにVoIP電話を接続しています。ユーザーからは、本社に比べて音声品質が劣るとの苦情が寄せられています。さらに調査したところ、支店のローカル優先度値は1であるのに対し、本社では5であることが判明しました。

AOS-CXスイッチのデフォルトのQoS動作に関する問題点を説明する言葉は何ですか？

- A.** QoSトラストはデフォルトでDSCPに設定され、VoIP電話のローカル優先度値は1にマッピングされます。
- B.** QoS トラストはデフォルトで CoS に設定され、VoIP 電話のローカル優先度値は 1 にマッピングされます。
- C.** QoS トラストはデフォルトで なし」に設定されており、各 VoIP 電話機のローカル優先度は CoS マップエントリ 1 に設定されています。
- D.** QoS トラストはデフォルトで なし」に設定されており、各 VoIP 電話のローカル優先度は CoS マップエントリ 0 に構成されています。

Answer: ([解答を表示する](#))

AOS-CXスイッチでは、QoSトラストモードが設定されていない場合、デフォルトで「なし」に設定されます。VoIP電話機はトラフィックにローカル優先度値を付与しますが、QoSトラストモードが「なし」の場合、デフォルトでCoSマップエントリ1に対応します。支店のローカル優先度値が1であることは、本社と比較してトラフィックの優先順位付けが正しく行われていないことを示している可能性があります。本社ではローカル優先度値が5であり、音声トラフィックの優先順位が高いことを示しています。

最新問題: 93

図を参照してください。どのサーバーが最も少ない量のデータを受信するでしょうか？

Access Points

Switches

MultiEdit

Access to AOS-CX search and custom configuration (editor & express configuration).

Logging

Level

Emergency

Logging Servers (4)

FQDN or IP address	Event Log Level	VRF
10.99.26.25	Emergency	Management
10.100.100.25	Information	Management
172.17.17.43	Warning	Default
192.168.0.56	Debug	Default

- A. 172.17.17.43
- B. 10.100.100.25
- C. 10.99.26.25
- D. 192.168.0.56

Answer: (解答を表示する)

ログサーバーの設定を示す図に基づくと、サーバー172.17.17.43はイベントログレベルが 警告」に設定されているため、受信するデータ量が最も少なくなります。これは、警告以上の深刻度に分類されるイベントのみがログに記録されることを意味し、通常、情報」、デバッグ」、緊急」などの深刻度の低いレベルよりも発生頻度は低くなります。

最新問題: 94

TCPの3ウェイハンドシェイクシーケンスの正しい順序は何ですか？

TCP 3-way Handshake sequence

A flow-controlled connection is established.
The initiating host sends a packet with no data to the target host with a SEQ=1 and sets the SYN flag to 1.
The initiating host sends a packet with SEQ=2, ACK=9, and ACK flag is raised.
The target host sends a packet with ACK=2, SEQ=8, and the SYN and ACK flags are set to 1.

Answer:

TCP 3-Way Handshake sequence

A flow-controlled connection is established.
The initiating host sends a packet with no data to the target host with a SEQ=1 and sets the SYN flag to 1.
The initiating host sends a packet with SEQ=2, ACK=9, and ACK flag is raised.
The target host sends a packet with ACK=2, SEQ=8, and the SYN and ACK flags are set to 1.

Order

The initiating host sends a packet with no data to the target host with a SEQ=1 and sets the SYN flag to 1.
The target host sends a packet with ACK=2, SEQ=8, and the SYN and ACK flags are set to 1.
The initiating host sends a packet with SEQ=2, ACK=9, and ACK flag is raised.
A flow-controlled connection is established.

Explanation:

TCP 3ウェイハンドシェイクのシーケンスは次のとおりです。

- * ステップ 1: 開始ホストは、SEQ=1 のパケットをターゲットホストに送信し、SYN フラグを 1 に設定します。
- * ステップ 2: ターゲット ホストは ACK=2、SEQ=8、SYN および ACK フラグが設定されたパケットで応答します。
- 1.
- * ステップ 3: 開始ホストは、SEQ=2、ACK=9、ACK フラグが 1 に設定されたパケットを送信します。
- * ステップ 4 : 通常制御接続が確立されます。

参考文献 https://en.wikipedia.org/wiki/Transmission_Control_Protocol <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

最新問題: 95

ドラッグアンドドロップ問題

適切なQoS概念とその定義を一致させてください。

QoS concept	Definition
Best Effort Service	A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Class of Service	A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes
Differentiated Services	A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard
WMM	A method where traffic is treated equally in a first-come, first-served manner

Answer:

QoS concept	Definition
Class of Service	A method for classifying network traffic at Layer 2 by marking 802.1Q VLAN Ethernet frames with one of eight service classes
Differentiated Services	A method for classifying network traffic at Layer 3 by marking packets with one of 64 different service classes
WMM	A method for classifying network traffic using access categories based on the IEEE 802.11e QoS standard
Best Effort Service	A method where traffic is treated equally in a first-come, first-served manner

最新問題: 96

CX 6100スイッチが正しく起動しない場合は、トラブルシューティングを行う必要があります。スイッチにアクセスして、OSイメージとServiceOSで使用可能な起動オプションを確認できるオプションを選択してください。

- A. USB-Cコンソールポート
- B. VSFメンバーUSB-Cコンソールポート
- C. USB-Aコンソールポート
- D. VSFコンダクター管理ポート \$SSH使用)

Answer: A (メッセージを残す)

USB-Cコンソールポートは、起動プロセス中にスイッチへの直接コンソールアクセスを提供します。

この接続を介して、起動シーケンスを中断したり、起動メニューにアクセスしたり、トラブルシューティングや復旧のために利用可能なOSイメージやServiceOSオプションを表示または選択したりできます。

最新問題: 97

MACアドレスがB8-31-B5-80-41-4Fのデバイスについて、正しい記述はどれですか？

- A. デバイスのOUIはB8-31-B5、デバイスのNICシリアル番号は80-41-4Fです。
- B. デバイスのOUIはB8-31、デバイスのNICシリアル番号はB5-80-41-4Fです。
- C. デバイスのOUIは80-41-4F、デバイスのNICシリアル番号はB8-31-B5です。
- D. デバイスのOUIはB8-31-B5、デバイスのシリアル番号はMD5ハッシュで80-41-4Fです。

Answer: A (メッセージを残す)

MACアドレスは、組織固有識別子 (OUI)とネットワークインターフェースコントローラ (NIC)シリアル番号の2つの部分に分かれています。OUIはMACアドレスの最初の3オクテットで、製造元固有の値です。NICシリアル番号は最後の3オクテットで、デバイス固有の値です。

したがって、MAC アドレス B8-31-B5-80-41-4F の場合、OUI は B8-31-B5 であり、NIC シリアル番号は 80-41-4F。

最新問題: 98

信号強度を測定する際には、一般的にdBmが用いられ、0dBmは1mWの電力に相当する。

-20 dBmは何に相当しますか？

- A. -1 mW
- B. 0.01 mw
- C. 10 mW
- D. 1mW

Answer: B ([メッセージを残す](#))

dBmは、特定の電力レベルと1mWの比率を表す電力の単位です。dBmをmWに変換する式は、 $P(\text{mW}) = 1\text{mW} * 10^{(P(\text{dBm})/10)}$ です。したがって、-20 dBmは0.01 mWに相当します。 $P(\text{mW}) = 1\text{mW} * 10^{(-20/10)} = 0.01 \text{ mW}$ 参考資料：
https://www.rapidtables.com/convert/power/dBm_to_mW.html

最新問題: 99

認証情報が不明または紛失した状態で、Aruba CXスイッチに物理的にアクセスできます。認証情報を再構築するために考えられる手順は何ですか？ 2つ選択してください。）

- A. コンソール経由でスイッチを接続します。次に、スイッチの電源を入れ直します。
- B. クリアボタンを長押しします。その後、スイッチの電源を入れ直してください。
- C. クリアボタンを長押しします。次に、リセットボタンを2秒間押し続け、両方のボタンを離します。
- D. ワンタイムパスワードについては、Arubaサポートにお問い合わせください。
- E. ブートプロファイル0を使用します。

Answer: B,E ([メッセージを残す](#))

認証情報が不明または紛失した場合にAruba CXスイッチへのアクセスを回復するには、クリアボタンを長押ししてからスイッチの電源を入れ直し、パスワードをリセットします。また、ブートローダーメニューでブートプロファイル0を使用することで、不明な認証情報を含む可能性のある現在の起動設定をバイパスできます。

最新問題: 100

顧客は、Windows 10クライアントを使用するユーザー向けに認証ポリシーを作成する必要があり、さらに、単一のRADIUSセッション内でデバイス認証情報とユーザー認証情報の両方をTorで認証する必要があるという要件があります。この要件に対する適切な解決策は何でしょうか？

- A. ClearPass 6.9 (EAP-TTLS対応)
- B. ClearPass 6.9 (EAP-TLS対応)
- C. ClearPass 6.9 (PEAP対応)
- D. ClearPass 6.9 (EAP-TEAP対応)

Answer: ([解答を表示する](#))

EAP-TEAPは、単一のRADIUSセッション内でデバイス認証とユーザー認証の両方をサポートするトンネルベースの認証方式です。ClearPass 6.9は、Windows 10クライアントの認証方式としてEAP-TEAPをサポートしています。

参考文献：

https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM_UserGuide/EAP-TEAP/EAP-TE

最新問題: 101

MACアドレスがB8-31-B5-80-41-4Fのデバイスについて、正しい記述はどれですか？

- A. デバイスのOUIはB8-31-B5、デバイスのNICシリアル番号は80-41-4Fです。
- B. デバイスのOUIはB8-31、デバイスのNICシリアル番号はB5-80-41-4Fです。
- C. デバイスのOUIは80-41-4F、デバイスのNICシリアル番号はB8-31-B5です。
- D. デバイスのOUIはB8-31-B5、デバイスのシリアル番号はMD5ハッシュで80-41-4Fです。

Answer: (解答を表示する)

MACアドレスは、組織固有識別子（OUI）とネットワークインターフェイスコントローラ（NIC）シリアル番号の2つの部分に分かれています。OUIはMACアドレスの最初の3オクテットで、製造元固有の値です。NICシリアル番号は最後の3オクテットで、デバイス固有の値です。したがって、MACアドレスがB8-31-B5-80-41-4Fの場合、OUIはB8-31-B5、NICシリアル番号は80-41-4Fとなります。

最新問題: 102

ネットワーク技術者が支店の新しいSSIDをテストしています。接続はでき、IPアドレスも取得でき、DNS名も解決できます。しかし、インターネットを閲覧することができません。

支店の既存のSSIDでは、新しいSSIDと同じVLAN上でインターネット接続が正常に機能しています。ワイヤレスクライアントには、インターネットアクセスを許可するための新しい役割が割り当てられているはずです。

ネットワーク技術者は、両方のSSIDが同様に機能することを確認するために、何を検証すべきでしょうか？

- A. 各SSIDの認証と暗号化のパラメータが有効で、同じであることを確認します。
- B. ファイアウォール ポリシーの最後のエントリが暗黙の「すべて拒否」であることを確認します。
- C. 支店のすべてのアクセスポイントで新しいSSIDがブロードキャストされていることを確認します。
- D. 割り当てられたファイアウォール ポリシーを確認し、ルールが正しく、適切な順序になっていることを確認します。

Answer: D (メッセージを残す)

ネットワーク技術者が、新しいSSIDでインターネット接続とDNS解決が成功しているにもかかわらずインターネットアクセスができないという問題に遭遇した場合、新しいSSIDに関連付けられているファイアウォールポリシーを確認する必要があります。ファイアウォールポリシーには、インターネットとの間のトラフィックを許可するルールが含まれている必要があります、意図どおりに適用されるよう正しい順序で設定されている必要があります。

既存のSSIDは正常に機能しているため、両者のファイアウォールルールを比較することは、トラブルシューティングの有効な方法となり得る。

最新問題: 103

ワイヤレスクライアントのローミングに関する決定はどこで行われるのか？

- A. クライアントデバイス
- B. 仮想コントローラー
- C. 発信元APと宛先APによる共同決定
- D. アルバ中央

Answer: A (メッセージを残す)

ワイヤレス クライアントのローミング決定は、主にクライアント デバイス自体によって行われます。クライアント デバイスは、現在の接続の信号強度と品質を監視し、現在の信号が一定のしきい値を下回った場合、またはより良いオプションが利用可能な場合に、別のアクセス ポイント (AP) にローミングすることを決定します。AP とコントローラーは、802.11k や 86.

802.11vでは、ローミングを行うかどうかの最終的な決定は、クライアントデバイスが独自のアルゴリズムと閾値に基づいて行います。

最新問題: 104

Aruba CX6200MのグローバルステータスインジケータLEDがオレンジ色に点滅している場合、それは何を示していますか？

- A. スイッチに回復可能な故障が発生しました。
- B. 自己テストが進行中です。
- C. ファームウェアイメージが破損しています。
- D. スイッチがファームウェアイメージを起動しています。

Answer: C ([メッセージを残す](#))

Aruba CX6200MスイッチのグローバルステータスインジケータLEDがオレンジ色に点滅している場合、通常はスイッチに障害が発生したことを示していますが、復旧可能です。このLEDの動作は、ネットワーク管理者に問題に対処する必要があることを知らせるアラートとして機能しますが、必ずしもスイッチが動作不能であることを意味するものではありません。

最新問題: **105**

CX 8400を使用して仮想スタックを作成する必要があります。VSX ISLに対応したケーブル接続を使用する場合、このシナリオに適した記述を選択してください。

A. SFP28 7m DAC

B. SFP56 3m DAC

C. QSFP28 3m DAC

D. SFP 5m DAC

Answer: C ([メッセージを残す](#))

CX 8400は、高速VSXインタースイッチリンク (ISL)にQSFP28インターフェースを使用します。

3m DACは、VSX環境において2台のスイッチ間で必要となるVSX ISLを確立するための互換性のあるケーブルオプションです。

最新問題: **106**

IPカメラ、アクセスポイント、その他のPoEデバイスを導入する際に、スイッチポートのPoE優先度を動的に設定するにはどうすればよいでしょうか？

A. PoE電源管理をダイナミックモードに設定する

B. PoE電源管理をクラスベースモードに設定する

C. スイッチモジュールでクイックPoEを有効にする

D. デバイスプロビジョニングのプロファイリングを有効にする

Answer: D ([メッセージを残す](#))

説明

プロファイリングとは、ArubaスイッチがMACアドレス、DHCPオプション、LLDP情報などの様々な属性に基づいて、接続されているデバイスを自動的に識別・分類できる機能です。プロファイリングを使用すると、デバイスの種類や電力要件に基づいて、スイッチポートのPoE優先度を動的に設定できます。

例えば、IPカメラはプリンターやPCよりもPoEの優先順位が高くなる場合があります。プロファイリングは、デバイスプロファイルに基づいて、VLAN、ACL、QoSなどの他の構成設定を適用するためにも使用できます。

参考資料: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-ove

有効な **HPE6-A85** 問題集は GoShiken.com が提供された合格しやすい HPE6-A85 試験問題集！ GoShiken.com が最新の **HPE6-A85** 試験問題集を提供しています。GoShiken.com HPE6-A85 試験問題は最新で、解答が正確でございます。最新の GoShiken.com HPE6-A85 問題集をゲットする人はこちら: <https://www.goshiken.com/HP/HPE6-A85-mondaishu.html> (**13430%OFF**問題集溶と正解付きで **30%**w 特別割引コード: **Freepdfdumps**)

最新問題: **107**

Microbranch環境を管理するには、どのタイプのデバイスとグループペルソナが必要ですか？

A. ArubaOS 10 APグループペルソナ

B. ArubaOS 10 ブランチゲートウェイグループペルソナ

C. ArubaOS 8 APグループペルソナ

D. ArubaOS 8 ブランチゲートウェイグループペルソナ

Answer: ([解答を表示する](#))

Arubaネットワークのコンテキストでは、マイクロブランチ環境は、必要な機能に合わせたグループペルソナを使用して管理されます。ArubaOS 10 Branch Gateway Group Personaは、ブランチネットワークの要件に必要な機能と制御を提供するため、マイクロブランチ環境の管理に適したデバイスタイプおよびグループペルソナとなります。

最新問題: 108

顧客が、会社全体のグループベースポリシー (GPO) を介してユーザー証明書とデバイス証明書を実装しました。ネットワーク認証時にクライアント証明書を必要とするEAP方式はどれですか？

- A. EAP-TTLS
- B. EAP-TLS
- C. EAP-TEAP
- D. PEAP

Answer: B (メッセージを残す)

EAP-TLS は、ネットワークへの認証時にクライアント証明書を必要とする認証方式です。公開鍵暗号とデジタル証明書を使用して、クライアントとサーバー間の相互認証を提供します。参照: https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM_UserGuide/EAP-TLS/EAP-TLS.htm EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) は、認証にサーバー側とクライアント側の両方の証明書を必要とする EAP 方式です。ユーザーと認証サーバーの両方が証明書を使用して互いの身元を証明する必要がある相互認証プロセスを使用するため、最も安全な EAP 方式の 1 つと考えられています。グループ ベース ポリシー (GPO) を介してユーザーおよびデバイス証明書を実装すると、クライアント側の証明書に関する EAP-TLS の要件とよく一致します。

最新問題: 109

ホットスポットに関する質問

HPE Aruba Networking CentralでCX 6200Fスイッチを設定しています。管理ポートは専用の帯域外管理ネットワークに接続されています。

次にクリックすべき画像をクリックしてください。

Access PointsSwitches

MultiEdit

Access to AOS-CX search and custom configuration (editor & express configuration).

SNMP

Enable and configure SNMP

SNMP

Enable SNMP on the selected VRF

☐ Default VRF☐ Management VRF

Mode

v3

Users (1)

Name	Authentication Mode	Privacy Mode
snmp-V3-user	md5	des

Trap Destination

IP Address	VRF
------------	-----

Answer:

Access Points

Switches

MultiEdit

Access to AOS-CX search and custom configuration (editor & express configuration).

SNMP

Enable and configure SNMP

SNMP

Enable SNMP on the selected VRF

Default VRF

Management VRF

Mode

v3

Users (1)

Name	Authentication Mode	Privacy Mode
snmp-V3-user	md5	des

Trap Destination

IP Address	VRF
------------	-----

最新問題: 110

Aruba CX6200MのグローバルステータスインジケータLEDがオレンジ色に点滅している場合、それは何を示していますか？

A. スイッチに回復可能な故障が発生しました。

B. 自己テストが進行中です。

C. ファームウェアイメージが破損しています。

D. スイッチがファームウェアイメージを起動しています。

Answer: (解答を表示する)

Aruba CX6200MスイッチのグローバルステータスインジケータLEDがオレンジ色に点滅している場合、通常はスイッチに障害が発生したことを示していますが、復旧可能です。このLEDの動作は、ネットワーク管理者に問題に対処する必要があることを知らせるアラートとして機能しますが、必ずしもスイッチが動作不能であることを意味するものではありません。

最新問題: 111

EDGE1とCORE1スイッチでいくつかのshowコマンドを実行して、問題のトラブルシューティングに必要な情報を収集します。showコマンドの出力画像を使用して、EDGE1アップリンクがダウンしている理由を特定します。

EDGE1# TROUBLESHOOTING - SHOW COMMANDS OUTPUT

```
EDGE1# show span vlan 20
Port      Role      State
TCN-Tx    TCN-Rx
-----
lag1      Disabled  Blocking
 2         2
EDGE1# show run int 1/1/51
interface 1/1/51
 no shutdown
 description Uplink_To_Core1
 lag 1
 exit
EDGE1# show run int 1/1/52
interface 1/1/52
 no shutdown
 description Uplink_To_Core1
 lag 1
 exit
EDGE1# show run int lag1
interface lag 1
 no shutdown
 no routing
 vlan trunk native 20
 vlan trunk allowed all
 lacp mode active
 exit
```

```
EDGE1# show lacp int
Actor details of all interfaces:
```

Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key	Forwarding State
1/1/51	lag1	52	1	ALFOE	b8:d4:e7:b5:22:80	65534	1	lacp-block
1/1/52	lag1	53	1	ALFOE	b8:d4:e7:b5:22:80	65534	1	lacp-block

CORE1# TROUBLESHOOTING - SHOW COMMANDS OUTPUT

```
CORE1# show span vlan 20
Port      Role      State
Rx        TCN-Tx    TCN-Rx
-----
lag1      Designated  Forwarding
 2         2
CORE1# show run int 1/1/51
interface 1/1/51
 no shutdown
 lag 1
 exit
```

```
CORE1# show run int 1/1/52
interface 1/1/52
 no shutdown
 lag 1
 exit
```

```
CORE1# show run int lag 1
interface lag 1
 no shutdown
 no routing
 vlan trunk native 20
 vlan trunk allowed all
 exit
```

```
CORE1# show lacp int
```

```
Actor details of all interfaces:
```

```
CORE1# show lacp int
```

```
Actor details of all interfaces:
```

Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key	Forwarding State
1/1/51	lag1							up
1/1/52	lag1							up

- A. 物理インターフェースが正しいLAGのメンバーではありません。
- B. スパニングツリーのブロック状態により、コアアップリンクがエッジとの接続を確立できません。
- C. コアが誤った物理的インターレースに接続されています
- D. コアアップリンクでLACPが設定されていません

Answer: D (メッセージを残す)

LACPは、複数の物理リンクを単一の論理リンクに集約して帯域幅と冗長性を向上させるプロトコルです。LACPを正しく動作させるには、リンクの両端でLACPを設定する必要があります。この例では、EDGE1のアップリンクポートチャンネル1にLACPが設定されていますが、CORE1の対応するポートチャンネル1にはLACPが設定されていません。このため設定が一致せず、リンクが確立されません。参考資料：

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/lacp.htm

最新問題: 112

HPE Aruba Networking APの無線ステータスLEDがオレンジ色に点灯している場合、何を示していますか？

- A. スイッチから供給されるPoE電力が不足しているため、APの2つの無線機器両方に電力を供給できません。
- B. 無線機はメッシュモードで動作しています

C. この無線機は5GHz帯のみで動作します。

D. 無線機はモニターモードまたはスペクトル分析モードで有効になっています。

Answer: D ([メッセージを残す](#))

Aruba AP アクセスポイント (AP) のオレンジ色に点灯する無線ステータス LED アクセスポイント (AP) は、Wi-Fi またはその他の無線規格を使用して無線デバイスを有線ネットワークに接続するデバイスです。

AP は無線信号の送信機および受信機として機能し、特定のエリアに無線カバレッジを提供します。AP は、ルート、リピーター、ブリッジ、メッシュなどのさまざまなモードで動作できます。AP は、セキュリティ、QoS、ローミング、負荷分散などのさまざまな機能もサポートできます。AP はスタンドアロン デバイスとして動作することも、コントローラまたはクラウド サービスによって管理することもできます。AP は、show ap active、show ap database、show ap bss-table などのコマンドを使用して検証できます。は、無線がモニタ モードまたはスペクトル分析モードで有効になっていることを示します。モニタ モードは、AP がすべてのチャンネルをスキャンして、無線トラフィック、干渉、不正デバイスなどの情報を収集できるモードです。スペクトル分析モードは、AP がすべてのチャンネルをスキャンして、RF 無線周波数 (RF) に関する情報を収集できるモードです。無線周波数 (RF) は、3 kHz から 300 GHz までの周波数を持つ電磁波を指す用語です。RF 波は、通信、放送、レーダー、ナビゲーション、リモート コントロールなど、さまざまな目的で使用されます。

RF波は、振幅、周波数、または位相を変化させることで変調され、情報を符号化できます。RF波は、減衰、反射、屈折、回折、散乱、干渉、ノイズなど、さまざまな要因の影響を受けることもあります。RF波は、スペクトラムアナライザ、パワーメータ、アンテナなどのデバイスを使用して測定できます。環境、ノイズ源、チャンネル利用率など。どちらのモードも、ワイヤレスパフォーマンスのトラブルシューティングと最適化に役立ちますが、無線機での通常のデータ送受信は無効になります。Aruba APの無線ステータスLEDがオレンジ色に点灯しないのは、次の理由によるものです。

- スイッチから AP の両方の無線に電力を供給するのに十分な PoE が供給されていません: このオプションは、Aruba AP の点滅するオレンジ色の電源ステータス LED によって示されるため、false です。点灯しているオレンジ色の無線ステータス LED によって示されるのではなく、Aruba AP の点滅するオレンジ色の電源ステータス LED によって示されるのです。オレンジ色の電源ステータスLEDが点滅している場合は、APがスイッチまたはインジェクターから十分な電力を供給されておらず、正常に動作できないことを意味します。緑色の電源ステータスLEDが点灯している場合は、APがスイッチまたはインジェクターから十分な電力を供給されており、正常に動作できることを意味します。

- 無線がメッシュモードで動作しています: このオプションは偽です。Aruba AP では、無線がメッシュモードで動作している場合は、無線ステータス LED が緑色に点灯し、オレンジ色の点灯では示されません。無線ステータス LED が緑色に点灯している場合は、無線が通常モードまたはメッシュモードで動作しており、割り当てられたチャンネルでデータの送受信ができることを意味します。メッシュモードは、有線接続を必要とせずに、AP が他の AP とワイヤレスで接続してメッシュネットワークを形成できるモードです。

- 無線機は 5 GHz 帯域のみで動作します: このオプションは、無線機が 5 GHz 帯域で動作しているため、偽です。

Aruba APでは、5GHz帯のみが有効になっている場合は、無線ステータスLEDが青色に点灯し、橙色に点灯することはありません。青色に点灯している無線ステータスLEDは、無線がデュアルバンドモードで動作しており、2.4GHz帯と5GHz帯の両方でデータの送受信が可能であることを意味します。

最新問題: 113

IPカメラ、アクセスポイント、その他のPoEデバイスを導入する際に、スイッチポートのPoE優先度を動的に設定するにはどうすればよいのでしょうか？

A. スイッチモジュールでクイックPoEを有効にする

B. デバイスプロビジョニングのプロファイリングを有効にする

C. PoE電源管理をクラスベースモードに設定する

D. PoE電源管理をダイナミックモードに設定する

Answer: ([解答を表示する](#)**)**

プロファイリングとは、ArubaスイッチがMACアドレス、DHCPオプション、LLDP情報などの様々な属性に基づいて、接続されているデバイスを自動的に識別・分類できる機能です。プロファイリングを使用すると、デバイスの種類や電力要件に基づいて、スイッチポートのPoE優先度を動的に設定できます。

例えば、IPカメラはプリンターやPCよりもPoEの優先度が高い場合があります。プロファイリングは、デバイスプロファイルに基づいてVLAN、ACL、QoSなどの他の構成設定を適用するためにも使用できます。参考文献：

https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/profiling.htm

最新問題: 114

単一のAruba CX 6300Mスイッチ構成では、L3接続を使用してスイッチの仮想インターフェイス120と130間のルーティングトラフィックを確立するにはどうすればよいのでしょうか？

A. Aruba 6300Mではルーティングはデフォルトで有効になっています。

B. ルートリーキングはデフォルトVRFで設定する必要があります。

- C. SVIインターフェースから `no routing` を削除します。
- D. SVI 120と130の間に静的ルートを作成します。

Answer: A ([メッセージを残す](#))

Aruba CX 6300Mスイッチでは、スイッチ仮想インターフェース (SVI) 間のルーティングはデフォルトで有効になっています。

したがって、SVI 120 と 130 のような SVI 間のトラフィックは、SVI 上に `ルーティングなし` の設定がない限り、ルートルーティングやスタティックルートなどの追加設定を必要とせずに内部的にルーティングできます。

最新問題: 115

ネットワーク技術者が、Aruba Central から設定を受信しない支店の新しい AP のトラブルシューティングを行っています。支店の他の AP は期待どおりに動作しています。 `show ap debug cloud-server command` の出力では、 `cloud config received` が FALSE であることが示されています。

新しいアクセスポイントがインターネットに接続できることを確認した後、次に何を確認しますか？

- A. 無効化と有効化をアクティブ化してプロビジョニングの更新をトリガーします
- B. `arubanetworks.com` で AP がデバイスに ping できることを確認します。
- C. API にライセンスが割り当てられていることを確認します
- D. Aruba Central を無効化してから有効化することで、設定の更新をトリガーします。

Answer: C ([メッセージを残す](#))

説明

AP がインターネットに接続されているにもかかわらず、Aruba Central から設定情報を受信できない場合、考えられる原因の一つは、API に Aruba Central でライセンスが割り当てられていないことです。Aruba Central で管理される API には、それぞれライセンスが必要です。

参考資料 https://www.arubanetworks.com/techdocs/Central/2.5.2-GA/HTML_frameset.htm#GUID-8F0E7E8B

最新問題: 116

SVL を使用したインバンド管理を使用している場合、Aruba CX スwitch でデフォルトルートを 10.4.5.1 に設定するには、どのコマンドを使用しますか？

- A. IP デフォルトゲートウェイ 10.4.5.1
- B. `ip route 0.0.0.0/0 10.4 5.1 vrf mgmt`
- C. `ip route 0.0.0.0/0 10.4.5.1`
- D. デフォルトゲートウェイ 10.4.5.1

Answer: C ([メッセージを残す](#))

SVI を使用したインバンド管理を使用している場合に、Aruba CX スwitch で 10.4.5.1 へのデフォルト ルートを設定するために使用されるコマンドは、`ip route 0.0.0.0/0 10.4.5.1` です。このコマンドは、スイッチに直接接続されていないネットワークに到達するための宛先ネットワーク アドレス (0.0.0.0) とプレフィックス長 (/0)、およびネクスト ホップ アドレス (10.4.5.1) を指定します。デフォルト ルートは、SVI スwitch 仮想インターフェイスを通過するインバンド管理トラフィックに使用されるデフォルトの VRF 仮想ルーティングおよび転送に適用されます。VRF は、同じルーター内でルーティング テーブルの複数のインスタンスを同時に共存できるようにするテクノロジーです。VRF は通常、セキュリティ、プライバシー、または管理目的でネットワーク トラフィックをセグメント化するために使用されます。SVI は、スイッチ上の仮想インターフェイスで、同じスイッチまたはトランク リンクで接続された異なるスイッチ上の異なる VLAN 間でパケットをルーティングできるようにします。SVI は VLAN に関連付けられており、IP アドレスとサブネットマスクが割り当てられています。

最新問題: 117

UX の利点を 2 つ挙げてください。(2 つ選択してください。)

- A. AUX1 はインターネット接続なしで使用できます
- B. UX1 は遠隔地で最適な WiFi チャンネルを計算するのに役立ちます
- C. UX デザイナーはクライアント/ユーザーのように振る舞う
- D. UX1 は、指定された場所にあるすべての AP の Wi-Fi カバレッジを測定します。

E. UXI は、HTTP VOIP や Office 365 などのさまざまなアプリケーションをチェックできます。

Answer: C,E (メッセージを残す)

UXI (User Experience Insight)は、ユーザーの行動をシミュレートし、ユーザー視点からネットワークパフォーマンスをテストするデバイスです。HTTP、VOIP、Office 365などのさまざまなアプリケーションをチェックし、レイテンシ、ジッター、パケット損失、スループットなどの指標を測定できます。参考資料 <https://www.arubanetworks.com/products/networking/user-experience-insight/>

Arubaネットワークなどで使用されているようなユーザーエクスペリエンスインサイト (UXI) センサーは、クライアントの動作を模倣し、ユーザー視点から様々なネットワークサービスやアプリケーションのパフォーマンスをテストするように設計されています。HTTP、VOIP、Office 365などのクラウドサービスを含む様々なアプリケーションのユーザーアクティビティをシミュレートし、ユーザーエクスペリエンスの質を測定することで、ネットワークパフォーマンスとユーザーエクスペリエンスに関する貴重な洞察を提供します。

最新問題: 118

別添資料を参照してください。

Access PointsSwitches

MultiEdit ☐

Access to AOS-CX search and custom configuration (editor & express configuration).

Logging

LevelEmergency

Logging Servers (4)

FQDN or IP address	Event Log Level	VRF
10.99.26.25	Emergency	Management
10.100.100.25	Information	Management
172.17.17.43	Warning	Default
192.168.0.56	Debug	Default

どのサーバーが最も少ない量のデータを受信するでしょうか？

A. 172.17.17.43

- B. 10.100.100.25
- C. 10.99.26.25
- D. 192.168.0.56

Answer: (解答を表示する)

ログサーバーの設定を示す図に基づくと、サーバー172.17.17.43はイベントログレベルが 警告」に設定されているため、受信するデータ量が最も少なくなります。これは、警告以上の深刻度に分類されるイベントのみがログに記録されることを意味し、通常、情報」、デバッグ」、緊急」などの深刻度の低いレベルよりも発生頻度は低くなります。

最新問題: 119

show lacp interfaces」コマンドでLACPの状態を確認した際に、ALFOE」というステータスが表示されるのはどういう意味ですか？

- A. ローカルスイッチのインターフェースはスタティックLAGとして設定されています。
- B. LACPがピア側で設定されていません
- C. LACPは同期処理中です
- D. LACPは問題なく正常に動作しています

Answer: D (メッセージを残す)

説明

ALFOE」の状態は、LACP（リンクアグリゲーション制御プロトコル）が2つのデバイス間でリンクアグリゲーションの動的なネゴシエーションを提供するネットワークプロトコルであることを意味します。LACPIは、複数の物理リンクを1つの論理リンクに結合することで、帯域幅、冗長性、および負荷分散を向上させます。LACPIはIEEE 802.3ad規格で定義されています。show lacp interfaces」でLACPを確認すると、問題なく正常に動作しています。ALFOE」の状態は、次の略語です。

A: アクティブ - インターフェースは、ピアデバイスとのリンクアグリゲーションをネゴシエートするために、LACPパケットをアクティブに送信しています。

L: リンクアップ - インターフェースがピアデバイスと物理的に接続されています。

F: 集約可能 - このインターフェースは、他のインターフェースと集約して単一の論理リンクにすることができます。

D: 同期済み - インターフェイスはピア デバイスとの間でリンク アグリゲーション パラメータのネゴシエーションを正常に完了し、論理リンク上でトラフィックを送受信できます。

E: 収集/配信 - インターフェースは、ピアデバイスからの受信トラフィックを収集し、論理リンク上のピアデバイスへの送信トラフィックを配信します。

他の選択肢が正しくない理由は以下のとおりです。

ローカルスイッチのインターフェースは static-LAG として構成されています。static-LAG は LACP を使用してリンクアグリゲーションをネゴシエートしないため、このオプションは false になります。static-LAG では、両方のデバイスでリンクアグリゲーションパラメータを手動で構成する必要があり、ステータスインジケータもありません。

LACPがピア側で設定されていません :このオプションはfalseです。ピア側でLACPが設定されていない場合、インターフェースの状態は ALFOE」ではなく ALF-」になります。これは、インターフェースがピアデバイスと同期またはデータの収集/配信を行わないことを意味します。

LACPが同期処理中です :このオプションはfalseです。LACPが同期処理中の場合、インターフェースの状態は ALFOE」ではなく ALF-O」になります。つまり、インターフェースはピアデバイスとの間でデータの収集/配信を行っていません。

参考文献 :

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/lag/lag-overview.htm

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/lag/lag-lACP.htm

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/lag/lag-lACP-status.htm

最新問題: 120

Arubaのモビリティマスターアーキテクチャを使用する場合、ネットワーク管理者はどの機能を使ってRFプランニングと最適化サービスを一元化できますか？

- A. エアウェーブ
- B. クライアントマッチ

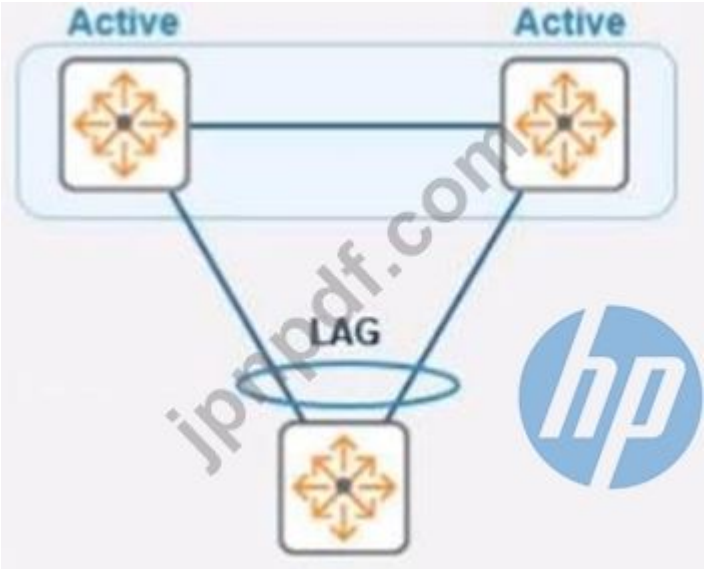
- C. エアマッチ
- D. クライアントウェーブ

Answer: C (メッセージを残す)

AirMatch は、Aruba ワイヤレス ネットワークの集中型 RF プランニングおよび最適化サービスを提供する機能です。クラウド ベースのアルゴリズムと機械学習を使用して、RF パフォーマンスとユーザー エクスペリエンスを最適化します。参照:https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdf Aruba ネットワークでは、推奨される仮想スイッチング フレームワーク (VSF) トポロジには、デジジー チェーンとマルチ アクティブ検出 (MAD) およびリング トポロジが含まれます。MAD を使用したデジジー チェーン トポロジは、複数のスイッチを直列に接続するシンプルで効果的な方法を提供し、VSF 内の複数のスイッチが同時にアクティブになる可能性がある状況を検出して処理するためのメカニズム (MAD) が確実に存在するようにします。リング トポロジは、VSF メンバー間でループ接続パターンを作成することで冗長性を提供し、ネットワークの回復力と信頼性を向上させます。

最新問題: 121

展示資料を参照してください。



指定されたトポロジーでは、2台のAruba CX 8325スイッチがアクティブゲートウェイを使用するVSXスタックを構成しています。クライアントがVSXをデフォルトゲートウェイとして使用してアクセススイッチに接続されている場合、VSXペアの仮想IPの性質と動作はどうなりますか？

- A. プライマリVSXスイッチで仮想IPが有効になっています
- B. 仮想フローティングIPは、障害発生時にフェイルオーバーします。
- C. 仮想IPは両方のCXスイッチで有効です
- D. 仮想IPはVSXと同期したSVI IPアドレスを使用します

Answer: B (メッセージを残す)

仮想スイッチング拡張 (VSX) スタックにおいて、仮想IP (VIP) は、アクセススイッチに接続されたクライアントに単一のデフォルトゲートウェイIPアドレスを提供します。このVIPは、プライマリVSXスイッチ上でアクティブとなるフローティングIPです。プライマリスイッチに障害が発生した場合、VIPはセカンダリスイッチにフェイルオーバーし、クライアントトラフィックのルーティングが中断なく継続されるようにします。

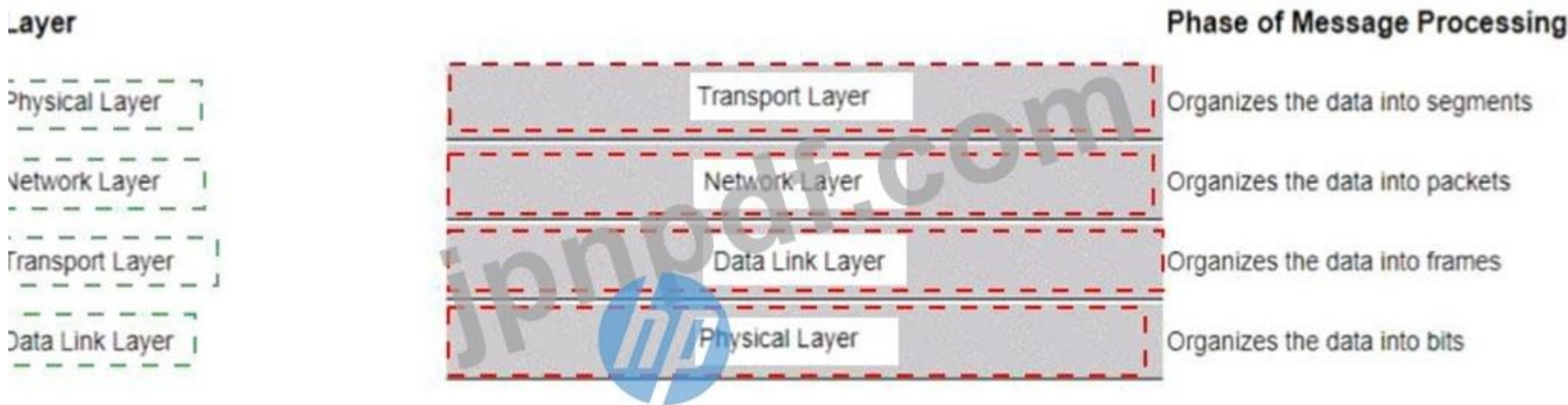
有効な **HPE6-A85** 問題集は GoShiken.com が提供された合格しやすい HPE6-A85 試験問題集！ GoShiken.com が最新の **HPE6-A85** 試験問題集を提供しています。GoShiken.com HPE6-A85 試験問題は最新で、解答が正確でございます。最新の GoShiken.com HPE6-A85 問題集をゲットする人はこちら: <https://www.goshiken.com/HP/HPE6-A85-mondaishu.html> (134**30%OFF**問題集溶と正解付きで **30%**w特別割引コード: **Freepdfdumps**)

最新問題: 122

メッセージ処理のフェーズを、オープンシステム相互接続 (OSI) レイヤーに対応させてください。



Answer:



Explanation:

層: 1) 物理層 メッセージ処理のフェーズ: d) データをビットに編成する 層: 2) データリンク層 メッセージ処理のフェーズ: c) データをフレームに編成する 層: 3) ネットワーク層 メッセージ処理のフェーズ: b) データをパケットに編成する 層: 4) トランスポート層 メッセージ処理のフェーズ: a) データをセグメントに編成する OSI モデルは、ネットワーク処理を 7 つの層に分割し、各層は伝送チェーンの異なるステップを表します。各層には独自の機能があり、明確に定義されたタスクを担当します。ユーザーデータは、デバイスが外部に送信するまで、最上位層から下位層へと順次渡されます。最下位層である物理層は、データを物理媒体で送信できるビットに変換します。第 2 層であるデータリンク層は、ビットを 2 つのノード間のリンクで送信できるフレームに編成します。第 3 層であるネットワーク層は、フレームをノードのネットワーク全体にルーティングできるパケットに編成します。第 4 層であるトランスポート層は、パケットを 2 つのエンドポイント間で信頼性の高いエラーのない通信を提供できるセグメントに編成します 12。参考文献: 1 <https://www.linode.com/docs/guides/introduction-to-osi-networking-model/> 2 https://en.wikipedia.org/wiki/OSI_model

最新問題: 123

アクセスポイントからの信号が物体を通過する際に吸収されて弱まると、何が起こるのでしょうか？

- A. APIはボンディングチャネルを使用してクライアントへの遅延を低減します。
- B. 信号対雑音比 \$NR\$)が増加する
- C. 信号対雑音比 \$NR\$)が低下する
- D. Aruba Centralは、クライアントを動的に近隣のアクセスポイントに移動します。

Answer: C ([メッセージを残す](#))

信号対雑音比 \$NR\$)は、目的信号のレベルと背景雑音のレベルを比較する指標です。SNRは信号電力と雑音電力の比として定義され、多くの場合デシベル \$B\$)で表されます。SNRが高いほど信号は明瞭で検出や解釈が容易ですが、SNRが低いほど信号は雑音によって劣化または不明瞭になり、識別や復元が困難になる可能性があります1。

AP アクセスポイントからの信号が壁や家具などの物体を通過する際に吸収されて弱まると、信号電力が低下します。これにより SNR が低下し、無線接続の品質に影響します。また、他の AP や同じ周波数帯で動作するデバイスなどの他のソースからの干渉により、ノイズ電力が増加することもあります。したがって、AP からの信号が物体を通過する際に吸収されて弱まると SNR が低下するというのが正解です。

参考文献：

1 https://en.wikipedia.org/wiki/Signal-to-noise_ratio

2 https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_%28SNR%2

最新問題: 124

顧客が、会社全体のグループベースポリシー（GPO）を介してユーザー証明書とデバイス証明書を実装しました。ネットワーク認証時にクライアント証明書を必要とするEAP方式はどれですか？

A. EAP-TTLS

B. EAP-TLS

C. EAP-TEAP

D. PEAP

Answer: B ([メッセージを残す](#))

EAP-TLSは、ネットワークへの認証時にクライアント証明書を必要とする認証方式です。公開鍵暗号とデジタル証明書を使用して、クライアントとサーバー間の相互認証を提供します。参考資料：

<https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content>

/CPPM_UserGuide/EAP-TLS/EAP-TLS.htm

EAP-TLS（拡張認証プロトコル - トランスポート層セキュリティ）は、認証にサーバー側とクライアント側の両方の証明書を必要とするEAP方式です。ユーザーと認証サーバーが証明書を使用して互いの身元を証明する相互認証プロセスを採用しているため、最も安全なEAP方式の一つと考えられています。グループベースポリシー（GPO）を使用してユーザー証明書とデバイス証明書を実装することは、クライアント側証明書に関するEAP-TLSの要件によく適合します。

最新問題: 125

WPAキー階層のどの部分がデータの暗号化および/または復号化に使用されますか？

A. ペアワイズ時間キー（PTK）

B. ペアワイズマスターキー（PMK）

C. キー確認キー（KCK）

D. 一度だけ使用される番号（nonce）

Answer: A ([メッセージを残す](#))

データの暗号化および/または復号化に使用される WPA キー階層の部分は、ペアワイズ一時キー（PTK）です。PTK は PMK から派生したキーです。ペアワイズマスターキー（PMK）は PSK から派生したキーです。事前共有キー（PSK）は、通信開始前に 2 当事者間で共有されるキーです。ANonce 認証者ノンス（ANonce）は、認証者（AP など、ネットワーク リソースへのアクセスを制御するデバイス）によって生成される乱数です。SNonce サプリカントノンス（SNonce）は、サプリカント（STA など、ネットワーク リソースにアクセスしたいデバイス）によって生成される乱数です。AA 認証者アドレス（AA）は認証者の MAC アドレスです。SA サプリカントアドレス（SA）は、擬似乱数関数（PRF）を使用したサプリカントの MAC アドレスです。

PTKは4つのサブキーで構成されています。

- KCK（キー確認キー）はメッセージの完全性チェックに使用されます

- KEK（キー暗号化キー）は暗号化キーの配布に使用されます。

- TKテンポラルキー（TK）はデータ暗号化に使用されます

- MICメッセージ整合性コード（MIC）キー

データ暗号化に特に使用されるサブキーは、TKテンポラルキー（TK）です。TKはペアワイズトランジェントキー（PTK）とも呼ばれます。TKは、通信中に時間または送信されるパケット数に基づいて定期的に変化します。

その他のオプションは、以下の理由によりWPAキー階層の一部ではありません。

- PMK: PMKはWPAキー階層の一部ではなく、PTKを生成するための入力です。

- KCK: KCKはWPAキー階層の一部ですが、データの暗号化には使用されず、メッセージの完全性チェックに使用されます。

- ノンス: ノンスはWPAキー階層の一部ではなく、PTKを生成するための入力です。

最新問題: 126

Arubaのどのテクノロジーが、無線帯域とAP無線機器間で負荷分散機能を提供しますか？

- A. アルバESP
- B. Aruba ClientMatch
- C. Aruba AirWave
- D. アルバ中央

Answer: B ([メッセージを残す](#))

Aruba ClientMatchは、クライアントの動作を継続的に監視し、Wi-Fiパフォーマンスを最適化するためにクライアント接続を自動的に調整するテクノロジーです。これには、クライアントを最も混雑の少ないアクセスポイントとWLAN上で最適な無線に誘導することが含まれており、異なる無線帯域とアクセスポイントの無線間で効果的な負荷分散を実現します。

最新問題: 127

チャンネル幅が同じ5GHz帯と6GHz帯のチャンネルを比較する場合、正しい記述はどれですか？

- A. 5GHzチャンネルは、6GHzチャンネルと比較して、伝送距離は同じですが、クライアントに提供するスループットが異なります。
- B. 5GHzチャンネルは、他のチャンネルと比較して伝送距離が異なり、クライアントに異なるスループットを提供します。
- 6GHzチャンネル
- C. 5GHzチャンネルは、6GHzチャンネルと比較して、伝送距離が同じで、クライアントに同じスループットを提供します。
- D. 5GHzチャンネルは6GHzチャンネルと比較して伝送距離が異なりますが、クライアントに提供するスループットは同じです。

Answer: ([解答を表示する](#))

チャンネル幅が同じ 5 GHz チャンネルと 6 GHz チャンネルを比較する場合、正しい記述は、5 GHz チャンネルは 6 GHz チャンネルと比較して伝送距離が異なり、クライアントに提供するスループットも異なるということです。この記述は、高周波信号は減衰が大きい傾向があるという事実を反映しています。減衰とは、伝送距離や物体または媒体を通過する際に信号強度が低下することを指す一般的な用語です。減衰が大きいということは、高周波信号は低周波信号よりも伝送距離が短く、スループットが低いことを意味します。

この声明に関する事実をいくつか挙げると以下のとおりです。

5GHz帯のチャンネルは6GHz帯のチャンネルよりも周波数が低いため、6GHz帯のチャンネルよりも減衰が少ない。

減衰率が低いということは、5GHz帯のチャンネルは、同じチャンネル幅の6GHz帯のチャンネルよりも、より長い距離を伝送でき、クライアントに対してより高いスループットを提供できることを意味します。

しかし、屋内環境では信号伝搬に影響を与える障害物や反射が多いため、5GHz帯と6GHz帯のチャンネル間の距離とスループットの差はそれほど大きくない可能性があります。

6GHz帯のチャンネルを5GHz帯のチャンネルよりも使用する利点は、5GHz帯のチャンネルよりも利用可能なスペクトルが多く、干渉が少なく、重複しないチャンネルが多いことです。

他の選択肢が正しくない理由は以下のとおりです。

- 5 GHz チャンネルは 6 GHz チャンネルと同じ距離を伝送し、クライアントに異なるスループットを提供します: このオプションは誤りです。高周波信号は減衰が大きいため、5 GHz チャンネルは 6 GHz チャンネルと同じ距離を伝送しません。
- 5 GHz チャンネルは 6 GHz チャンネルと比較して、同じ距離を伝送し、同じスループットをクライアントに提供します: このオプションは誤りです。高周波信号の減衰が大きいため、5 GHz チャンネルは 6 GHz チャンネルと同じ距離を伝送したり、同じスループットを提供したりしません。
- 5 GHz チャンネルは 6 GHz チャンネルと比較して伝送距離が異なり、クライアントに同じスループットを提供します: このオプションは誤りです。高周波信号の減衰が大きいため、5 GHz チャンネルは 6 GHz チャンネルと同じスループットを提供しません。

最新問題: 128

あなたは顧客との会議で、ネットワーク冗長化機能であるマルチプルスパニングツリー (MSTP)について説明するよう求められました。この機能について正しい説明はどれですか？

- A. デフォルトでは、MSTP 構成 ID の改訂は現在の MSTP ルート優先度として使用されます。
- B. スイッチIMCアドレスを使用したデフォルトのMSTP設定ID名
- C. デフォルトではスイッチのシリアル番号を使用したMSTP設定ID名
- D. MSTP設定IDのリビジョンはデフォルトでスイッチのシリアル番号になります

Answer: [\(解答を表示する\)](#)

MSTP は、複数の VLAN を持つネットワークでのループを防止するための IEEE 標準プロトコルです。MSTP では、複数の VLAN を、より少ない数のスパニングツリーインスタンスにマッピングできます。構成 ID は、名前とリビジョンの 2 つのパラメータで構成されます。名前は、同じ構成 ID と VLAN とインスタンスのマッピングを共有するスイッチのグループである MSTP 領域を識別する 32 バイトの ASCII 文字列です。リビジョンは、構成 ID のバージョンを示す 16 ビットの数値。デフォルトでは、MSTP 構成 ID 名はスイッチ IMC アドレスに設定されます。これは、スイッチの MAC アドレス (メディア アクセス コントロール アドレス) から派生した一意の識別子です。MAC アドレスは、スイッチのネットワーク セグメント内の通信でネットワーク アドレスとして使用するために、ネットワーク インターフェイス コントローラ (NIC) に割り当てられる一意の識別子です。

最新問題: 129

各AAAサービスを正しい定義と一致させてください（一致した項目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）。

Definition

A list of rules that specifies which entities are permitted or denied access

Control users access on the network

Tracking user activity on the network

Who can access the network based on credentials/certificates



AAA Service

Accounting

Authentication

Authorization

Answer:

Definition

A list of rules that specifies which entities are permitted or denied access

Control users access on the network

Tracking user activity on the network

Who can access the network based on credentials/certificates

Tracking user activity on the network

Who can access the network based on credentials/certificates

Control users access on the network

AAA Service

Accounting

Authentication

Authorization

最新問題: 130

2.4GHz帯の無線LAN環境において、同一チャネル干渉を回避しながら同時に使用できる3つのチャネルはどれですか？

- A. 1,6, 11
- B. 1、5、10
- C. 3,6, 9
- D. 2,7, 11

Answer: A ([メッセージを残す](#))

2.4GHz帯の無線LAN環境では、チャンネル1、6、11を同時に使用することが推奨されます。これらのチャンネルは互いに重なり合わないため、同一チャンネル干渉を回避できます。各チャンネルは十分な周波数間隔で分離されているため、信号が干渉することはありません。これは、他のチャンネルの組み合わせでは実現できないことです。

最新問題: 131

あなたは顧客との会議で、ネットワーク冗長化機能であるVRRPについて説明するよう求められました。この機能について正しく説明できるのはどれですか？

- A. HPE Aruba Networking独自のIPゲートウェイ冗長性を提供します
- B. 標準規格に基づいたIPゲートウェイ冗長性を提供します
- C. AOS-CXスイッチでは、デフォルトのVRFを有効にする必要があります。
- D. ゲートウェイの完全な冗長性を実現するには、3つのメンバーが動作する必要があります。

Answer: ([解答を表示する](#))

VRRPは、複数のルーターが仮想IPアドレスを共有し、そのうちの1つがアクティブゲートウェイとして機能することで、IPゲートウェイの冗長性を提供する、オープンな標準ベースのプロトコルです。

最新問題: 132

AOS-CXスイッチへの入力時に、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。このタスクに最適なテクノロジーは何ですか？

- A. 律速段階
- B. DWRRキューイング
- C. QoSシェーピング
- D. 厳密なキューイング

Answer: A ([メッセージを残す](#))

ArubaOS-CX スwitchへの入力時に過剰なブロードキャスト トラフィックをドロップするための最適なテクノロジーは、レート制限です。レート制限とは、ネットワーク管理者が帯域幅のしきい値または制限を設定することで、スイッチのポートまたは VLAN に入入りするトラフィック量を制御できる機能です。レート制限は、ネットワークの輻輳を防止し、ネットワーク パフォーマンスを向上させ、サービス レベル契約 (SLA) を遵守させ、サービス拒否 (DoS) 攻撃を軽減するために使用できます。レート制限は、インターフェイス設定モードで storm-control コマンドを使用することで、ArubaOS-CX スwitchへの入力時にブロードキャスト トラフィックに適用できます。このコマンドを使用すると、ネットワーク管理者は、入力ポートでブロードキャスト トラフィックが使用できる帯域幅の割合または 1 秒あたりのパケット数を指定できます。ブロードキャスト トラフィックが指定されたしきい値を超えると、スイッチは超過分のパケットをドロップします。その他のオプションは、入力時に過剰なブロードキャスト トラフィックをドロップするためのテクノロジーではありません。理由は以下のとおりです。

- DWRRキューイング :DWRRはDeficit Weighted Round Robinの略で、出力ポート上の異なるトラフィッククラスまたはキューに異なる重みまたは優先度を割り当てるキューイングアルゴリズムです。

DWRRは、各キューがその重みに基づいて適切な帯域幅を確保しつつ、優先度の低いキューが帯域幅不足に陥ることを防ぎます。DWRRは、入力時に過剰なブロードキャストトラフィックを破棄するのではなく、出力時に送信トラフィックをスケジュールします。

- QoSシェーピング :QoSはQuality of Serviceの略で、ネットワークリソースを管理し、トラフィックの種類に応じて異なるレベルのサービスを提供する一連の技術です。QoSシェーピングは、利用可能な帯域幅またはレート制限に合わせて、出力ポートで送信トラフィックを遅延またはバッファリングする技術です。QoSシェーピングは、入力時に過剰なブロードキャストトラフィックを破棄するのではなく、出力時に送信トラフィックを平滑化します。

- 厳密キューイング：厳密キューイングは、出力ポート上の異なるトラフィッククラスまたはキューに異なる優先順位を割り当てる別のキューイングアルゴリズムです。厳密キューイングでは、帯域幅要件や重みに関係なく、優先順位の高いキューが常に優先順位の低いキューよりも先に処理されることが保証されます。厳密キューイングは、入力時に過剰なブロードキャストトラフィックを破棄するのではなく、出力時に送信トラフィックをスケジュールします。

最新問題: 133

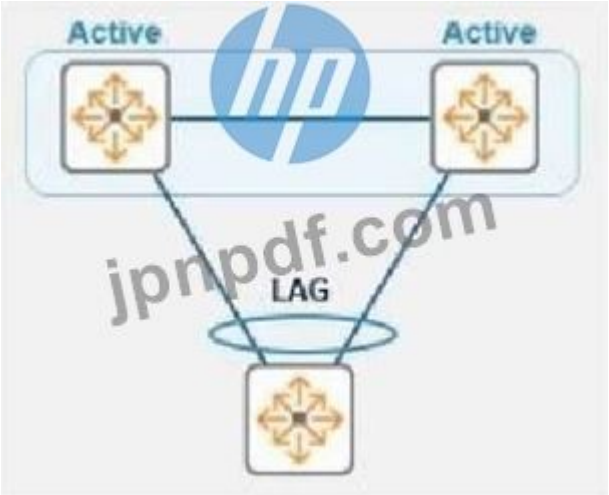
どのプロトコルデータユニット (PDU)がネットワーク層のPDUを表していますか？

- A. PDU3 - パケット
- B. PDU4セグメント
- C. PDU1 - 信号
- D. PDU2 - フレーム

Answer: ([解答を表示する](#))

OSIモデルにおいて、ネットワーク層は中間ルータを経由するルーティングを含むパケット転送を担当します。したがって、ネットワーク層のPDUはパケットと呼ばれます。

最新問題: 134
図を参照してください。このトポロジでは、2台のAruba CX 8325スイッチがアクティブゲートウェイを使用するVSXスタックを構成しています。クライアントがVSXをデフォルトゲートウェイとして使用してアクセススイッチに接続されている場合、VSXペアの仮想IPアドレスの性質と動作はどうなりますか？



- A. プライマリVSXスイッチで仮想IPが有効になっています
- B. 仮想フローティングIPは、障害発生時にフェイルオーバーします。
- C. 仮想IPは両方のCXスイッチで有効です
- D. 仮想IPはVSXと同期したSVI IPアドレスを使用します

Answer: C ([メッセージを残す](#))

VSXアクティブゲートウェイを使用すると、仮想ゲートウェイIPが両方のVSXスイッチでアクティブになり、両方のピアが共有デフォルトゲートウェイを使用するクライアントのトラフィックを転送できるようになります。

Valid HPE6-A85 Dumps shared by GoShiken.com for Helping Passing HPE6-A85 Exam! GoShiken.com now offer the **newest HPE6-A85 exam dumps**, the GoShiken.com HPE6-A85 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com HPE6-A85 dumps with Test Engine here: <https://www.goshiken.com/HP/HPE6-A85-mondaishu.html> (134 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)