HP.HPE6-A85.v2023-10-10.q21

試験コード:	HPE6-A85
試験名称:	Aruba Campus Access Associate Exam
認定資格:	HP
無料問題数:	21
バージョン:	v2023-10-10
アクセス数:	355
ページビュー数:	210
https://www.jpnpdf.com/HP.HPE6-A85.v2023-10-10.q21-mondaishu.html	

最新問題: **1**
IP カメラ AP を展開するときに、スイッチ ポートで PoE 優先順位を動的に設定するにはどうすればよいですか。他の PoE デバイスはどうですか?
A. PoE 電源管理を動的モードに設定します。
B. PoE 電源管理をクラスベース モードに設定します。
C. スイッチ モジュールで Quick 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 (メーッセージを残す**)**
説明
プロファイリングは、Aruba スイッチが MAC アドレス、DHCP オプション、LLDP 情報などのさまざまな属性に基づいて、接続されているデバイスを自動的に識別および分類できるようにする機能です。プロファイリングを使用すると、スイッチ ポートの PoE 優先順位を動的に設定できます。デバイスのタイプと電力要件。
たとえば、IP カメラはプリンタや PC よりも高い PoE 優先順位を持つ場合があります。プロファイリングを使用して、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こともできます。
参考文献:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-ove

最新問題: **2**
WPA3-Personal は、ステーションがワイヤレス ネットワークに接続するたびに異なるペアワイズ マスター キー (PMK) を生成するソースとして何を使用しますか?
A. セッション固有の情報 (MAC および nonce)
B. 日和見無線暗号化 (OWE)
C. 同等者同時認証 (SAE)
D. キー暗号化キー (KEK)
Answer: A (メーッセージを残す**)**
説明

ステーションがワイヤレス ネットワークに接続するたびに、WPA3-Personal が異なるペアワイズ マスター キー (PMK) を生成するために使用するソースは、セッション固有の情報 (MAC およびノンス) です。WPA3-Personal は、Simultaneous Authentication of Equals (SAE) を使用して、WPA2-Personal の PSK 認証を置き換えます。SAE は、Diffie-Hellman 鍵交換を使用して、盗聴者に公開することなく 2 者間の共有秘密を導出する安全な鍵確立プロトコルです。SAE には次の手順が含まれます。
ステーションとアクセス ポイントは、MAC アドレスとノンスと呼ばれる乱数を含むコミット メッセージを交換します。
ステーションとアクセス ポイントは、独自のパスワードと受信した MAC アドレスおよびノンスを使用して、SAE パスワード要素 (PE) と呼ばれる共有秘密を計算します。
ステーションとアクセス ポイントは、独自の PE、受信した MAC アドレスおよびナンスを使用して、SAE Key Seed (KS) と呼ばれる共有秘密を計算します。
ステーションとアクセス ポイントは、独自の KS と受信した MAC アドレスおよびノンスを使用して、SAE キー確認キー (KCK) と呼ばれる共有秘密を計算します。
ステーションとアクセス ポイントは、独自の KCK と受信した MAC アドレスおよびノンスを使用して、SAE 確認と呼ばれる確認値を計算します。
ステーションとアクセス ポイントは、SAE 確認値を含む確認メッセージを交換します。
ステーションとアクセス ポイントは、受信した SAE 確認値が独自の計算値と一致することを確認します。それらが一致すると、認証は成功し、ステーションとアクセス ポイントは SAE PMK と呼ばれる共有秘密を確立しました。
SAE PMK は、各認証プロセスで交換される MAC アドレスと nonce に依存するため、セッションごとに異なります。SAE PMK は、データ フレームを暗号化するためのペアワイズ一時キー (PTK) を生成する 4 ウェイ ハンドシェイクの入力として使用されます。
他のオプションは、次の理由により、ステーションがワイヤレス ネットワークに接続するたびに WPA3-Personal が異なる PMK を生成するために使用するソースではありません。
Opportunistic Wireless Encryption (OWE): OWE は、認証やパスワードを必要とせずにオープン ネットワークの暗号化を提供する機能です。OWE は SAE と同様のキー確立プロトコルを使用しますが、PMK は生成しません。代わりに、PTK を生成する 4 ウェイ ハンドシェイクの入力として使用されるペアワイズ シークレット (PS) を生成します。
Simultaneous Authentication of Equals (SAE): SAE はソースではありませんが、セッション固有の情報をソースとして使用して、ステーションがワイヤレス ネットワークに接続するたびに異なる PMK を生成するプロトコルです。
キー暗号化キー (KEK): KEK はソースではなく、PTK を生成する 4 ウェイ ハンドシェイクの出力です。KEK は、アクセス ポイントによって配布されるグループ キーを暗号化するために使用されます。
参考資料: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e
https://www.wi-fi.org/file/wi-fi-alliance-unlicensed-spectrum-in-the-us
https://www.cisco.com/c/en/us/products/colternate/wireless/catalyst-9100ax-access-points/wpa3-dep-guide-og.ht
https://info.support.huawei.com/info-finder/encyclopedia/en/WPA3.html
https://rp.os3.nl/2019-2020/p99/presentation.pdf

最新問題**: 3**
6 GHz 帯域の主な特徴は何ですか?
A. 6 GHz 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、6 GHz 帯域は、北米の 40 MHz チャネルよりも多くの 80 MHz チャネルを提供します。
5GHz帯。
C. 6 GHz 帯域は既存の帯域と完全に下位互換性があります。

D. 低電力デバイス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**)**
説明
指定されたオプションの中で当てはまる 6 GHz 帯域の主な特徴は、北米では 5 GHz 帯域の 40 MHz チャネルよりも 6 GHz 帯域が多くの 80 MHz チャネルを提供することです。この特性により、Wi-Fi 6E をサポートするワイヤレス デバイスにより多くのスペクトル可用性、より少ない干渉、より高いスループットが提供されます。Wi-Fi Enhanced (Wi-Fi 6E) は、新しい環境で動作する Wi-Fi 6 (802.11ax) 標準の拡張です。6 GHz 未満の既存の帯域に加えて、6 GHz 付近のライセンス不要の周波数スペクトルを利用できます。この特性に関するいくつかの事実は次のとおりです。
北米では、新しいスペクトル (5925 ～ 7125 MHz) のライセンス不要部分全体で、3 つのチャネル幅 (20 MHz、40 MHz、および 80 MHz) のそれぞれで最大 7 つの非重複チャネルが利用可能です。これは、Wi-Fi デバイスで合計最大 21 個の重複しないチャネルを利用できることを意味します。
比較すると、北米では、その下の既存のスペクトルの無認可部分全体 (2400 ～ 2483 MHz および 5150 ～ 5825 MHz) の 2 つのチャネル幅 (20 MHz と 40 MHz) のそれぞれで利用できる重複しないチャネルは 9 つだけです。）。これは、Wi-Fi デバイスで利用できる重複しないチャネルは合計で最大 9 つだけであることを意味します。
したがって、北米では、新しいスペクトルの各チャネル幅で、その下の既存のスペクトルよりも 2 倍以上の重複しないチャネルが利用可能になります。
具体的には、それ以下の既存のスペクトルでは、80 MHz 幅 (7 つ) では 40 MHz 幅 (3 つ) の 2 倍以上の非オーバーラップ チャネルが利用可能です。
他のオプションは次の理由により true ではありません。
6 GHz WLAN では、物体に吸収される RF 信号が少なくなります。減衰が大きいため、高周波信号の方が低周波信号よりも物体に吸収される傾向があるため、このオプションは false です。減衰とは、使用中に信号強度が低下することを指す一般用語です。距離を超えた、または物体や媒体を介した伝送。したがって、6 GHz WLAN の RF 信号は、より低い周波数の WLAN の RF 信号よりも物体に吸収されやすくなります。
6 GHz 帯域は既存の帯域と完全に下位互換性があります。Wi-Fi デバイスが 6 GHz 付近の新しいスペクトルで動作するには Wi-Fi 6E 標準をサポートする必要があるため、このオプションは false です。Wi-Fi 6E 標準をサポートしていない既存の Wi-Fi デバイスは、このスペクトルを使用できず、それ以下の既存の帯域でのみ動作できます。
低電力デバイスは屋内および屋外での使用が許可されます: 低電力屋内デバイス (LPI) は、特定の電力制限および登録要件の下でのみ屋内での使用が許可されているため、このオプションは false です。LPI デバイスの屋外使用は、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、および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。
参考資料: 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/colterior/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**: 4**
いくつかのクラスの LOT デバイスに対してワイヤレス アクセスを設定する必要があります。そのうちのいくつかは 802 でのみ動作します。11b. 各クラスには一意の PSK が必要で、役割として異なるセキュリティ ポリシーが適用される必要があります。デバイスには 15 ～ 20 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。どのオプションがこれらの要件を満たすかです。」

A. 5 GHz および 6 GHz 帯域を使用する各 LoT クラスの MPSK を備えた単一 SSID
B. 2.4 GHz および 5 GHz 帯域を使用する各 LoT クラスの MPSK を備えた単一 SSID
C. 5 GHz および 6 GHz 帯域を使用した、IoT クラスごとに固有の PSK を持つ個別の SSID
D. 2.4 GHz および 5 GHz 帯域を使用した、IoT クラスごとに固有の PSK を持つ個別の SSID
Answer: D (メーッセージを残す)
説明
要件を満たすオプションは、2.4 GHz および 5 GHz 帯域を使用して、IoT クラスごとに一意の 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次の利点があります。
各 IoT クラスには、異なるセキュリティ ポリシーをロールとして適用するために使用できる固有の PSK があります。これにより、WLAN ネットワークのセキュリティと柔軟性が強化されます。
個別の SSID により、さまざまな LOT クラスの分離と管理が向上します。これにより、WLAN ネットワークのパフォーマンスとスケーラビリティが向上します。
2.4 GHz 帯域と 5 GHz 帯域の両方を使用すると、2.4 GHz 帯域を使用する 802.11b でのみ動作する LOT デバイスとの下位互換性が可能になります。また、5 GHz 帯域 2 を使用する 802.11a、802.11g、802.11n、または 802.11ac をサポートする LoT デバイスのスループットが向上し、干渉が軽減されます。
他のオプションは次の理由により要件を満たしません。
5 GHz および 6 GHz 帯域を使用する各 IoT クラスの MPSK を備えた単一 SSID: このオプションは、2.4 GHz 帯域を使用する 802.11b でのみ動作する IoT デバイスをサポートしません。また、単一の SSID が異なる LoT 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は最適化されません。
2.4 GHz および 5 GHz 帯域を使用する各 IoT クラスの MPSK を備えた単一 SSID: 単一の SSID は、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、このオプションは WLAN ネットワークのパフォーマンスを最適化しません。
5 GHz および 6 GHz 帯域を使用する、IoT クラスごとに一意の PSK を持つ個別の SSID: このオプションは、2.4 GHz 帯域を使用する 802.11b でのみ動作する IoT デバイスをサポートしません1。
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**: 5**
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、ルートを交換するには隣接デバイスで何が一致する必要がありますか?
A. こんにちはタイマー
B. DR構成
C. ECMP方式
D. BDR 構成
Answer: (解答を表示する)
説明
OSPF 最短パスを最初に開きます。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 ルーターは、各インターフェイスで定期的に送信される Hello パケットを使用して近隣ルーターとルーティング情報を交換します。隣接関係を確立するには、隣接関係とは、ルーティング情報を交換する目的で、選択した隣接ルータ間で形成される関係です。OSPF ルータは、インターフェイス上で 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

メータに同意する必要があります。Hello タイマーが隣接ルーター間で一致しない場合、隣接ルーターは形成されず、ルートは交換されません。
参考資料:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/osfp/o

最新問題**: 6**
Aruba Central を使用する場合、ネットワークの健全性の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ものは何ですか?
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 (メーッセージを残す**)**
説明
OAIOps は、人工知能と機械学習を使用してネットワークの健全性の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ようにする Aruba Central の機能です。OAIOps は、ネットワーク パフォーマンス、根本原因分析、異常検出、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) センサーと統合して、有線および無線ネットワーク全体のユーザー 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**: 7**
ワイヤレス クライアントのローミングはどこで決定されますか?
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. アルバセントラル
Answer: A (メーッセージを残す**)**
説明
ワイヤレス 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 レートなどの独自の基準に基づいてクライアント デバイスによって行われます。ネットワークは、近隣レポート、ロード バランシング、バンド ステアリングなどの情報を提供することによって、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。、などですが、最終的な決定はクライアント次第です。
参考資料:https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/wlan-roaming/cli

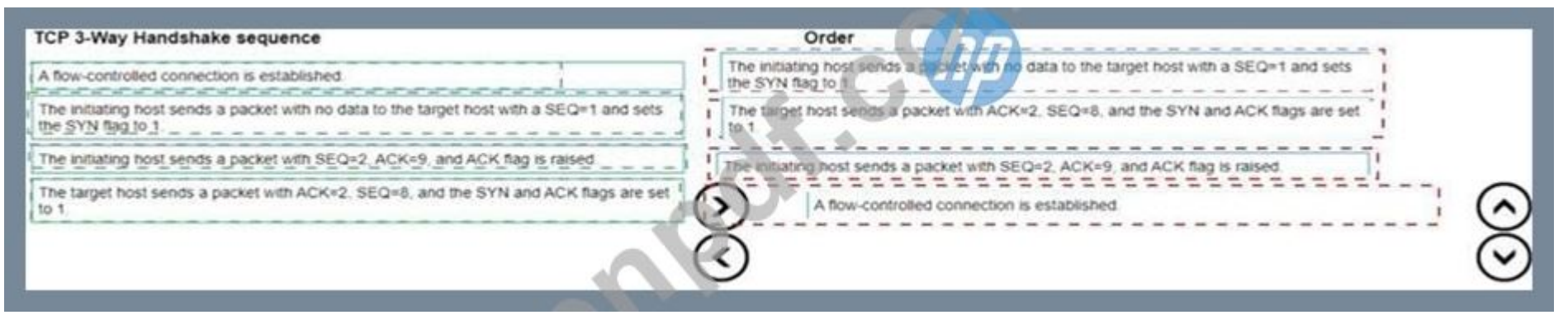
最新問題**: 8**
Aruba スタンドアロン AP を使用する場合、クライアント VLAN 割り当てに ネイティブ VLAN」を選択します。クライアント IP はどのサブネットに存在しますか?
A. モビリティ コントローラーと同じサブネット
B. Aruba ESP ゲートウェイと同じサブネット
C. モビリティ コンダクターと同じサブネット
D. アクセスポイントと同じサブネット
Answer: D (メーッセージを残す**)**

説明
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 アドレスを取得することになります。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。
参考文献 :https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/iap-dhcp/iap-dhc

最新問題**: 9**
レイヤ 3 ルート ループを軽減するためにレイヤ 3 IPv4 パケット ヘッダーで送信されるのはどれですか?
A. チェックサム
B. 生存時間
C. プロトコル
D. 宛先IP
Answer: B (メーッセージを残す**)**
説明
レイヤ 3 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、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す 8 ビットのフィールドです。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ーによって 1 ずつ減分されます。TTL がゼロに達すると、パケットはドロップされ、ICMP インターネット制御メッセージ プロトコル (ICMP) インターネット制御メッセージ プロトコル (ICMP) は、IP ネットワークに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、パラメーターの問題、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、タイプなどのフィールドを含む特定の形式を持ちます。、コード、チェックサム、識別子、シーケンス番号、データなど。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。など。メッセージがソースデバイスに送り返されます。TTL は、ループされたネットワーク トポロジ内でパケットが無制限に循環するのを防ぐため、レイヤー 3 ルート ループを軽減するために使用されます。TTL は、ネットワーク リソースを節約し、ループされたパケットによって引き起こされる輻輳を回避するのにも役立ちます。
他のオプションは、次の理由により、レイヤー 3 IPv4 パケット ヘッダーのフィールドではありません。
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。チェックサムはソース デバイスによって計算され、IP ヘッダー内のすべてのフィールドの値に基づいて宛先デバイスによって検証されます。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 ルート ループを軽減しません。
プロトコル: プロトコルは、IP データグラムによって伝送されるペイロードのタイプを示す 8 ビットのフィールドです。プロトコルは、TCP など、データ送信に 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) 伝送制御プロトコル (TCP) は、信頼性が高く、順序付けられ、エラー チェックされたデータ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。異なるデバイス上のアプリケーション間で。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、およびウィンドウ処理を使用してデータ配信とフロー制御を保証します。TCP は、再送信、輻輳回避、高速回復などのメカニズムを使用して、パケット損失や輻輳に対処します。TCP はデータをセグメントと呼ばれる小さな単位に分割します。これらは 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形式を持ちます。TCP セグメントは、telnet、ftp、ssh、debug ip tcptransactions 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、コネクションレス型トランスポート層プロトコルです。

最新問題**: 10**
TCP 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?

Answer:



説明
TCP 3 ウェイ ハンドシェイク シーケンスは次のとおりです。
ステップ 1: 開始ホストは、データのないパケットを SEQ=1 でターゲット 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、および SYN フラグと ACK フラグが に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、および 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: 通常制御された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**: 11**
AP からの信号が物体を通過するときに吸収されて弱まるとどうなりますか?
A. AP はボンディングされたチャネルを使用して、クライアントへの遅延を短縮します。
B. 信号対雑音比 (SNR) が増加します。
C. 信号対雑音比 (SNR) が低下します。
D. Aruba Central はクライアントを隣接する AP に動的に移動します
Answer: C (メーッセージを残す**)**
説明
信号対雑音比 (SNR) は、目的の信号のレベルとバックグラウンド ノイズのレベルを比較する尺度です。SNR は信号パワーとノイズ パワー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、信号がクリアで検出または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、信号がノイズによって破損または隠蔽されており、区別または回復が難しい可能性があることを意味します1。AP アクセス ポイントからの信号のとき。AP は、無線デバイスが Wi-Fi または関連規格を使用して有線ネットワークに接続で

きるようにするデバイスです。信号が壁や家具などの物体を通過するときに吸収されて弱まると、信号パワーが減少します。これにより SNR が低下し、ワイヤレス接続の品質に影響します。他の発生源からの干渉によってノイズ電力も増加する可能性があります。同じ周波数帯域で動作する他の AP やデバイスなど 2。したがって、正解は、AP からの信号が物体を通過するときに吸収されて弱まると、SNR が低下するということです。参考文献: 1
https://en.wikipedia.org/wiki/信号対雑音比 2
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_%28SNR%29

最新問題**: 12**
アドミニストレーティブ ディスタンスの目的の説明
A. 外部 BGP 経由でチーム化されたルートは、OSPF 経由で学習されたルートよりもアドミニストレーティブ ディスタンスが高くなります。
B. スタティック ルートのアドミニストレーティブ ディスタンスは 10 です
C. アドミニストレーティブ ディスタンスは、ルート エントリの信頼性評価として使用されます。
D. アドミニストレーティブ ディスタンスが高いほど優先されます。
Answer: C (メーッセージを残す**)**

最新問題**: 13**
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はどれが正しいですか?
A. 手動プロビジョニングには DHCP は必要ありませんが、DNS が必要です
B. 手動プロビジョニングには 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 が必要ですが、DNS は必要ありません
D. 手動プロビジョニングには DHCP と DNS が必要です
Answer: B (メーッセージを残す**)**
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。ユーザーは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 Aruba Central に入力し、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

最新問題**: 14**
顧客の導入環境に新しい Aruba 6300M をオンボードするよう求められました。オンサイトではなくリモートで作業しています。同僚がスイッチを設置しています。同僚がエッジ 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ました。あなたは次のことを行うように求められています。インターフェイス 1/1/51 および 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します。プロジェクトのシニア エンジニアは、次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に依頼しました。
1. VLAN 20 を Mgmt という名前でローカル VLAN データベースに追加します。
2. 10.1.1 0/24 サブネットのアドレス 10 を使用して、管理用に VLAN 20 に L3 SV1 を追加します。3. アップリンクに対してアクティブな LACP モードを使用して LAG 1 を追加します。
4 LAG 上のネイティブ VLAN として VLAN 20 を使用します。5. インターフェイスがすべて ON であることを確認します。
どの構成スクリプトがタスクを達成しますか?

A. Edge1# conf t vlan 20 name Mgmt interface vlan 20 ip address 10.1.1.10/24 no shut インターフェイスラグ 1 shut vlan access 20 lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 インターフェイスラグ1ノーシャット
B. Edgel# conf t vlan 20 name Mgmt Interface VLAN 20 IP address 10 1.1 10/24 no shut インターフェイス 1/1/51.1/1/52 シャット 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 インターフェイス 1/1/51.1/1/52 シャットなし
C. Edgel# conf t vlan 20 name Mgmt Interface vlan 20 ip address 10 1 1 10/24 no shut インターフェイスラグ 1 shut vlan トランク ネイティブ 20 vlan トランク許可すべて lacp モード active Int 1/1/51.1/1/52シャット ルーティング ラグ 1 なし インターフェイス ラグ 1 なし シャット インターフェイス 1/1/51.1/1/52 シャットなし
D. conf t vlan 20 名前管理 IP アドレス 10 1 1.10/24 no shut インターフェイスラグ 1 shut vlan トランクネイティブ 1 vlan トランク許可すべて lacp モード active int 1/1/51.1/1/52 shut no ルーティングインターフェイスラグ 1シャットインターフェースがありません 1/1/51.1/1/52 ノーシャット
Answer: C (メーッセージを残す)
説明
この構成スクリプトは、シニア エンジニアによって与えられたガイドラインに従ってタスクを実行します。Mgmt という名前の VLAN 20 を作成し、IP アドレス 10.1.1.10/24 の VLAN 20 に L3 SVI を追加し、アップリンクに対して LACP モードがアクティブな LAG 1 を作成し、VLAN 20 を LAG 上のネイティブ VLAN として使用し、インターフェイスがはすべてオンになっています。
参考文献 :https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-8F0E7E8B-0F4

最新問題**: 15**
推奨される VSF トポロジは何ですか? (2つ選択してください。)
A. スター
B. デイジーチェーンプラスMAD
C. フルメッシュ
D. フルメッシュ+MAD
E. リング
Answer: B,E (メーッセージを残す)
説明
のみ: デイジー チェーンと MAD およびリングは、Aruba スイッチに推奨される VSF トポロジです。これらは、VSF スタックに高可用性と冗長性を提供します。MAD (Multiple Active Detection) は、VSF スタック内のスプリット ブレイン シナリオを検出して解決するメカニズムです。
参考文献 :https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-D6EF042E-EEE

最新問題**: 16**
要求どおりにエッジ スイッチのアップリンクを設定した後、同僚がコアへの ping に失敗したと言います。あなたは同僚に、接続が差し込まれており、スイッチの電源が入っていることを確認するように依頼します。同僚は両方が正しいことを確認します。あなたはコア スイッチに ping を試みます。ping が失敗していることを確認します。
この展開の性質を理解した上で、この問題のトラブルシューティングにどのようなコマンドを使用できるか
A. Ping 10.11 1 - コアに ping して、接続性を確認します。トランクを表示 - 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。スパニング ツリーを表示します。- スパニング ツリーのブロック状態を確認します。ポート アクセス クライアント インターフェイスをすべて表示します。- 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失敗した認証試行を表示します。

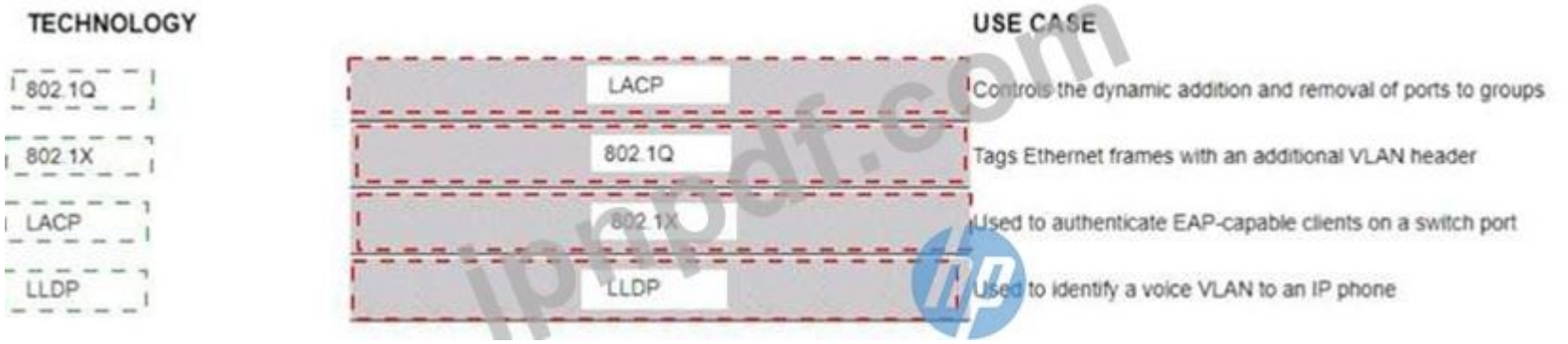
show runinterface vlan20 - I_3 接続に対してレイヤ 3 SVI 設定が正しいことを再確認します。Show lldp neighors - コアをL2 ネイバーは、正しいリンクが正しいポートに接続されているかどうかを確認します。
B. Diag diag Cable-diag 1/1/51 diag Cable-diag 1/1/52 - 物理リンクの診断情報を表示して、レイヤー 1 接続の中断に関するステータスを取得するには、show ip Route - 確認します。デフォルト ゲートウェイがルーティング テーブルに存在すること show ip ospf - レイヤ 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する show ip dns - 有効な DNS ソースがあるかどうかを表示する
C. 10.1.1.1 に ping - コアに ping を実行して、接続を確認します。show lacp agg - どのリンク アグリゲーションが現在どの物理ポートを使用して設定されているかを確認します。show lacp int - LACP ステータスと、リンクがブロックされているかどうかを確認します。トポロジ show lldp neighors - コアを L2 ネイバーとして認識できるかどうかを確認し、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 runinterface 1/1/51.1/1/52 - 物理インターフェイスを確認します。no-shut であり、ラグのメンバーである show runinterface lag 1 - 正しい VLAN トランキング設定が論理インターフェイスに適用されていることを確認するため show run int vlan 20 - L3 SVI が no shut であり、正しいサブネットに設定されていることを確認するため
D. Show run - スイッチの実行構成を表示します。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するには、show run | begin 20 'interface vlan 20' - L3 SVI 設定を表示します Show runinterface 1/1/51.1/1/52 - 物理インターフェイスがシャットされておらず、LAG 1 のメンバーとして追加されていることを確認します Show run int lag 1 - LACP ブロック状態を解消するために LACP モードがアクティブに設定されていることを確認します
Answer: C (メーッセージを残す)
説明
これらのコマンドは、レイヤー 3 の到達可能性、レイヤー 2 の隣接関係、LACP の構成とステータス、VLAN トランキングの構成、インターフェイスのステータスなど、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場合があります。
参考文献 :https://www.arubanetworks.com/techdocs/AOS-CX_10_04/CLI/GUID-8F0E7E8B-0F4B-4A3C-AE7

最新問題**: 17**
信号強度を測定する場合は、dBm が一般的に使用され、0 dBm は 1 mW の電力に相当します。
-20 dBm は何に相当しますか?
A. .-1mW
B. .01mw
C. 10mW
D. 1mW
Answer: B (メーッセージを残す)
説明
dBm は、1 mW に対する特定の電力レベル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) = 0.01mW 参考文献:https://www.rapidtables.com/convert/power/dBm_to_mW.html

最新問題: **18**
スイッチング テクノロジーを適切な使用例に合わせてください。

Answer:



説明
使用例: a) グループへのポートの動的な追加と削除を制御します テクノロジー: 3) LACP 使用例: b) 追加の VLAN ヘッダーでイーサネット フレームにタグ付けします テクノロジー: 1) 802.1Q 使用例: c) EAP 対応の認証に使用されますスイッチ ポート上のクライアント テクノロジー: 2) 802.1X 使用例: d) IP 電話への音声 VLAN を識別するために使用されます 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使用例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さまざまなブロードキャスト ドメインに論理的にセグメント化し、セキュリティ、パフォーマンス、管理性を向上させることができます。802.1Q は、フレームがどの VLAN に属しているかを示す VLAN 識別子 (VID) を含む追加の VLAN ヘッダーでイーサネット フレームをタグ付けします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標準です。
PNAC を使用すると、ネットワーク管理者は、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承認できます。802.1X は、拡張認証プロトコル (EAP) を使用して、サプリカント (ネットワークにアクセスするデバイス)、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の間で認証メッセージを交換します。(RADIUS サーバーなど、サプリカントの資格情報を検証するデバイス)

3) LACP
LACP は Link Aggregation Control Protocol の略で、複数の物理リンクを 1 つの論理リンクにバンドルする方法を定義する IEEE 802.3ad 標準の一部であり、リンク アグリゲーション グループ (LAG) または EtherChannel とも呼ばれます。LAG は、ネットワーク接続の帯域幅、負荷分散、冗長性の向上を実現します。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 LAG3 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およびアドバタイズする方法を定義する IEEE 802.1AB 標準の一部です。LLDP は OSI モデルのレイヤー 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 を送信することにより、IP 電話に音声 VLAN を識別できます。
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**: 19**
スイッチ EDGE1 および CORE1 にいくつかの show コマンドを入力して、問題のトラブルシューティングのための情報を収集しようとします。show コマンドの出力イメージを使用して、EDGE1 アップリンクがダウンしている理由を特定します。

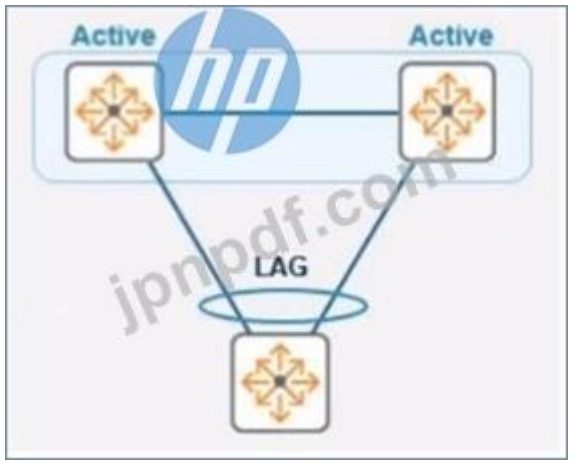
```
DGE1# show span vlan 20
ort         Role          State
   TCN-Tx     TCN-Rx
---------- ------------- ---------
-- ---------- ----------
agl         Disabled      Blocking
   2           2
DGE1# show run int 1/1/51
nterface 1/1/51
   no shutdown
   description Uplink_To_Core1
   lag 1
   exit
DGE1# show run int 1/1/52
nterface 1/1/52
   no shutdown
   description Uplink_To_Core1
   lag 1
   exit
DGE1# show run int lag1
nterface lag 1
   no shutdown
   no routing
   vlan trunk native 20
   vlan trunk allowed all
   lacp mode active
   exit
E1# show lacp int
or details of all interfaces:
---------------------------------------------------------------------------------------------
f       Aggr        Port  Port  State   System-ID          System Aggr Forwarding
        Name        Id    Pri             Pri    Key State
---------------------------------------------------------------------------------------------
/51     lag1        53    1     ALFOE   b0:d4:e7:b5:22:80 65534  1    lacp-block
/52     lag1        53    1     ALFOE   b0:d4:e7:b5:22:80 65534  1    lacp-block
```

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

A. 物理インターフェイスは正しい LAG のメンバーではありません。
B. スパニングツリー ブロック状態により、コア アップリンクがエッジに接続できなくなります。
C. コアが間違った物理インターレースに接続されています
D. LACP がコア アップリンクに設定されていません
Answer: (解答を表示する**)**
説明
LACP は、帯域幅と冗長性を向上させるために、複数の物理リンクを 1 つの論理リンクに集約できるようにするプロトコルです。LACP が正しく動作するには、リンクの両端で LACP を設定する必要があります。この場合、EDGE1 のアップリンク ポート チャネル 1 には LACP が設定されていますが、CORE1 の対応するポート チャネル 1 には LACP が設定されていません。これにより不一致が発生し、リンクが起動できなくなります。

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

最新問題: **20**
展示を参照してください。



指定されたトポロジでは、Aruba CX 8325 スイッチのペアが、アクティブ ゲートウェイを使用する VSX スタック内にあります。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 の性質と動作は何ですか?

A. 仮想 IP はプライマリ VSX スイッチでアクティブです
仮想フローティング IP は障害が発生した場合にフェイルオーバーします。
B. 仮想 IP は両方の CX スイッチでアクティブです
C. 仮想 IP は VSX と同期された SVI IP アドレスを使用します

Answer: A (メーッセージを残す**)**
説明
Virtual Switching Extension (VSX) は、2 つの Aruba CX スイッチが、単一のコントロール プレーンとデータ プレーンを持つ単一の論理デバイスとして動作できるようにする機能です。VSX は、キャンパスおよびデータセンターのネットワークに高可用性、拡張性、および簡素化された管理を提供します3。VSX では、1 つのスイッチがプライマリ スイッチとして指定され、もう 1 つがセカンダリ スイッチとして指定されます。プライマリ スイッチは、ARP アドレス解決プロトコルを所有し、それに応答します。ARP は、特定のインターネット層アドレス (通常は IPv4 アドレス) に関連付けられた MAC アドレスなどのリンク層アドレスを検出するために使用される通信プロトコルです。このマッピングは、インターネット プロトコル スイートの重要な機能です。VSX ペアの仮想 IP アドレスを要求します4。仮想 IP アドレスは、アクセス スイッチに接続されているクライアントのデフォルト ゲートウェイとして使用されます。
参考文献: 3
https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-overview.htm 4
https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-ip-addressing.htm 5
https://www.arubanetworks.com/techdocs/AOS-CX_10_04/UG/Content/cx-ug/vsx/vsx-failover.htm

最新問題: **21**
配信およびレイヤー 3 サービスに使用される 6300M スイッチのスタック ペアを使用して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 スイッチの複数のアクセス 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。これと同様の複数の VLAN/サブネットを作成します。これらは複数のアクセス スタックで利用されます。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はどれですか?

A. 各ダウンストリーム スイッチの 6300M スタック上のサブネット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します。

B. 各ダウンストリーム スイッチのサブネットに SVI を作成します。
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 (メーッセージを残す)
説明
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設定する正しい方法は、SVI スイッチ仮想インターフェイス $VI）を作成することです。スイッチ仮想インターフェイス $VI）は、VLAN を表し、レイヤ 3 ルーティングを提供するスイッチ上の仮想インターフェイスです。その VLAN の機能。SVI は、VLAN 間ルーティングの有効化、VLAN 内のホストのゲートウェイ アドレスの提供、VLAN への ACL または QoS ポリシーの適用に使用されます。
、など。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、物理ルーテッド インターフェイスに比べていくつかの利点があります。通常、SVI には、VLAN ID（vlan 10 など）と、VLAN のサブネット内で割り当てられた IP アドレスに従って番号が付けられます。SVI は、インターフェイス vlan、ip アドレス、no shutdown などのコマンドを使用して作成および設定できます。SVI は、show ipinterfacebrief、showvlan、showiproute などのコマンドを使用して確認できます。6300M スタック上のサブネット内。
SVI は、VLAN を表すスイッチ上の仮想インターフェイスであり、その VLAN にレイヤ 3 ルーティング機能を提供します。6300M スタック上のサブネットに SVI を作成すると、スイッチがその VLAN 内のユーザ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。6300M スタック上のサブネットに SVI を作成すると、ルーティングに必要な物理インターフェイスとケーブルの数が減り、ネットワークの設計と管理も簡素化されます。
他のオプションは、次の理由により、サブネットがこの VLAN に関連付けられるようにルーティング可能なインターフェイスを構成する正しい方法ではありません。
各ダウンストリーム スイッチの 6300M スタック上のサブネット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: 各ダウンストリーム スイッチの 6300M スタック上のサブネット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には、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るため、このオプションは正しくありません。インターフェースのリソースを消費し、ケーブルのコストが増加します。各ダウンストリーム スイッチの 6300M スタック上のサブネットに物理的にルーティングされる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設定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も複雑になります。
各ダウンストリーム スイッチのサブネットに SVI を作成します。各ダウンストリーム スイッチのサブネットに SVI を作成すると、各ダウンストリーム スイッチが独自の VLAN のゲートウェイとして機能するため、異なるサブネット間の VLAN 間ルーティングが有効にならないため、このオプションは正しくありません。それだけ。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 アドレスも作成され、IP の競合やルーティング エラーが発生します。
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別の IP アドレスに割り当てます。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 アドレスに変更しても、各ダウンストリーム スイッチは依然として独自の VLAN のみのゲートウェイとして機能するため、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。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別の IP アドレスに割り当てると、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-ove
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-con

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 (**104** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)