HP.HPE6-A85.v2026-02-02.q111

試験コード：	HPE6-A85
試験名称：	Aruba Campus Access Associate Exam
認証ベンダー：	HP
無料問題の数：	111
バージョン：	v2026-02-02
ページの閲覧量：	110
問題集の閲覧量：	1333

https://www.jpnshiken.com/shiken/HP.HPE6-A85.v2026-02-02.q111.html

質問: **1**
顧客の導入環境に新しいAruba 6300Mをオンボードするよう依頼されました。作業はオンサイトではなくリモートで行います。スイッチの設置は同僚が担当します。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、管理用のVLAN 20に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を追加する
4. LAGのネイティブVLANとしてVLAN 20を使用する
5. インターフェースがすべてオンになってい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 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 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 すべての遅延 1 LACP モード アクティブ インターフェース
1/1/51.1/1/52 シャットオフなし
C. Edgel# 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 シャットオフなし
正解: **(**正解を表示します**)**
この設定スクリプトは、シニアエンジニアのガイドラインに従ってタスクを達成します。VLAN 20をMgmtという名前で作成し、VLAN 20にIPアドレス10.1.1.10/24のL3 SVIを追加し、LAGを作成します。
1 はアップリンクに対して LACP モードをアクティブにし、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すべてオンになってい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/GUID-

8F0E7E8B-0F4

質問: **2**
既存の IAP-315 アクセス ポイントを持つネットワーク管理者は、Aruba Central に興味があり、特定の機能に必要なライセンスを知る必要があります。機能ごとに必要なライセンスを一致させてください (一致は複数回使用できます)。

正解:

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コンプライアンス - Foundation c) 展開された AP のヒートマップ - Advanced d) AOS10 クラスターのライブアップグレード - Advanced Aruba Central ライセンスガイド 1 によれば、Foundation ライセンスでは、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が提供されます。Advanced ライセンスでは、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が提供されます。
https://www.arubanetworks.com/techdocs/central/2.5.3/content/pdfs/ライセンスガイド.pdf

質問: **3**
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正しい記述はどれですか?
A. 手動プロビジョニングではDHCPは不要ですが、DNSが必要です。
B. 手動プロビジョニングではDHCPは不要で、DNSも不要です。
C. 手動プロビジョニングにはDHCPが必要で、DNSは必要ありません。
D. 手動プロビジョニングにはDHCPが必要であり、DNSが必要です
正解: **(**正解を表示します**)**
説明
手動プロビジョニングは、DHCPやDNSを使用せずにAruba Centralにスイッチを追加する方法です。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

質問: **4**
ゆっくりオレンジ色に点滅するスタック LED は何を示していますか?
A. 1 つのスイッチにスタッキング障害が発生しています。
B. ポートにスタッキング障害が発生しています。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しています。お待ちください。
正解: **(**正解を表示します**)**
スタックLEDがオレンジ色でゆっくり点滅している場合は、スイッチでスタック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整っているか、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。参考 :https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/stacking-leds。htm

質問: **5**
6GHz帯の主な特徴は何ですか？
A. 6 GHz WLAN では、物体によって吸収される RF 信号が少なくなります。
B. 北米では、6GHz帯では、40MHzのチャンネルよりも多くの80MHzのチャンネルが提供されています。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ます。
正解: **(**正解を表示します**)**
説明
提示された選択肢の中で6GHz帯の最も確かな特徴は、北米では6GHz帯の80MHzチャネルが5GHz帯の40MHzチャネルよりも多く利用可能であるということです。この特徴により、Wi-Fi 6Eをサポートする無線デバイスは、より多くの周波数帯域を利用でき、干渉が少なく、スループットが向上します。Wi-Fi Enhanced（Wi-Fi 6E）は、Wi-Fi 6（802.11ax）規格の拡張版であり、既存の6GHz帯以下の周波数帯域に加えて、新たに利用可能になった6GHz付近の無認可周波数帯域でも動作します。この特徴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つのチャネル幅（20MHz、40MHz、80MHz）それぞれに最大7つの重複しないチャネルが利用可能です。つまり、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21個になります。
比較すると、北米では、既存の無認可帯域（2400～2483MHzおよび5150～5825MHz）全体において、2つのチャネル幅（20MHzおよび40MHz）それぞれに、重複しないチャネルがわずか9つしかありません。つまり、Wi-Fiデバイスが利用できる重複しないチャネルは合計で最大9つしかありません。
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利用できる重複しないチャネルの数が、その下の既存のスペクトルの 2 倍以上になります。
具体的には、80 MHz 幅 (7 つ) では、それ以下の既存のスペクトルの 40 MHz 幅 (3 つ) よりも 2 倍以上の非重複チャネルが利用可能です。

他のオプションは、次の理由により正しくありません。
6GHz帯WLANでは物体によるRF信号の吸収が少ない :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、低周波信号よりも物体による吸収が大きい傾向があるためです。減衰とは、長距離伝送時、または物体や媒体を介した伝送時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、6GHz帯WLANのRF信号は、低周波帯WLANのRF信号よりも物体による吸収が大きくなります。
6 GHz帯は既存の帯域と完全な下位互換性があります。Wi-Fiデバイスは、6 GHz帯を中心とした新しいスペクトルで動作するためにWi-Fi 6E規格をサポートする必要があるため、このオプションは無効です。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します。
低電力デバイスは屋内および屋外での使用が許可されています: 低電力屋内デバイス (LPI) は、一定の電力制限および登録要件の下で屋内での使用のみが許可されているため、このオプションは false です。LPI デバイスの屋外での使用は、FCC (米国連邦通信委員会 (FCC) は米国政府の独立機関であり、米国全土におけるラジオ、テレビ、有線、衛星、ケーブルによる通信を規制しています) などの規制当局によって禁止されています。ただし、超低電力デバイス (VLP) の屋外での使用は、一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/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

質問: **6**
セキュリティのために WPA2-Personal を使用すると、WLAN 環境にどのような脆弱性が生じますか?
A. 認証局によって生成されたX509証明書を使用します
B. ペアワイズ一時キー（PTK）は各セッションに固有です
C. ペアワイズマスターキー（PMK）はすべてのユーザーによって共有されます
D. WPA 4ウェイハンドシェイクを使用しません
正解: **(**正解を表示します**)**
WPA2-Personalをセキュリティに使用した場合、WLAN環境に導入される脆弱性は、PMK（ペアワイズマスターキー）がPSK（事前共有キー）から派生した鍵であることです。PSKは通信開始前に2者間で共有される鍵で、どちらも固定されています。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を生成できます。これは、PSK または PMK が攻撃者によって侵害された場合、それらを使用して PTK で暗号化されたすべてのトラフィックを復号化できることも意味します。PTK (Pairwise Temporal Key) は PMK から派生したキー、ANonce Authenticator Nonce (ANonce) は認証子 (AP などのネットワーク 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、SNonce Supplicant Nonce (SNonce) はサプリカント (STA などのネットワーク リソースにアクセスするデバイス) によって生成される乱数、AA Authenticator Address (AA) は認証子の MAC アドレス、SA Supplicant Address (SA) は疑似乱数関数 (PRF) を使用するサプリカントの MAC アドレスです。PTK は 4 つのサブキーで構成されます: KCK キー確認キー (KCK) はメッセージの整合

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 メッセージ整合性コード (MIC) キーが使用されます。
その他のオプションは、以下の理由により弱点ではありません。
証明機関によって生成された X 509 証明書を使用します。: WPA2 パーソナルは認証に X 509 証明書も証明機関も使用しないため、このオプションは false です。X 509 証明書と証明機関は、802.1X と EAP を使用する WPA2 エンタープライズ モードで使用されます。拡張認証プロトコル (EAP) は、パスワード、証明書、トークン、生体認証などの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、ワイヤレス ネットワークやポイントツーポイント接続で使用され、サプリカント (ネットワークにアクセスするデバイス) と認証サーバー (サプ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 サーバーによるユーザー認証用 RADIUS (リモート認証ダイヤルイン ユーザー サービス) 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的な認証、承認、アカウンティング (AAA) 管理を提供するネットワーク プロトコルです。
Pairwise Temporal Key（PTK）はセッションごとに固有です :このオプションは無効です。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、通信中に時間や送信パケット数に基づいて定期的にPTKが変更されることを意味します。これにより、リプレイ攻撃を防ぎ、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 :WPA2-Personalは鍵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、このオプションは無効です。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を生成するプロセスです。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することができます。

質問**: 7**
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、クライアントへの影響を最小限に抑えながら、RF 近隣データに基づいてすべての AP を分割するテクノロジはどれですか。
A. アルバクライアントマッチ
B. Aruba Aiの洞察
C. アルバ エアマッチ
D. アルバ ESP
正解**: (**正解を表示します**)**
説明
Aruba AirMatchは、RF無線周波数を最適化する機能です。RFとは、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、空間を伝搬できる電磁場が生成されます。機械学習アルゴリズムと履歴データを用いて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、RFneighborhoodデータに基づいてすべてのAPをパーティション化し、クライアントへの影響を最小限に抑えることで、Aruba APのファームウェアのライブ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採用しています。参考資料：

https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdfhttps://www.arubanetworks.com/techdocs/ArubaOS

質問: **8**
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正しい記述はどれですか?
A. 手動プロビジョニングではDHCPは不要ですが、DNSが必要です。
B. 手動プロビジョニングではDHCPは不要で、DNSも不要です。
C. 手動プロビジョニングにはDHCPが必要で、DNSは必要ありません。
D. 手動プロビジョニングにはDHCPが必要であり、DNSが必要です
正解: **B (**コメントを発表する**)**
手動プロビジョニングは、DHCPやDNSを使用せずにAruba Centralにスイッチを追加する方法です。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。
参考文献:
https://help.central.arubanetworks.com/latest/documentation/online_help/content/devices/switches/p

質問: **9**
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 トラフィックをどのように確立するのでしょうか。
A. Aruba 6300M ではルーティングがデフォルトで有効になっています。
B. ルート リークはデフォルトの VRF で設定する必要があります。
C. SVI インターフェイスから「ルーティングなし」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。
正解: **(**正解を表示します**)**
Aruba CX 6300Mスイッチでは、スイッチ仮想インターフェース（SVI）間のルーティングがデフォルトで有効になっています。そのため、SVI120とSVI130間のトラフィックは、SVIに「no routing」設定が存在しない限り、ルートリーク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ルーティングできます。

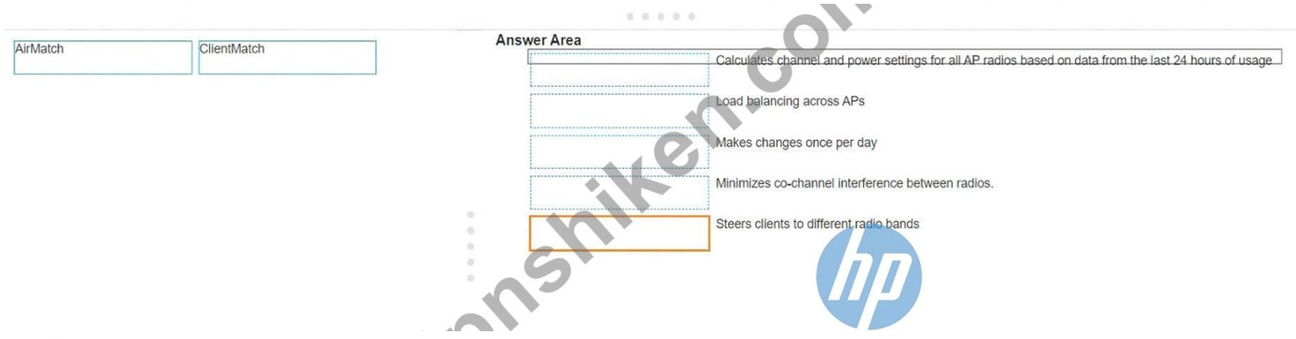
質問: **10**
WPA3-Personal では、ステーションがワイヤレス ネットワークに接続するたびに異なる Pairwise Master Key (PMK) を生成するために、ソースとして何を使用するのでしょうか?
A. セッション固有の情報（MACとノンス）
B. 無線暗号化（OWE）
C. 同時同等認証 (SAE)
D. キー暗号化キー (KEK)
正解: **A (**コメントを発表する**)**
説明
WPA3-Personalでは、ステーションがワイヤレスネットワークに接続するたびに異なるペアワイズマスターキー（PMK）を生成するために、セッション固有の情報（MACアドレスとノンス）を使用します。WPA3-Personalは、WPA2-PersonalのPSK認証に代わる、同等性同時認証（SAE）を使用します。SAEは、Diffie-Hellman鍵交換

を用いて、盗聴者に漏洩することなく二者間で共有秘密鍵を生成する、安全な鍵確立プロトコルです。SAEは以下の手順で実行されます。
ステーションとアクセス ポイントは、MAC アドレスと nonce 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 nonce を使用して、SAE パスワード エレメント (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 と受信した MAC アドレスおよび nonce 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 nonce 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 nonce を使用して、SAE Confirm 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 Confirm 値を含む Confirm 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 Confirm値が、それぞれが計算した値と一致することを確認します。一致する場合、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鍵を確立します。
SAE PMKは、各認証プロセスで交換されるMACアドレスとノンスに依存するため、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鍵（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。
その他のオプションは、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 PMK を生成するために WPA3-Personal が使用するソースではありません。その理由は次のとおりです。
OWE（Opportunistic Wireless Encryption）：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実現する機能です。OWEはSAEと同様の鍵確立プロトコルを使用しますが、PMK（鍵確立鍵）を生成しません。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Pairwise Secret（PS）を生成します。
同時同等認証 (SAE): SAE はソースではありませんが、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、セッション固有の情報をソースとして使用して異なる PMK を生成するプロトコルです。
キー暗号化キー（KEK）：KEKはPTKを生成する4ウェイハンドシェイクのソースではなく、出力です。KEKは、アクセスポイントから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/collateral/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

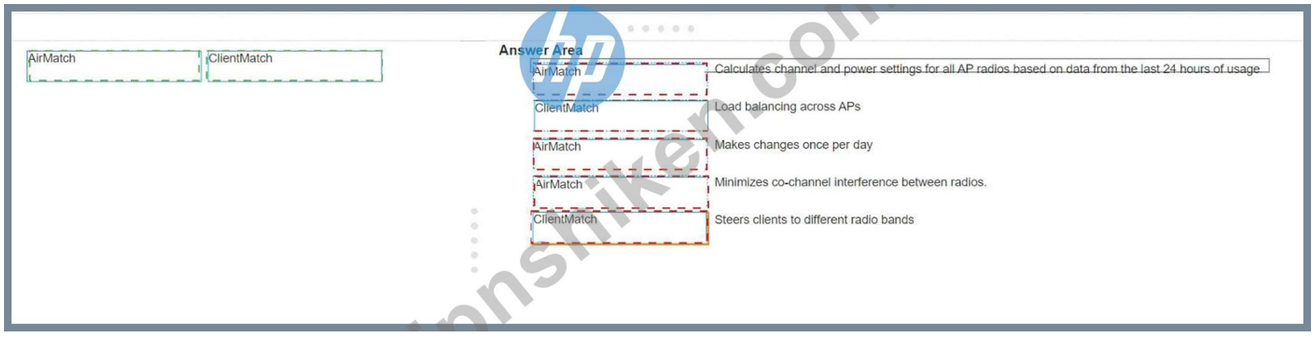
質問**: 11**
ゼロ タッチ プロビジョニング (ZTP) が最も効果的なシナリオはどれですか? (2 つ選択)
A. IT スタッフがいない小規模ネットワーク向け。

B. 構成が頻繁に変更されるネットワークの場合。
C. 高いセキュリティが懸念され、手動での設定が必要な場合。
D. 大規模なネットワークを迅速に展開する場合。
正解: **(**正解を表示します**)**

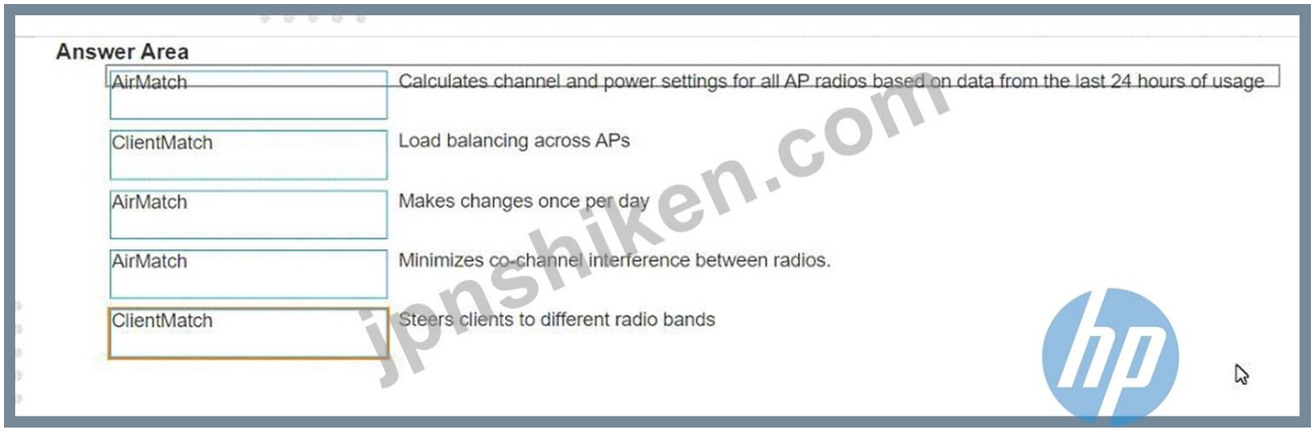
質問: **12**
Aruba Central テクノロジーを適切な機能と一致させてください。(一致は複数回使用できます。)



正解:



Explanation:
コンピュータのスクリーンショット 説明は自動的に生成されました



質問: **13**
Microbranch 環境を管理するには、どのようなタイプのデバイス タイプとグループ 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
正解: **(**正解を表示します**)**
Arubaネットワークにおいて、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グループペルソナは、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とグループペルソナです。

質問: **14**
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 WLAN に安全に追加できる Aruba テクノロジーはどれですか。
A. 有線同等プライバシー (WEP)
B. 複数事前共有鍵 (MPSK)
C. 無線暗号化 (OWE)
D. 一時鍵整合性プロトコル (TKIP)
正解: **(**正解を表示します**)**
多重事前共有キー (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 ワイヤレス 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、ワイヤレス コンピュータ ネットワークであり、無線通信を使用して 2 台以上のデバイスをリンクして、自宅、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にローカル エリア ネットワーク (LAN) を形成します。MPSK は、WPA2 PSK Wi-Fi Protected Access 2 事前共有キーを拡張します。WPA2 PSK は、オプションの事前共有キー (PSK) 認証を使用して WPA2 でネットワークを保護する方式で、エンタープライズ認証サーバーがないホーム ユーザー向けに設計されています。同じ SSID サービス セット識別子 (SSID) 上の異なるデバイスに異なる PSK を許可するモードです。SSID は、ワイヤレス ローカル エリア ネットワーク (WLAN) 経由で送信されるパケットのヘッダーに付加される、大文字と小文字が区別される 32 文字の英数字の一意の識別子です。 SSIDは、モバイルデバイスがIEEE 802.11 WLANアーキテクチャのコンポーネントである基本サービスセット（BSS）に接続しようとする際の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 :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

質問: **15**
セキュリティのために WPA2-Personal を使用すると、WLAN 環境にどのような脆弱性が生じますか?
A. 認証局によって生成されたX509証明書を使用します
B. ペアワイズ一時キー（PTK）は各セッションに固有です
C. ペアワイズマスターキー（PMK）はすべてのユーザーによって共有されます
D. WPA 4ウェイハンドシェイクを使用しません
正解: **(**正解を表示します**)**
WPA2-Personalをセキュリティに使用した場合、WLAN環境に導入される脆弱性は、PMK（ペアワイズマスターキー）がPSK（事前共有キー）から派生した鍵であることです。PSKは通信開始前に2者間で共有される鍵で、どちらも固定されています。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

成できます。これは、PSK または PMK が攻撃者によって侵害された場合、それらを使用して PTK で暗号化されたすべてのトラフィックを復号化できることも意味します。PTK (Pairwise Temporal Key) は PMK から派生したキー、ANonce Authenticator Nonce (ANonce) は認証子 (AP などのネットワーク 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、SNonce Supplicant Nonce (SNonce) はサプリカント (STA などのネットワーク リソースにアクセスするデバイス) によって生成される乱数、AA Authenticator Address (AA) は認証子の MAC アドレス、SA Supplicant Address (SA) は疑似乱数関数 (PRF) を使用するサプリカントの MAC アドレスです。PTK は 4 つのサブキーで構成されます: KCK キー確認キー (KCK) はメッセージの整合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 メッセージ整合性コード (MIC) キーが使用されます。
その他のオプションは、以下の理由により弱点ではありません。
* 証明機関によって生成された X 509 証明書を使用します。: WPA2 パーソナルは認証に X 509 証明書も証明機関も使用しないため、このオプションは false です。X 509 証明書と証明機関は、802.1X と EAP を使用する WPA2 エンタープライズ モードで使用されます。EAP (ExtensibleAuthentication Protocol) は、パスワード、証明書、トークン、生体認証などの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、ワイヤレス ネットワークやポイントツーポイント接続で使用され、サプリカント (ネットワークにアクセスするデバイス) と認証サーバー (サプ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 サーバーによるユーザー認証用 RADIUS (Remote Authentication Dial-In User Service) 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的な認証、承認、アカウンティング (AAA) 管理を提供するネットワーク プロトコルです。
* Pairwise Temporal Key （PTK）はセッションごとに固有です :このオプションは無効です。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、通信中に時間や送信パケット数に基づいて定期的にPTKが変更されることを意味します。これにより、リプレイ攻撃を防ぎ、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 :WPA2-Personalは鍵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、このオプションは無効です。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を生成するプロセスです。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することができます。
参考資料: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management
https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf

質問**: 16**
クライアントが WLAN 内のあるアクセス ポイントから別のアクセス ポイントにローミングすると、どのような変化が起こりますか?
A. 802.11 フレームの宛先 MAC アドレスを変更します。
B. 新しいアクセス ポイントの SSID と一致するように SSID を変更します。
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 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。
正解**: (**正解を表示します**)**

クライアントがアクセスポイント間を移動する際には、そのアクセスポイントの宛先MACアドレスを変更する必要があります。
802.11フレームは、接続先の新しいアクセスポイントに合わせて更新されます。SSIDは通常WLAN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サブネット内にいる限りデフォルトゲートウェイも変わりません。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内の宛先MACアドレスの更新が含まれます。

質問: **17**
顧客との会議で、ネットワーク冗長機能VRRPの仕組みを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何ですか？
A. VRRPはメッセージングにBPDUを使用します
B. VRRPはメッセージングにマルチキャストを使用します
C. VRRPはメッセージングにユニキャストを使用します
D. VRRPはメッセージングにブロードキャストを使用します
正解: **(**正解を表示します**)**
仮想ルータ冗長プロトコル（VRRP）は、利用可能なインターネットプロトコル（IP）ルータを参加ホストに自動的に割り当てるネットワークプロトコルです。VRRPは、マスターの選出プロセスと仮想IPアドレスのアドバタイズのために、ルータ間の通信にマルチキャスト経由でメッセージを送信します。

質問: **18**
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は何を示していますか?
A. スイッチから供給されるPoE電力が不十分で、APの両方の無線に電力を供給できません。
B. 無線はメッシュモードで動作しています
C. 無線は 5 GHz 帯域でのみ動作しています。
D. 無線はモニターモードまたはスペクトル解析モードで有効になっています
正解: **D (**コメントを発表する**)**
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は、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。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、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。また、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します。AP はスタンドアロン デバイスにすることも、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。これは、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。モニタ モードは、AP がすべてのチャネルをスキャンして、ワイヤレス 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 がすべてのチャネルをスキャンして、RF 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 ～ 300 GHz 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 コントロールなどの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情報をエンコードすることにより変調できます。RF 波は、減衰、反射、屈折、回折、散乱、干渉、ノイズなどのさまざまな要因の影響を受ける可能性があります。RF 波は、スペクトル アナライザ、電力計、アンテナなどのデバイスを使用して、環境、ノイズ源、チャネル使用率などを測定できます。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、無線での通常のデータ送受信を無効にします。
その他のオプションは、Aruba AP のオレンジ色の無線ステータス LED では示されません。その理由は次のとおりです。
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 :PoEが不足しているため、このオプションはFalseです。Power over Ethernet （PoE）Power over Ethernet （PoE）は、ネットワークデバイスが同じイーサネット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を用意する必要がなくなります。
PoE は IEEE 802.3af および IEEE 802.3at 標準で定義されており、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、給電装置 (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、受電装置 (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 では、無線ステータス LED がオレンジ色の点灯ではなく、電源ステータス LED がオレンジ色の点滅で示されます。電源ステータス LED がオレンジ色の点滅は、AP がスイッチまたはインジェクタから十分な電力を受け取っておらず、正常に動作できないことを意味します。電源ステータス LED が緑色に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け取っており、正常に動作できることを意味します。
無線はメッシュモードで動作しています :このオプションは無効です。Aruba APでは、無線がメッシュモードで動作していることは、オレンジ色の無線ステータスLEDではなく、緑色の無線ステータスLEDの点灯で示されます。緑色の無線ステータスLEDの点灯は、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。メッシュモードとは、APが他のAPと無線で接続し、有線接続を必要とせずにメッシュネットワークを形成できるモードです。
無線は5GHz帯のみで動作しています :このオプションは誤りです。Aruba APでは、無線が5GHz帯のみで動作している場合、無線ステータスLEDはオレンジ色ではなく青色に点灯します。青色の無線ステータスLEDが点灯している場合は、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帯の両方でデータを送受信でき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

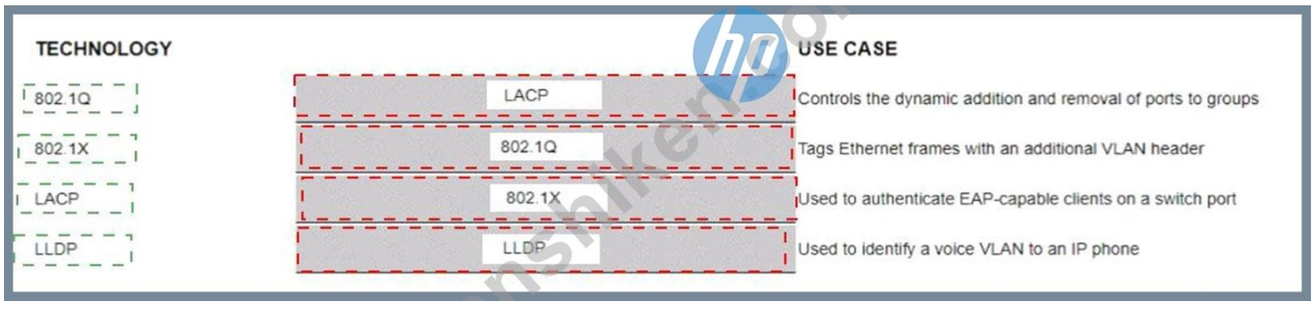
質問: **19**
ArubaOS-CX スイッチへの入力時に過剰なブロードキャスト トラフィックをドロップする必要があります。このタスクに最適なテクノロジーは何ですか。
A. レート制限
B. DWRRキューイング
C. QoSシェーピング
D. 厳格なキューイング
正解: **(正解を表示します)**
ArubaOS-CX スイッチへの入力時に過剰なブロードキャスト トラフィックをドロップするのに最適なテクノロジーは、レート制限です。レート制限は、帯域幅のしきい値または制限を設定することで、ネットワーク管理者がスイッチのポートまたは VLAN に出入りするトラフィックの量を制御できる機能です。レート制限を使用すると、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) を適用し、サービス拒否 (DoS) 攻撃を緩和することができます。レート制限は、インターフェイス コンフィギュレーション モードで storm-control コマンドを使用して、ArubaOS-CX スイッチ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したしきい値を超えると、スイッチは超過したパケットをドロップします。
その他のオプションは、次の理由により、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テクノロジではありません。
* DWRRキューイング :DWRRはDeficit Weighted Round Robin（重み付けラウンドロビン）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、各キューが重みに基づいて公平に帯域幅を確保し、低優先度キューのリソース不足を回避します。DWRRは、入力時に過剰なブロードキャストトラフィックをドロップするのではなく、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、要件に基づいてさまざまな種類のトラフィックに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、出力ポートの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ドロップするのではなく、出力時に送信トラフィックをスムーズにします。
* ストリクトキューイング :ストリクトキューイングは、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度を割り当てる別のキューイングアルゴリズムです。ストリクトキューイングでは、帯域幅要件や重み付けに関係なく、優先度の高いキューが常に優先度の低いキューよりも先に処理されます。ストリクトキューイングは、入力時に過剰なブロードキャストトラフィックをドロップするのではなく、出力時に送信トラフィックをスケジュールします。
参考資料: https://en.wikipedia.org/wiki/Rate_limiting https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/storm-control.htm https://www.arubanetworks.com/techdocs/AOS-

CX_10_08/NOSCG/Content/cx-noscg/qos/dwrr.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/shaping.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/strict.htm

質問: **20**
802のみで動作するIoTデバイスのいくつかのクラスにワイヤレスアクセスを構成する必要があります。
11b. 各クラスには固有のPSKが必要であり、ロール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。これらの要件を満たすオプションはどれですか？
A. 5 GHz および 6 GHz 帯域を使用する各 IoT クラス用の MPSK を使用した単一の SSID
B. 2.4GHz および 5GHz 帯域を使用する各 IoT クラス用の MPSK を使用した単一の SSID
C. 5GHz および 6GHz 帯域を使用し、各 IoT クラスごとに固有の PSK を持つ個別の SSID
D. 2.4GHzおよび5GHz帯域を使用し、各IoTクラスごとに固有のPSKを持つ個別のSSID
正解: **(**正解を表示します**)**
セキュリティ要件が異なる複数のクラスの IoT デバイスにワイヤレス アクセスを構成する場合、単一の SSID と複数の事前共有キー (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、固有の PSK を使用するため、クラスごとに固有のセキュリティ ポリシーを適用できます。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、ネットワーク管理が不必要に複雑になり、SSID のオーバーヘッドが増大します。

質問: **21**
スイッチング テクノロジーを適切なユース ケースに適合させます。

正解:



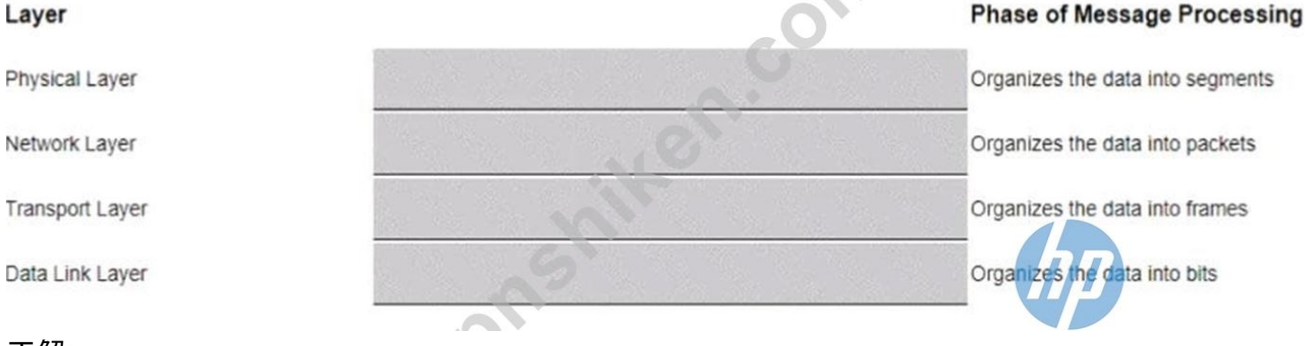
Explanation:
使用例: a) グループへのポートの動的な追加と削除を制御します。テクノロジー: 3) LACP 使用例: b) 追加の VLAN ヘッダーを使用してイーサネット フレームにタグを付けます。テクノロジー: 1) 802.1Q 使用例: c) スイッチ ポートで EAP 対応クライアントを認証するために使用されます。テクノロジー: 2) 802.1X 使用例: d) IP 電話に対して音声 VLAN を識別するために使用されます。テクノロジー: 4) LLDP 次の表は、スイッチング テクノロジーとその使用例をまとめたものです。
テクノロジー
使用事例
1) 802.1Q
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複数のブロードキャストドメインに分割し、セキュリティ、パフォーマンス、および管理性を向上させることができます。802.1Qは、イーサネットフレームにVLAN識別子（VID）を含む追加のVLANヘッダーをタグ付けします。VIDは、フレームがどのVLANに属しているかを示します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標準です。
PNAC を使用すると、ネットワーク管理者はデバイスを認証および承認してから、ネットワーク リソースへのアクセスを許可できます。802.1X は、拡張認証プロトコル (EAP) を使用して、サプリカント (ネットワークへのアクセスを希望するデバイス)、認証装置 (スイッチなどの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 サーバーなどのサプ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
LACPはLink Aggregation Control Protocol（リンクアグリゲーション制御プロトコル）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とも呼ばれます）にまとめる方法を定義しています。LAGは、ネットワーク接続の帯域幅、負荷分散、冗長性を向上させます。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（リンク層検出プロトコル）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通知する方法を定義するIEEE 802.1AB規格の一部です。LLDPはOSI参照モデルの第2層で動作し、TLV（Type-Length-Value）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は、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を識別するために使用できます。
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/リンクアグリゲーション https://en.wikipedia.org/wiki/リンク層検出プロトコル

質問**: 22**
ワイヤレス クライアントのローミングの決定はどこで行われますか?

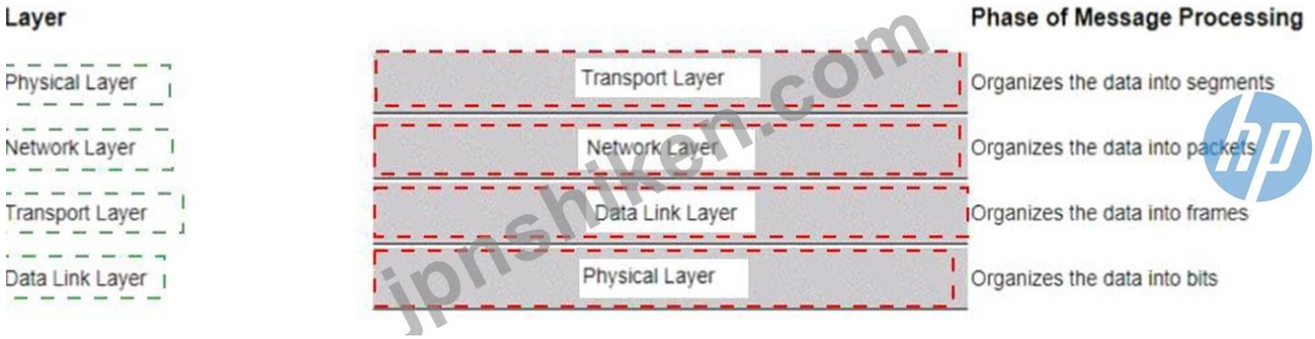
A. クライアントデバイス
B. 仮想コントローラ
C. 発信元APと宛先APによる共同決定
D. アルバセントラル
正解: **(**正解を表示します**)**
ワイヤレス クライアントのローミングの決定は、信号強度、ノイズ レベル、データ レートなどの独自の基準に基づいてクライアント デバイスによって行われます。ネットワークは、ネイバー レポート、負荷分散、バンド ステアリングなどの情報を提供することでクライアントのローミングの決定に影響を与えることができますが、最終的な決定はクライアントが行います。
参考資料: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/wlan- roaming/cl

質問: **23**
ゆっくりオレンジ色に点滅するスタック LED は何を示していますか?
A. 1 つのスイッチにスタッキング障害が発生しています。
B. ポートにスタッキング障害が発生しています。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しています。お待ちください。
正解: **C (**コメントを発表する**)**
スタックLEDがオレンジ色でゆっくり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、スイッチがスタックに参加する準備が整っているか、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。参考：
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/stacking-leds.htm

質問: **24**
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) 層と一致させます。



正解:



Explanation:
レイヤー: 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 レイヤー: 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 レイヤー: 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 レイヤー: 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 OSI モデルは、ネットワーク プロセスを 7 つのレイヤーに分割し、各レイヤーは伝送チェーンの異なるステップを表しています。各レイヤー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ています。ユーザー データは、デバイスが外部に送信するまで、最上位レイヤーから下位レイヤーへと順番に渡されます。最下位レイヤーである物理層は、データを物理メディアを介して送信できるビットに変換します。2 番目のレイヤーであるデータ リンク層は、ビットを 2 つのノード間のリンクを介して送信できるフレームに編成します。3 番目のレイヤー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、パケットをセグメントに編成し、2つのエンドポイント間で信頼性が高くエラーのない通信を実現します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

質問: **25**
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。正常な接続を確実にするためにどの RADIUS メッセージを確認する必要がありますか?
A. 承認済み
B. アクセス許可
C. 成功
D. 認証済み
正解: **B** (コメントを発表する)
説明
802.1X接続を成功させ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サーバがサプリカント（ネットワークへのアクセスを希望するデバイス）を認証・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ます。これらの属性は、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）がサプリカントのトラフィックをどのように処理すべきかを指定します。
その他のオプションは、次の理由により RADIUS メッセージではありません。
承認済み: これは RADIUS メッセージではありませんが、認証と承認が成功した後、認証子のポートがサプリカントからのトラフィックを渡すことができ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）がパスワード、証明書、トークン、生体認証などの複数の認証方法をサポートする認証フレームワークであることを示すステータスです。EAPは、ワイヤレスネットワークやポイントツーポイント接続で使用され、サプリカント（ネットワークへのアクセスを要求するデバイス）と認証サーバー（サプリカントの資格情報を検証するデバイス）間の安全な認証を提供します。サプリカントと認証サーバー間の交換が正常に完了しました。
認証済み: これは RADIUS メッセージではありませんが、サプリカントの認証が成功した後、認証子のポートが認証サーバーから EAP 成功メッセージを受信したことを示す状態です。
参考資料: 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#ポートベースのネットワークアクセス制御
https://en.wikipedia.org/wiki/拡張認証プロトコル#EAP_exchange

質問: **26**
ネットワーク技術者は、Aruba 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 プロセスを開始するときに、問題を表示および確認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
正解: **A (**コメントを発表する**)**
アラートとイベント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あらゆる種類のアラートとイベントが表示されます。「Config」アイコンを使用して、さまざまなアラートカテゴリと重大度1に応じたアラートと通知を設定できます。また、リストビューとサマリービュー2でアラートとイベントを表示することもできます。参考 :1
https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/configuring-alerts.htm 2
https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/viewing-alerts.htm

質問: **27**
顧客は、Windows 10 クライアントを使用するユーザーに対して承認ポリシーを作成する必要があり、1 つの Radius セッション内でデバイスとユーザーの資格情報の両方を Tor で承認する必要があります。
要件に対する正しい解決策は何でしょうか?
A. EAP-TTLS 対応 ClearPass 6.9
B. ClearPass 6.9（EAP-TLS 対応）
C. ClearPass 6.9（PEAP 対応）
D. ClearPass 6.9 と EAP-TEAP
正解: **D (**コメントを発表する**)**

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：https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM_UserGuide/EAP-TEAP/EAP-TEAP.htm
1つのRadiusセッション内でデバイスとユーザーの両方の認証情報を認証する必要がある場合、適切なソリューションは、EAP-TEAP（EAP-Tunneled Extensible Authentication Protocol）を搭載したClearPass 6.9です。EAP-TEAPは、クライアントとサーバー間に安全な通信チャネルを作成し、単一セッション内で複数の認証トランザクションの送信を可能にするトンネリングプロトコルです。この機能は、ネットワークリソースへのアクセスを許可する前にユーザーとデバイスの両方の認証情報を検証する必要があるシナリオで特に役立ちます。これにより、セキュリティがさらに強化され、ユーザーとデバイスの両方がネットワークへのアクセスを許可されていることが保証されます。

質問: **28**
VSFスタックで6300Mスイッチのペアを使用しています。スイッチには48個のSmartRate 5Gポート、2個のSFP28ポート、2個のSFP56ポートがあり、両方のSFP56ポートはスタッキングに使用されます。
可能な限り最大の帯域幅を使用して、別の同一スタックへの LACP 接続を提供する必要があります。
何を設定すればよいでしょうか?
A. 各スイッチの2つのSFP28ポートと6つのSR5ポートを使用する16メンバーのLAG
B. 各スイッチの4つのSR5ポートを使用する8メンバーLAG
C. 各スイッチの2つのSFP28ポートと2つのSR5ポートを使用する8メンバーLAG
D. 各スイッチの2つのSFP28ポートを使用する4メンバーLAG
正解: **A (**コメントを発表する**)**
LACP接続で利用可能な帯域幅を最大限に利用するには、データ転送に使用可能なすべてのポートを使用してリンクアグリゲーショングループ（LAG）を構成する必要があります。SFP56ポートはスタッキングに使用されるため、次善策として、各スイッチの2つのSFP28ポートと可能な限り多くのSmartRate 5G（SR5）ポートを使用することが挙げられます。これにより、各スイッチの2つのSFP28ポートと6つのSR5ポートがLAGに寄与し、16メンバーのLAGを構築できます。

質問: **29**
WPA3-Personal では、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 Pairwise Master Key (PMK) を生成するために、ソースとして何を使用するのでしょうか?
A. セッション固有の情報（MACとノンス）
B. 無線暗号化（OWE）
C. 同時同等認証 (SAE)
D. キー暗号化キー (KEK)
正解: **C (**コメントを発表する**)**
WPA3-Personalは、WPA2で使用されている事前共有キー（PSK）方式のより安全な代替方式である同時同等認証（SAE）を使用することで、ワイヤレスネットワークのセキュリティを強化します。SAEは初期キー交換を強化し、オフライン辞書攻撃に対する保護を強化します。また、各セッションに、クライアントとアクセスポイン

ト間のやり取りから生成された固有のペアワイズマスターキー（PMK）MACアドレスやナンスなどのセッション固有の情報を含む）が確実に保持されるようにします。

質問: **30**
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. レート制限
B. DWRRキューイング
C. QoSシェーピング
D. 厳格なキューイング
正解: **(**正解を表示します**)**
説明
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のに最適なテクノロジーは、レート制限です。レート制限は、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 に出入りするトラフィックの量を制御できる機能です。レート制限を使用すると、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) を適用し、サービス拒否 (DoS) 攻撃を緩和することができます。レート制限は、インターフェイス コンフィギュレーション 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したしきい値を超えると、スイッチは超過したパケットをドロップします。
その他のオプションは、次の理由により、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テクノロジではありません。
DWRRキューイング :DWRRはDeficit Weighted Round Robin（重み付けラウンドロビン）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、各キューが重みに基づいて公平に帯域幅を確保し、低優先度キューのリソース不足を回避します。DWRRは、入力時に過剰なブロードキャストトラフィックをドロップするのではなく、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、要件に基づいてさまざまな種類のトラフィックに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、出力ポートの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ドロップするのではなく、出力時に送信トラフィックをスムーズにします。
ストリクトキューイング :ストリクトキューイングは、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度を割り当てる別のキューイングアルゴリズムです。ストリクトキューイングでは、帯域幅要件や重み付けに関係なく、優先度の高いキューが常に優先度の低いキューよりも先に処理されます。ストリクトキューイングは、入力時に過剰なブロードキャストトラフィックをドロップするのではなく、出力時に送信トラフィックをスケジュールします。
参考資料: https://en.wikipedia.org/wiki/Rate_limiting

https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/storm-control.htm
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/dwrr.htm
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/shaping.htm
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/qos/strict.htm

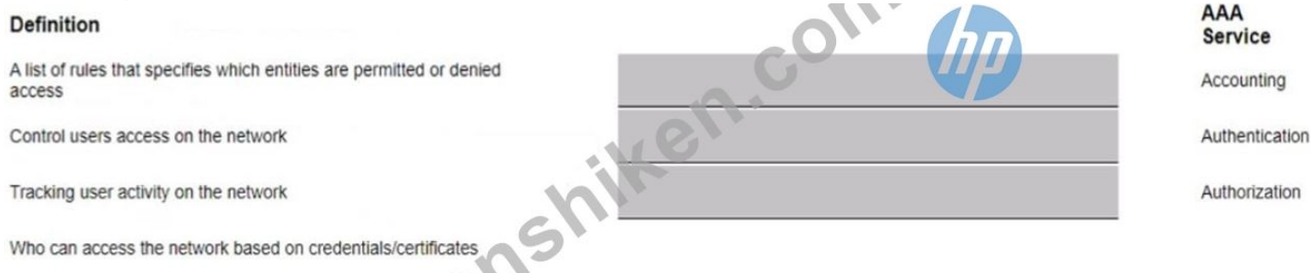
質問: **31**
推奨される VSF トポロジは何ですか? (2 つ選択してください。)
A. スター
B. デイジーチェーンとMAD
C. フルメッシュ
D. フルメッシュ＋MAD
E. リング
正解: **(**正解を表示します**)**
限定 :デイジーチェーンとMAD、そしてリングは、Arubaスイッチに推奨されるVSFトポロジです。これらは、VSFスタックに高可用性と冗長性を提供します。MAD（Multiple Active Detection）は、VSFスタックにおけるスプリットブレインシナリオを検出し、解決するためのメカニズムです。参考：
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-D6EF042E-EEEF-49F7-B67E-4CAC41CCB24D.html

質問: **32**
配布ラックあたり 200 ～ 380 台のクライアント、プリンター、AP にコスト効率よく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. アルバ CX 6400
B. アルバ CX 6200
C. アルバ CX 6300
D. アルバ CX 6000
正解: **C (**コメントを発表する**)**
Aruba CX 6300シリーズは、中密度から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。
CX 6300は、200～380台のクライアント、プリンター、APに対応し、高速アップリンク、クラス4 PoE（PoE+）のサポート、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、信頼性の高い接続と一貫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、CX 6400のように過剰仕様で高価であったり、CX 6200のように必要なポート密度を提供しなかったり、CX 6000のように製品ラインに存在しない場合があります。

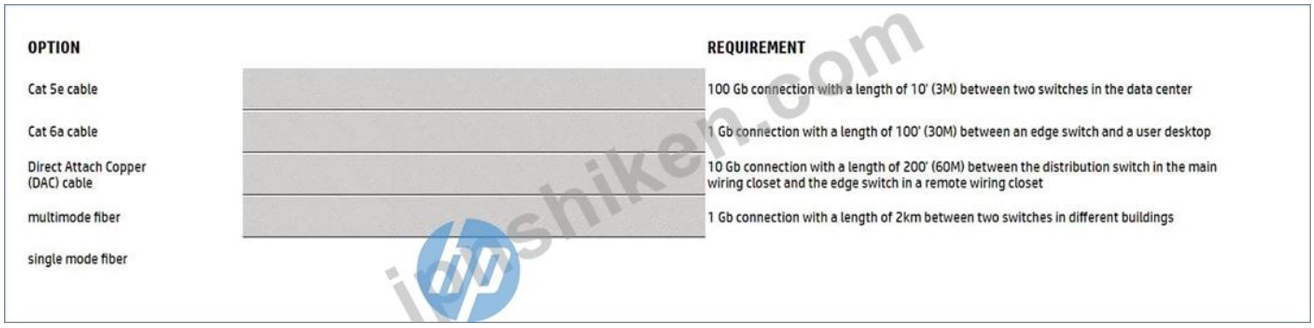
質問: **33**
Aruba AP でライブ ファームウェア アップグレードを実行する場合、クライアントへの影響を最小限に抑えながら、RF 近隣データに基づいてすべての AP を分割するテクノロジはどれですか。
A. アルバクライアントマッチ
B. Aruba Aiの洞察
C. アルバ エアマッチ
D. アルバ ESP
正解: **(**正解を表示します**)**
Aruba AirMatchは、RF無線周波数を最適化する機能です。RFとは、電波伝搬に関連する電磁スペクトル内の任意の周波数です。アンテナにRF電流が供給されると、空間を伝搬できる電磁場が生成されます。機械学習アルゴリズムと履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をパーティション化し、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。参考資料 :https://www.arubanetworks.com/assets/ds/DS_AirMatch。pdfhttps://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/arm/エアマッチ.htm

質問: **34**
各 AAA サービスを正しい定義と一致させます (一致は複数回使用される場合やまったく使用されない場合があります)

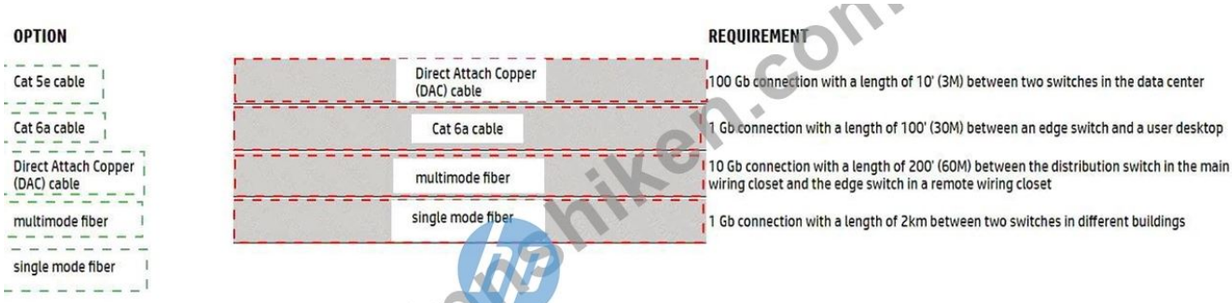


正解:

質問: **35**
各要件に応じて、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ます。 すべての長さは、パッチ ケーブル、サービス ループなど（使用されている場合）を含むケーブルの合計長さを示します。）



正解:



* 100 Gbps、3M: ダイレクトアタッチ銅線
* 1 Gbps、30M: カテゴリー Ga
* 10 Gbps、60M :マルチモードファイバー
* 1 Gbps、2km :シングルモード光ファイバー

質問: **36**
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]」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
正解: **B (**コメントを発表する**)**
スタティックルートとは、ルータまたはスイッチ上で手動で設定されるルートであり、管理者によって変更されない限り変更されません。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、またはダイナミックルーティングプロトコルでは到達できない特定の宛先へのトラフィックの到達方法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「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 であり、静的ルートの一般的な値であるため、静的ルートです。
参考文献:

https://en.wikipedia.org/wiki/静的ルーティング
https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.h

質問: **37**
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 ヘッダーに渡されるものはどれですか?
A. チェックサム
B. 生存時間
C. プロトコル
D. 宛先IP
正解: **B (**コメントを発表する**)**
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までに通過できるホップの最大数を示す 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によって 1 ずつ減算されます。TTL が 0 に達すると、パケットは破棄され、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、ソース 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メッセージは送信元デバイスに送り返されます。TTLは、ループしたネットワークトポロジ内でパケットが無期限に循環するのを防ぐため、レイヤ3ルートループを軽減するために使用されます。また、TTLはネットワークリソースを節約し、ループしたパケットによる輻輳を回避するのにも役立ちます。
その他のオプションは、次の理由により、レイヤー 3 IPv4 パケット ヘッダー内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16ビットのフィールドで、IPヘッダーの整合性を検証するために使用されます。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ルートループを軽減することはできません。
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 伝送制御プロトコル (TCP) などの、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。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、ウィンドウ処理を使用してデータ配信とフロー制御を保証します。また、TCP は、再送、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を処理します。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。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形式を持ちます。 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、

質問: **38**
病院では、患者データの診断と文書化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 を超えるポートを備えた配布ラックを備えたこの大規模病院に最適なアクセス スイッチは何ですか。
A. CX 6300
B. OCX 6400
C. OCX 6200
D. OCX 6100
正解: **(**正解を表示します**)**
単一の VSF スタックに 400 を超えるポートを備えた配布ラックを備えた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、次のような利点があります。
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。これにより、1つのVSFスタックで400ポート以上という要件を満たします。
CX 6300は、最大960Gbpsのスイッチング容量と最大714Mppsの転送速度を備えた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おける高スループットと低レイテンシの要件を満たします。
CX 6300は、ダイナミック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といった高度な機能をサポートしています。これらの機能は、デバイスやユーザーの種類に応じて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強化します。
CX 6300は、ネットワーク管理と自動化を簡素化するネットワーク構成および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、ネットワーク構成と保守に伴う複雑さと人的ミスが軽減されます。
その他のオプションは、次の理由により理想的ではありません。
OCX 6400 :このスイッチはデータセンター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、ネットワークのセキュリティと柔軟性の向上に役立つダイナミックセグメンテーションやポリシーベースルーティングもサポートしていません。
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。
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。

質問: **39**
同じチャネル幅を持つ 5 GHz チャネルと 6 GHz チャネルを比較する場合、正しい記述はどれですか。

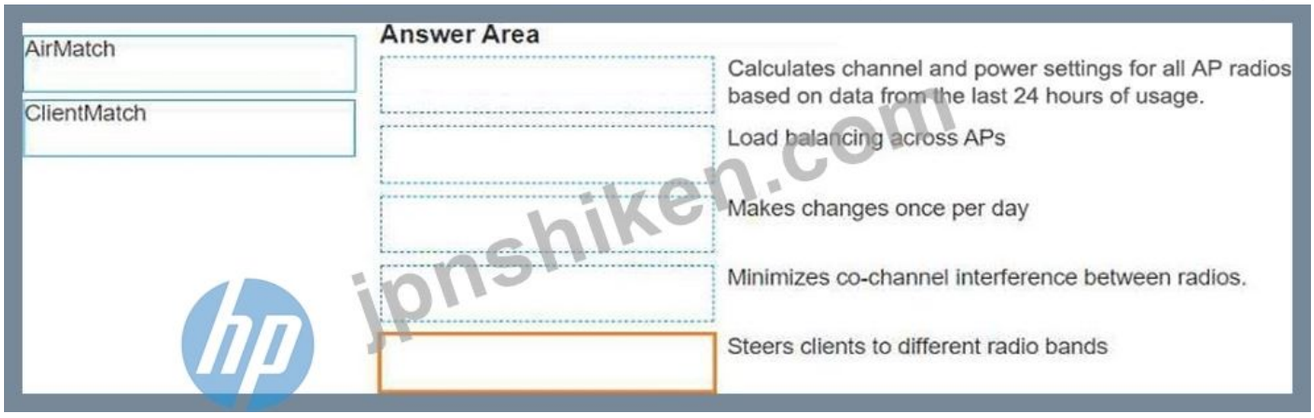
A. 5GHzチャネルは6GHzチャネルと同じ距離を移動しますが、クライアントに提供するスループットは異なります。
B. 5GHzチャネルは6GHzチャネルと比較して異なる距離を移動し、クライアントに異なるスループットを提供します。
C. 5GHzチャネルは6GHzチャネルと同じ距離を移動し、同じスループットをクライアントに提供します。
D. 5GHzチャネルは6GHzチャネルと比較して異なる距離を移動し、クライアントに同じスループットを提供します。
正解: **(**正解を表示します**)**
5GHzと6GHzのチャネルはどちらも同等のスループットを提供できますが、6GHz帯は周波数が高いため、信号到達範囲が5GHzの信号に比べて短く、障害物による減衰も大きくなります。そのため、5GHzチャネルは一般的に6GHzチャネルよりも長距離を伝送できますが、接続されたクライアントに対してはどちらも高いデータレートをサポートできます。

質問: **40**
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. ペアワイズ一時鍵 (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（ノンス）
正解: **(**正解を表示します**)**
説明
データの暗号化や復号化に使用される WPA キー階層の部分は、Pairwise Temporal Key (PTK) です。
PTK は、PMK から派生したキーです。PMK (Pairwise Master Key) は、PSK から派生したキーです。PSK (Pre-shared Key) は、通信を開始する前に 2 者間で共有されるキーです。ANonce Authenticator Nonce (ANonce) は、認証装置 (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、たとえば AP) によって生成される乱数です。SNonce Supplicant Nonce (SNonce) は、サプリカント (ネットワーク リソースにアクセスするデバイス、たとえば STA) によって生成される乱数です。AA Authenticator Address (AA) は、認証装置の MAC アドレスです。SA Supplicant Address (SA) は、疑似乱数関数 (PRF) を使用するサプリカントの MAC アドレスです。PTK は、次の 4 つのサブキーで構成されます。
KCK キー確認キー（KCK）はメッセージの整合性チェックに使用されます。
KEKキー暗号化キー（KEK）は暗号化キーの配布に使用されます
TKー時鍵（TK）はデータの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 Temporal Key (TK) です。TK は Pairwise Transient Key (PTK) とも呼ばれます。TK は、通信中に時間または送信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、次の理由により 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 を導出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、メッセージの整合性チェックに使用されます。

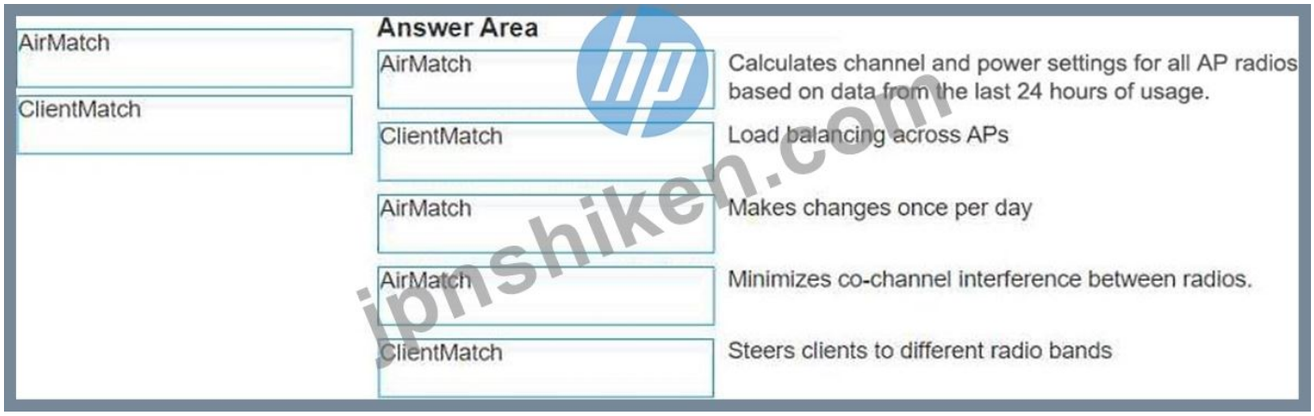
Nonce: Nonce は WPA キー階層の一部ではなく、PTK を導出するための入力です。
参考資料: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management
https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf

質問: **41**
UXI の 2 つの利点は何ですか? (2 つ選択してください)
A. UXIはインターネット接続なしでも使用できます
B. UXIは遠隔地の最適なWiFiチャンネルを計算するのに役立ちます
C. UXIはクライアント/ユーザーのように動作します
D. UXI 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。
正解: **C,E (**コメントを発表する**)**
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指標を測定できます。参考：
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、ユーザー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。

質問: **42**
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。(一致は複数回使用できます。)



正解:



質問: **43**
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アドレスを一致させます
B. クライアント側での設定は必要ありません
C. MAC許可リストは時間の経過とともに簡単に維持されます
D. MAC識別子は偽装が難しい
正解: **B** (コメントを発表する)
説明
レイヤー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、スイッチは割り当てられたロール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、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-ove

質問: **44**
ネットワーク技術者は、Aruba 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 プロセスを開始するときに、問題を表示および確認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
正解: **A** (コメントを発表する)
説明
「アラートとイベント」ダッシュボードには、デバイスのプロビジョニング、構成、ユーザー管理に関連するイベントで生成されたあらゆる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大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、リストビューとサマリービュー2でも表示できます。参考資料：

https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/configuring-alerts.htm 2
https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/viewing-alerts.htm

質問: **45**
複数の 20 MHz 幅の 802.11 チャネルを結合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. 高利得全方向性アンテナを利用する
正解: **(**正解を表示します**)**
複数の20MHz幅の802.11チャネルを結合することは、より広い帯域幅のチャネルを作成し、より高いデータレートの伝送をサポートする技術です。これにより、より多くのスペクトルリソースを使用し、干渉を低減することで、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。参考文献：
https://ieeexplore.ieee.org/document/9288995 複数の20MHz幅の802.11チャネルを結合することは、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チャネルをより広いチャネル（例：40MHz）に結合することで、より広い帯域幅のチャネル（例：40MHz）を作成できます。
40MHz、80MHz、あるいは160MHzといった周波数帯域を広くすることで、データ伝送容量が増加し、結果として無線接続全体のスループットが向上します。この方法は、高帯域幅の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。

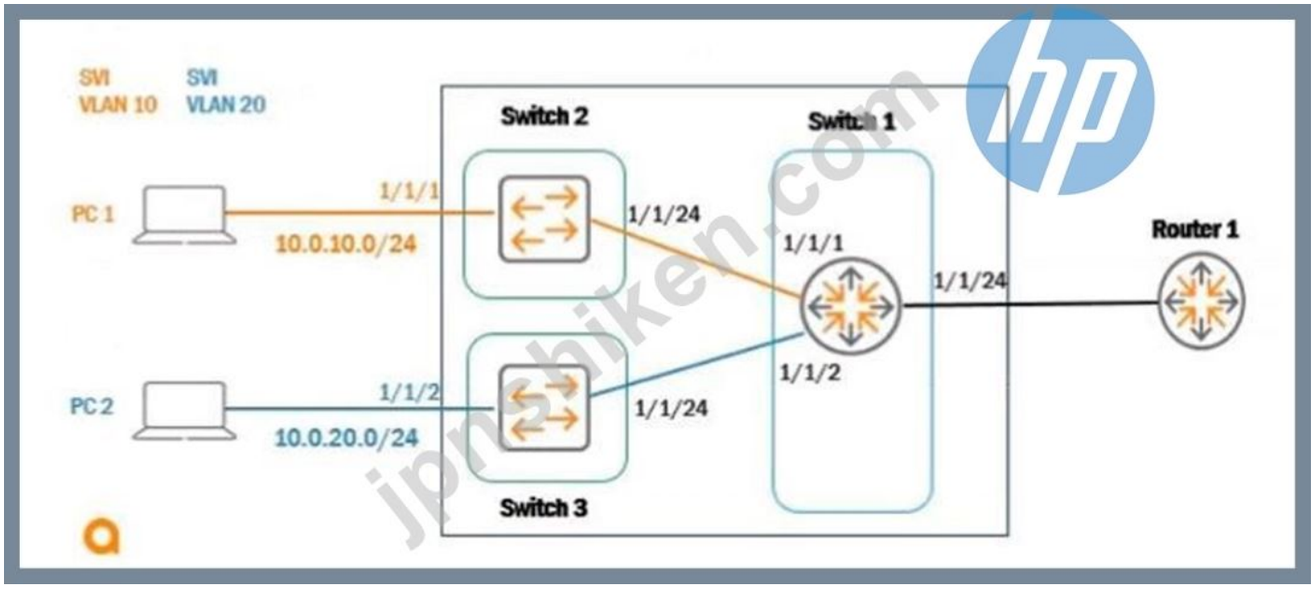
質問: **46**
AP からの信号が物体を通過する際に吸収されて弱まるとどうなりますか?
A. APはボンディングチャネルを使用してクライアントへの遅延を低減します
B. 信号対雑音比（SNR）が増加する
C. 信号対雑音比（SNR）が低下する
D. Aruba Centralはクライアントを近隣のAPに動的に移動します
正解: **(**正解を表示します**)**
信号対雑音比（SNR）は、目的の信号のレベルと背景雑音のレベルを比較する指標です。SNRは信号電力と雑音電力の比として定義され、通常はデシベル（dB）で表されます。SNRが高いということは、信号が明瞭で検出や解釈が容易であることを意味します。一方、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不明瞭になっており、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1。APアクセスポイント（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）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。ノイズ電力は、同じ周波数帯域で動作する他のAPやデバイスなど、他の発生源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、正解は、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が低下するということです。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_and_Wireless_Signal_Strength

質問: **47**
スパニング ツリー (STP) 設定を備えた 2 つの独立した ArubaOS-CX 6300 スイッチが、ポート 1/1/1 と 1/1/2 間の 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」および「no routing」コマンドがあります。
STP はこれらのポート上のトラフィックをどのように転送または破棄しますか?
A. MACアドレスが低いスイッチは両方のポートで転送し、MACアドレスが高いスイッチは両方のポートで転送します。
B. MACアドレスの低いスイッチは両方のポートで転送し、MACアドレスの高いスイッチは1つのポートで破棄します。
C. MACアドレスの低いスイッチは1つのポートで破棄し、MACアドレスの高いスイッチは両方のポートで転送します。
D. MACアドレスの低いスイッチは1つのポートで破棄し、MACアドレスの高いスイッチは1つのポートで破棄します。
正解: **D** (コメントを発表する)
STP スパニング ツリー プロトコルの方法。STP は、スイッチまたはブリッジ間の冗長パスがブロードキャスト ストーム、複数のフレームの送信、および MAC テーブルの不安定性を引き起こすループを作成することを防ぐことで、ブリッジされたイーサネット ローカル エリア ネットワークで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、2つのスイッチのブリッジID（プライオリティ値とMACアドレスで構成される）に基づいて、ルートブリッジを選択します。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、すべてのポートでトラフィックを転送します。
- STPは、両方のスイッチの各ポートに、ポートID（優先度とポート番号から構成される）に基づいて役割と状態を割り当てます。ポートIDが低いポートが指定ポートとなり、トラフィックを転送します。一方、ポートIDが高い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、両スイッチ間には2つのパスが存在する可能性があり、ループが発生します。このループを防ぐため、STPは各スイッチのポートの1つでトラフィックを破棄することで、これらのパスの1つをブロックします。

- 両方のスイッチのプライオリティ値が同じ（デフォルトは32768）であると仮定すると、MACアドレスが小さい方のスイッチのブリッジ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。
- 両ポートの優先度が同じ値（デフォルトは128）であると仮定すると、ポート1/1/1はポート番号が小さいため、両スイッチともポート1/1/2よりも低いポートIDを持ちます。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、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 アドレスが低いスイッチは 1 つのポート (ポート 1/1/2) のトラフィックを破棄し、MAC アドレスが高いスイッチも 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。
参考文献: 3 https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

質問: **48**
ゲートウェイ 172.16.1.1 経由でクラス c ネットワーク 10.2.10.0 に静的ルートを追加する正しいコマンドは何ですか?
A. IPルート 10.2.10.0/24 172.16.1.1
B. ip route 10.2.10.0.255.255.255.0 172.16.1.1 説明 アルバ
C. IPルート 10.2.10.0/24.172.16.11
D. ipルートスタティック 10.2 10.0.255.255.255.0 172.16.1.1
正解: **(**正解を表示します**)**
ゲートウェイ 172.16.1.1 経由でクラス c ネットワーク 10.2.10.0 にスタティック ルートを追加する正しいコマンドは、ip-route 10.2.10.0/24 172.16.1.1 です。このコマンドは、スイッチからその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 (10.2.10.0) とプレフィックス長 (/24)、およびネクストホップ アドレス (172.16.1.1) を指定します。その他のコマンドは、スタティック ルートを追加するための構文またはパラメータが間違っています。参考: https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm Aruba スイッチなどのネットワーク デバイスにスタティック ルートを追加する場合、正しいコマンド形式には通常、宛先ネットワーク、サブネット マスク (またはマスクの CIDR 表記)、およびネクストホップ IP アドレスが含まれます。コマンド「ip route 10.2.10.0/24 172.16.1.1」は、宛先ネットワーク「10.2.10.0」をクラスCサブネットマスク「/24」で正しく指定し、ネクストホップIPアドレス「172.16.1.1」をIPアドレスとして指定しています。このコマンドは簡潔で、ArubaOS-CXを含む多くのネットワークオペレーティングシステムでスタティックルートを追加するための標準構文に準拠しています。その他のオプションは、構文が誤っているか、スタティックルートを追加するための標準コマンドには通常含まれない不要なパラメータが含まれています。

質問: **49**



指定されたトポロジに基づいて、ルータ 1 で LLDP が有効になっている場合に、スイッチ 1 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の Aruba スイッチの要件は何ですか。

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 の有効化

C. int 1/1/24、lldp受信

D. int 1/1/24、CDPなし

正解: **(**正解を表示します**)**

説明

LLDP リンク層検出プロトコル。LLDP は、ネットワークデバイスがローカルエリアネットワーク上で自身の ID、機能、およびネイバーをアドバタイズするために使用する、ベンダー中立のリンク層プロトコルです。Aruba スイッチではデフォルトで有効になっていますが、no lldp コマンドを使用してポートごとに無効にすることができます。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には、そのポートのインターフェイス コンフィギュレーション モードに入り、lldp receive コマンドを使用する必要があります。

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

質問: **50**

VSFスタックで6300Mスイッチのペアを使用しています。スイッチには48個のSmartRate 5Gポート、2個のSFP28ポート、2個のSFP56ポートがあり、両方のSFP56ポートはスタッキングに使用されます。

利用可能な帯域幅を最大限に利用して、別の同一スタックにLACP接続を提供する必要があります。どのような設定が必要ですか？

A. 各スイッチの2つのSFP28ポートと6つのSR5ポートを使用する16メンバーのLAG

B. 各スイッチの4つのSR5ポートを使用する8メンバーLAG

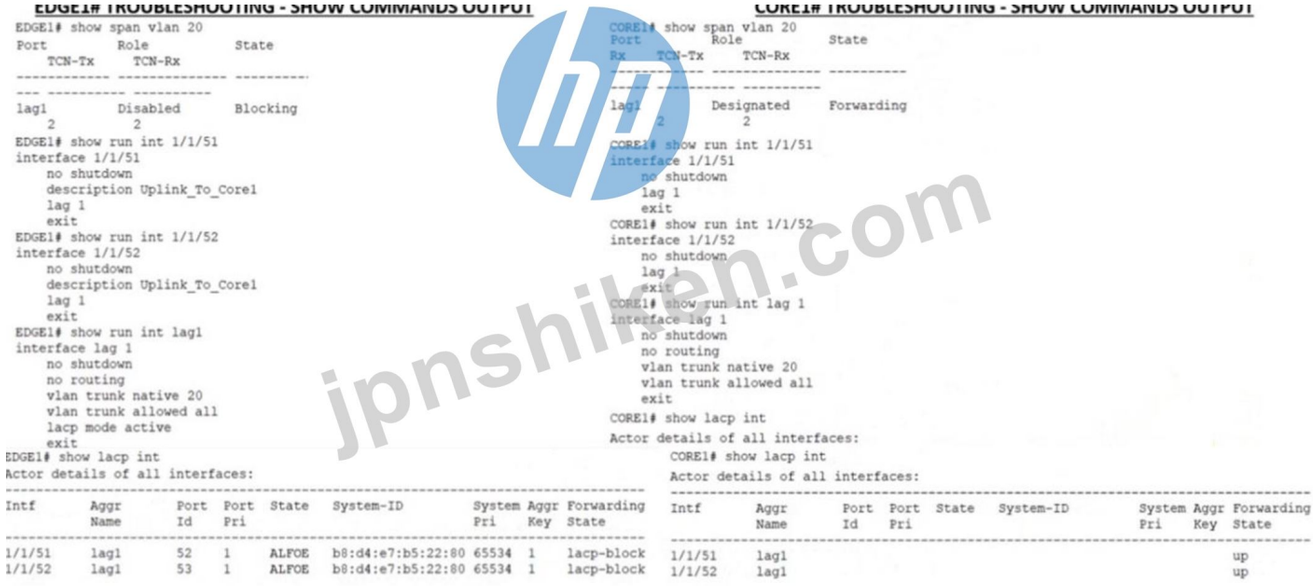
C. 各スイッチの2つのSFP28ポートと2つのSR5ポートを使用する8メンバーLAG

D. 各スイッチの2つのSFP28ポートを使用する4メンバーLAG

正解: **(**正解を表示します**)**

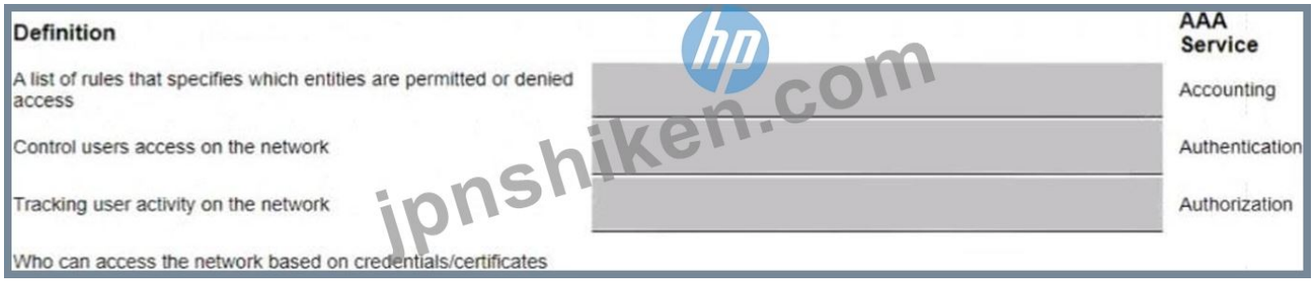
LACP接続で利用可能な帯域幅を最大限に利用するには、データ転送に使用可能なすべてのポートを使用してリンクアグリゲーショングループ（LAG）を構成する必要があります。SFP56ポートはスタッキングに使用されるため、次善策として、各スイッチの2つのSFP28ポートと可能な限り多くのSmartRate 5G（SR5）ポートを使用することが挙げられます。これにより、各スイッチの2つのSFP28ポートと6つのSR5ポートがLAGに寄与し、16メンバーのLAGを構築できます。

質問: **51**
スイッチEDGE1と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。



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に接続できなくなっています
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. コアアップリンクにLACPが設定されていません
正解: **(**正解を表示します**)**
LACPは、複数の物理リンクを単一の論理リンクに集約することで帯域幅と冗長性を向上させるプロトコルです。LACPが適切に機能するには、リンクの両端で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、リンクが起動しません。参考：
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/lacp.htm

質問: **52**
各 AAA サービスを正しい定義と一致させます (一致は複数回使用される場合やまったく使用されない場合があります)



正解:

Explanation:
各 AAA (認証、承認、アカウンティング) サービスとその定義の正しい組み合わせは次のとおりです。
アカウンティング: ネットワーク上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。承認: アクセスを許可または拒否するエンティティを指定するルールのリスト。アカウンティングはユーザー 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、承認は認証されたユーザーがネットワーク上で実行できる操作を決定します。

質問: **53**
IP カメラ、AP、その他の PoE デバイスを導入するときに、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すか?
A. スイッチモジュールでQuick 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
正解: **(**正解を表示します**)**
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、デバイスのタイプと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、デバイスのプロファイルに基づいて、VLAN、ACL、QoSなどの他の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-overview/プロファイリング.htm

質問: **54**
Aruba アクセス ポイントの構成に関して正しい記述は次のうちどれですか。

2つ選択してください）
A. Aruba AP は、Instant モードではコントローラなしで機能できます。
B. すべての Aruba AP が機能するには、Aruba Central に物理的に接続されている必要があります。
C. Aruba AP はクラスタリング テクノロジーをサポートしていません。
D. Aruba AP は、すぐに使用できるリモート AP (RAP) 機能をサポートします。
正解: **(**正解を表示します**)**

質問: **55**
6GHz帯の主な特徴は何ですか？
A. 6 GHz WLAN では、物体によって吸収される RF 信号が少なくなります。
B. 北米では、6 GHz 帯域では 5 GHz 帯域の 40 MHz チャネルよりも多くの 80 MHz チャネルが提供されます。
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ます。
正解: **(**正解を表示します**)**
提示された選択肢の中で6GHz帯の最も確かな特徴は、北米では6GHz帯の80MHzチャネルが5GHz帯の40MHzチャネルよりも多く利用可能であるということです。この特徴により、Wi-Fi 6Eをサポートする無線デバイスは、より多くの周波数帯域を利用でき、干渉が少なく、スループットが向上します。Wi-Fi Enhanced（Wi-Fi 6E）は、Wi-Fi 6（802.11ax）規格の拡張版であり、既存の6GHz帯以下の周波数帯域に加えて、新たに利用可能になった6GHz付近の無認可周波数帯域でも動作します。この特徴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つのチャネル幅（20MHz、40MHz、80MHz）それぞれに最大7つの重複しないチャネルが利用可能です。つまり、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21個になります。
比較すると、北米では、既存の無認可帯域（2400～2483MHzおよび5150～5825MHz）全体において、2つのチャネル幅（20MHzおよび40MHz）それぞれに、重複しないチャネルがわずか9つしかありません。つまり、Wi-Fiデバイスが利用できる重複しないチャネルは合計で最大9つしかありません。
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利用できる重複しないチャネルの数が、その下の既存のスペクトルの 2 倍以上になります。
具体的には、80 MHz 幅 (7 つ) では、それ以下の既存のスペクトルの 40 MHz 幅 (3 つ) よりも 2 倍以上の非重複チャネルが利用可能です。
他のオプションは、次の理由により正しくありません。
6GHz帯WLANでは物体によるRF信号の吸収が少ない :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、低周波信号よりも物体による吸収が大きい傾向があるためです。減衰とは、長距離伝送時、または物体や媒体を介した伝送時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、6GHz帯WLANのRF信号は、低周波帯WLANのRF信号よりも物体による吸収が大きくなります。
6 GHz帯は既存の帯域と完全な下位互換性があります。Wi-Fiデバイスは、6 GHz帯を中心とした新しいスペクトルで動作するためにWi-Fi 6E規格をサポートする必要があるため、このオプションは無効です。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します。

低電力デバイスは屋内および屋外での使用が許可されています: 低電力屋内デバイス (LPI) は、一定の電力制限および登録要件の下で屋内での使用のみが許可されているため、このオプションは false です。LPI デバイスの屋外での使用は、FCC (米国連邦通信委員会 (FCC) は米国政府の独立機関であり、米国全土におけるラジオ、テレビ、有線、衛星、ケーブルによる通信を規制しています) などの規制当局によって禁止されています。ただし、超低電力デバイス (VLP) の屋外での使用は、一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。

質問: **56**
ディストリビューションおよびレイヤ3サービスに使用する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VLAN/サブネットを複数作成し、複数のアクセススタックで利用します。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ースを正しく設定するにはどうすればよいですか？
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 スタックのサブネットに SVI を作成します。
正解: **(**正解を表示します**)**
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ー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ース）を作成することです。スイッチ仮想インターフェース（SVI）は、VLANを表すスイッチ上の仮想インターフェースであり、そのVLANにレイヤ3ルーティング機能を提供します。SVIは、VLAN間ルーティングの有効化、VLAN内のホストへのゲートウェイアドレスの提供、VLANへのACLまたはQoSポリシーの適用などに使用されます。
SVIは、物理ルーティングインターフェースに比べて、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の利点があります。SVIは通常、VLAN ID（例vlan 10）およびVLANのサブネット内のIPアドレスが割り当てられています。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設定できます。SVIは、6300Mスタックのサブネットで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を作成すると、スイッチはその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。また、6300Mスタックのサブネットに 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ースとケーブルの数が少なくなり、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、次の理由により、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構成する正しい方法ではありません。
* 6300Mスタック上のサブネット内に、各ダウンストリームスイッチ用の物理ルーティング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内に、各ダウンストリームスイッチ用

の物理ルーティング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、インターフェースリソースが消費され、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内に、各ダウンストリームスイッチ用の物理ルーティングインターフェースを作成すると、インターフェー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 :このオプションは正しくありません。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自身の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間ルーティングが有効になりません。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 スイッチは引き続き自身の 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 スペースが浪費され、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-noscg/l3-routing/l3-routing-overview.htm https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-config.htm

質問**: 57**
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どうなりますか?
A. AP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はクライアントを近隣のAPに動的に移動します
正解**: C (**コメントを発表する**)**
信号対雑音比 （SNR）は、目的の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、通常はデシベル （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。一方、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不明瞭になっており、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1。APアクセスポイント （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）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。ノイズ電力は、同じ周波数帯域で動作する他のAPやデバイスなど、他の発生源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、正解は、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が低下するということです。参考: 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_and_Wireless_Signal_Strength

質問: **58**
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. ペアワイズ一時鍵 (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（ノンス）
正解: **(正解を表示します)**
データの暗号化や復号化に使用される WPA キー階層の部分は、Pairwise Temporal Key (PTK) です。
PTK は、PMK から派生したキーです。PMK (Pairwise Master Key) は、PSK から派生したキーです。PSK (Pre-shared Key) は、通信を開始する前に 2 者間で共有されるキーです。ANonce Authenticator Nonce (ANonce) は、認証装置 (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、たとえば AP) によって生成される乱数です。SNonce Supplicant Nonce (SNonce) は、サプリカント (ネットワーク リソースにアクセスするデバイス、たとえば STA) によって生成される乱数です。AA Authenticator Address (AA) は、認証装置の MAC アドレスです。SA Supplicant Address (SA) は、疑似乱数関数 (PRF) を使用するサプリカントの MAC アドレスです。PTK は、次の 4 つのサブキーで構成されます。
* KCK キー確認キー（KCK）はメッセージの整合性チェックに使用されます
* KEKキー暗号化キー（KEK）は暗号化キーの配布に使用されます
* TKー時鍵（TK）はデータの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 Temporal Key (TK) です。TK は Pairwise Transient Key (PTK) とも呼ばれます。TK は、通信中に時間または送信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、次の理由により 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 を導出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、メッセージの整合性チェックに使用されます。
* Nonce: Nonce は WPA キー階層の一部ではなく、PTK を導出するための入力です。
参考資料: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf

質問: **59**
複数の 20 MHz 幅の 802.11 チャネルを結合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. 高利得全方向性アンテナを利用する
正解: **(正解を表示します)**
説明

複数の20MHz幅の802.11チャネルをボンディングすることは、より広い帯域幅のチャネルを作成し、より高いデータレートの伝送をサポートする技術です。これにより、より多くのスペクトルリソースを使用し、干渉を低減することで、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。参考文献：https://ieeexplore.ieee.org/document/9288995

質問: **60**
別紙を参照してください。
最も少ない量のデータを受信するサーバーはどれですか?
A. 172.17.17.43
B. 10.100.100.25
C. 10.99.26.25
D. 192.168.0.56
正解: **(**正解を表示します**)**
ログサーバーの構成を示す図によると、サーバー172.17.17.43は 警告」イベントログレベル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。つまり、警告以上の重大度に分類されるイベントのみがログに記録されます。これらのイベントは通常、より重大度が低いイベント（例えば、
情報」、 デバッグ」、または 緊急」。

質問: **61**
信号強度を測定する場合、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. .-1 mW
B. 0.01 MW
C. 10mW
D. 1mW
正解: **B (**コメントを発表する**)**
dBmは、1mWに対する所定の電力レベルの比率を表す電力単位です。dBmをmWに変換する式は、P(mW) = 1mW * 10^(P(dBm)/10)です。したがって、-20dBmは0.01mWに相当し、P(mW) = 1mW * 10^(-20/10) = 0.01mWとなります。参考 :https://www.rapidtables.com/convert/power/dBm_to_mW.html

質問: **62**
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アドレスを一致させます
B. クライアント側での設定は必要ありません
C. MAC許可リストは時間の経過とともに簡単に維持されます
D. MAC識別子は偽装が難しい
正解: **B** (コメントを発表する)
レイヤー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、サーバーは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、スイッチは割り当てられたロール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、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：
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/mac-authentication.htm

質問: **63**
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 トラフィックをどのように確立するのでしょうか。
A. Aruba 6300M ではルーティングがデフォルトで有効になっています。
B. ルート リークはデフォルトの VRF で設定する必要があります。
C. SVI インターフェイスから 〝ルーティングなし」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。
正解: **A** (コメントを発表する)
Aruba CX 6300M スイッチでは、スイッチ仮想インターフェイス (SVI) 間のルーティングがデフォルトで有効になっています。
したがって、SVI に 〝ルーティングなし」設定が存在しない限り、120 と 130 などの SVI 間のトラフィックは、ルート リークや静的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。

質問: **64**
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正しい記述はどれですか?
A. 手動プロビジョニングではDHCPは不要ですが、DNSが必要です。
B. 手動プロビジョニングではDHCPは不要で、DNSも不要です。
C. 手動プロビジョニングにはDHCPが必要で、DNSは必要ありません。
D. 手動プロビジョニングにはDHCPが必要であり、DNSが必要です
正解: **C** (コメントを発表する)
Aruba Central では、DNS サービスに依存せずにスイッチを手動でプロビジョニングできますが、スイッチに IP アドレスを割り当てるには DHCP が必要です。DHCP は、スイッチが IP アドレスを取得するために不可欠です。IP アドレスは、ネットワーク内および Aruba Central と管理や設定のために通信するために必要です。一方、DNS は手動プロビジョニングでは必ずしも必須ではありません。Aruba Central やその他の管理インターフェースへの接続には、直接 IP アドレスを使用するか、その他の方法を使用できます。

質問: **65**
ディストリビューションおよびレイヤ3サービスに使用する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VLAN/サブネットを複数作成し、複数のアクセススタックで利用します。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ースを正しく設定するにはどうすればよいですか？
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 スタックのサブネットに SVI を作成します。
正解: **(**正解を表示します**)**
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を正しく設定するには、SVI スイッチ仮想インターフェイス (SVI) を作成します。スイッチ仮想インターフェイス (SVI) は、VLAN を表し、その VLAN にレイヤー 3 ルーティング機能を提供するスイッチ上の仮想インターフェイスです。SVI は、VLAN 間ルーティングの有効化、VLAN 内のホストへのゲートウェイ アドレスの提供、ACL または QoS ポリシーの VLAN への適用などに使用されます。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 (vlan 10 など) 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設定できます。SVI は、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。
6300MスタックのサブネットにSVIを作成します。SVIは、スイッチ上の仮想インターフェースで、VLANを表し、そのVLANにレイヤ3ルーティング機能を提供します。6300MスタックのサブネットにSVIを作成すると、スイッチはその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。また、6300Mスタックのサブネットに 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ースとケーブルの数が少なくなり、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、次の理由により、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構成する正しい方法ではありません。
6300Mスタック上のサブネット内に、各ダウンストリームスイッチ用の物理ルーティングインターフェースを作成する :このオプションは正しくありません。6300Mスタック上のサブネット内に、各ダウンストリームスイッチ用の物理ルーティング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、インターフェースリソースが消費され、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内に、各ダウンストリームスイッチ用の物理ルーティングインターフェースを作成すると、インターフェー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 :このオプションは正しくありません。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自身の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間ルーティングが有効になりません。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 スイッチは引き続き自身の 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 間ルーティングが有効になりません。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 スペースが浪費され、ネットワーク管理が複雑になります。

質問**: 66**
適切な QoS 概念とその定義を一致させます。
正解**:**

Explanation:
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、それぞれの要件に基づい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は、ネットワークパフォーマンスの向上、レイテンシの削減、スループットの向上、輻輳の防止に役立ちます。その概念と定義について。私の答えは次のとおりです。
QoS コンセプト:
* ベストエフォートサービス
* 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に平等に扱われる方法 a) 8 つのサービス クラスのうち 1 つで 802.1Q VLAN イーサネット フレームをマークすることにより、レイヤー 2 でネットワーク トラフィックを分類する方法 b) 64 の異なるサービス クラスのうち 1 つでパケットをマークすることにより、レイヤー 3 でネットワーク 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組み合わせは次のとおりです。
* 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なしに、先着順で平等に扱う方式です。これは、特定のQoS要件や保証が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は、帯域幅、遅延、ジッター、パケット損失を保証するものではありません。
* サービスクラス :これは、802.1Q VLAN Ethernetフレームを8つのサービスクラス （0〜7）のいずれかでマークすることにより、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、802.1Q VLAN タグ内の 3 ビットフィールドで、イーサネットフレームの優先度を示します。サービスクラスにより、ネットワークデバイスは優先度に基づいてさまざまな種類のトラフィックを識別し、処理することができます。サービスクラスは通常、LAN で使用されます。ローカルエリアネットワーク (LAN) は、家庭、オフィス、建物など、レイヤ 2 スイッチングが主流の環境など、限られた地理的領域内の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、パケットを64種類のサービスクラス（0～63）のいずれかにマークすることで、レイヤー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ヘッダー内の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異なる種類のトラフィックを識別し、処理することができます。差別化サービスは、通常、WANで使用されます。ワイドエリアネットワーク（WAN）は、国や大陸など、レイヤー3ルーティングが主流の環境など、広大な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 802.11規格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を向上させ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異なる種類のトラフィックを識別し、処理することができます。
参考資料: https://en.wikipedia.org/wiki/Quality_of_service https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_dfsrv/configuration/xe-16/qos-dfsrv-xe-16-book/qos-dfsrv-overview.html https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.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認定wmm

質問: **67**
ワイヤレス クライアントのローミングの決定はどこで行われますか?
A. クライアントデバイス
B. 仮想コントローラ
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
正解: **(**正解を表示します**)**
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、データレートなどのクライアントデバイス独自の基準に基づいて行われます。ネットワークは、ネイバーレポート、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が行います。参考 :https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/wlan-roaming/client-roaming.htm 無線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、現在の信号が特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）へのローミングを決定します。APとコントローラは、802.11kや

802.11v では、ローミングの最終決定は、アルゴリズムとしきい値に基づいてクライアント デバイスによって行われます。

質問: **68**
顧客との会議で、ネットワーク冗長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何ですか？
A. 現在のMSTPルート優先度としてデフォルトでMSTP構成IDリビジョン
B. スイッチのIMCアドレスを使用したデフォルトのMSTP構成ID名
C. スイッチのシリアル番号を使用したデフォルトのMSTP構成ID名
D. スイッチのシリアル番号としてデフォルトでMSTP構成IDリビジョン
正解: **B** (コメントを発表する)
MSTP (Multiple Spanning Tree Protocol)は、複数のVLANを持つネットワークにおけるループを防止するためのIEEE標準プロトコルです。MSTPを使用すると、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リージョンを識別する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ビットの数値です。デフォルトでは、MSTP構成ID名はスイッチのIMCアドレスに設定されています。IMCアドレスは、MACアドレス (メディアアクセス制御アドレス)から派生した一意の識別子です。MACアドレスは、ネットワークセグメント内の通信において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。スイッチの。参考 :https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/コンテンツ/arubaos-solutions/mstp/mstp.htm

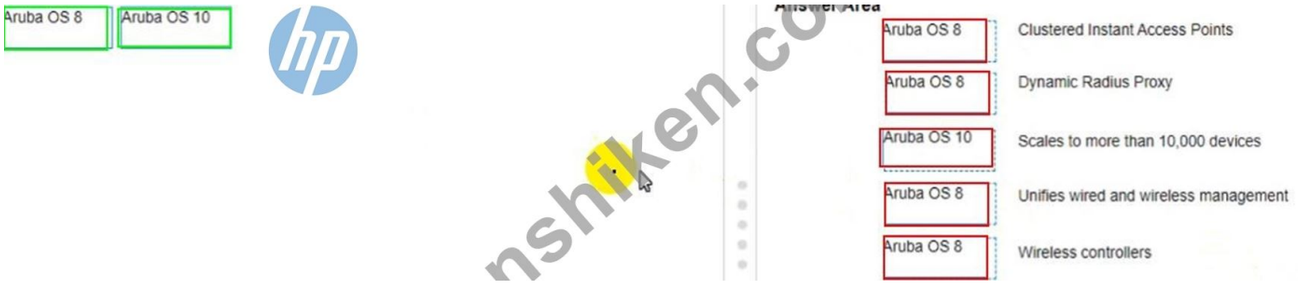
質問: **69**
既存の IAP-315 アクセス ポイントを持つネットワーク管理者は Aruba Central に興味があり、特定の機能に必要なライセンスを知る必要があります。機能ごとに必要なライセンスを一致させてください (一致は複数回使用できます)。

正解:

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コンプライアンス - Foundation
c) 展開された AP のヒートマップ - 高度
d) AOS10 クラスターのライブアップグレード - 上級
Aruba Central ライセンス ガイド 1 によると、Foundation ライセンスでは、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が提供されます。Advanced ライセンスでは、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が提供されます。
https://www.arubanetworks.com/techdocs/central/2.5.3/content/pdfs/ライセンスガイド.pdf

質問: **70**
機能を Aruba OS バージョンに一致させます (一致は複数回使用できます)。

正解:



質問: **71**

スパニング ツリー (STP) 設定を備えた 2 つの独立した ArubaOS-CX 6300 スイッチが、ポート 1/1/1 と 1/1/2 の間で 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」および 「no routing」コマンドがあります。STP はこれらのポートでどのようにトラフィックを転送または破棄しますか?
A. MACアドレスが低いスイッチは両方のポートで転送し、MACアドレスが高いスイッチは両方のポートで転送します。
B. MACアドレスの低いスイッチは両方のポートで転送し、MACアドレスの高いスイッチは1つのポートで破棄します。
C. MACアドレスの低いスイッチは1つのポートで破棄し、MACアドレスの高いスイッチは両方のポートで転送します。
D. MACアドレスの低いスイッチは1つのポートで破棄し、MACアドレスの高いスイッチは1つのポートで破棄します。
正解: **(**正解を表示します**)**
STP （スパニングツリープロトコル）は、スイッチまたはブリッジ間の冗長パスがループを発生させ、ブロードキャストストーム、多重フレーム送信、MACテーブルの不安定化を引き起こすのを防ぐことで、ブリッジ型イーサネットローカルエリアネットワークにおいてループフリーの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、ツリーに含まれない冗長リンクによるデータパケットの転送をブロックします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、2つのスイッチのブリッジID （プライオリティ値とMACアドレスで構成される）に基づいて、ルートブリッジを選択します。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、すべてのポートでトラフィックを転送します。
STPは、両方のスイッチの各ポートに、ポートID （プライオリティ値とポート番号で構成される）に基づいて役割と状態を割り当てます。ポートIDが低いポートが指定ポートとなり、トラフィックを転送します。一方、ポートIDが高い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、両スイッチ間には2つのパスが存在する可能性があり、ループが発生します。このループを防ぐため、STPは各スイッチのポートの1つでトラフィックを破棄することで、これらのパスの1つをブロックします。
両方のスイッチのプライオリティ値が同じ （デフォルトは32768）であると仮定すると、MACアドレスが小さい方のスイッチのブリッジ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。
両ポートの優先度が同じ値 （デフォルトは128）であると仮定すると、ポート1/1/1はポート番号が小さいため、両スイッチともポート1/1/2よりも低いポートIDを持ちます。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、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 アドレスが低いスイッチは 1 つのポート (ポート 1/1/2) のトラフィックを破棄し、MAC アドレスが高いスイッチも 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。

質問: **72**
グループ作成時にユーザーが Aruba Central で定義できるデバイス構成グループ タイプはどれですか?
(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
正解: **(**正解を表示します**)**
Aruba Centralでは、デバイス設定グループを作成し、各グループ内のデバイスに共通の設定を定義できます。ネットワーク要件や管理設定に応じて、さまざまな種類のグループを作成できます。
グループ作成時に Aruba Central で定義できる 2 種類のグループは次のとおりです。
- 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、複数のデバイスまたはデバイスグループに適用できる変数と式を使用して、構成テンプレートを作成できます。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 :デバイスをAruba Centralに初めて追加すると、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

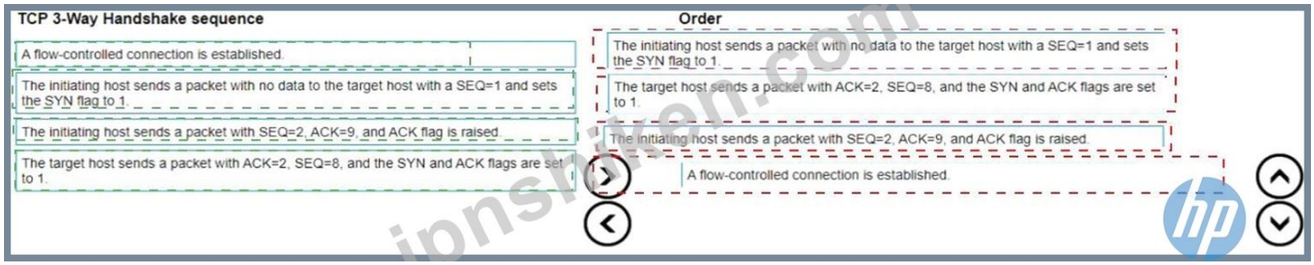
質問: **73**
Aruba ネットワーク機器の仮想スイッチング フレームワーク (VSF) の機能は何ですか?
A. スイッチをスタックして冗長性を実現できます。
B. 物理スイッチ上に仮想ネットワークを作成できるようになります。
C. 複数のスイッチにわたって仮想 LAN を構成します。
D. 物理スイッチを 1 つの論理スイッチに仮想化するために使用されます。
正解: **D (**コメントを発表する**)**

質問: **74**
セキュリティのために WPA2-Personal を使用すると、WLAN 環境にどのような脆弱性が生じますか?
A. 認証局によって生成されたX509証明書を使用します
B. ペアワイズ一時キー（PTK）は各セッションに固有です
C. ペアワイズマスターキー（PMK）はすべてのユーザーによって共有されます
D. WPA 4ウェイハンドシェイクを使用しません
正解: **(**正解を表示します**)**
説明
WPA2-Personalをセキュリティに使用した場合、WLAN環境に導入される脆弱性は、PMK（ペアワイズマスターキー）がPSK（事前共有キー）から派生した鍵であることです。PSKは通信開始前に2者間で共有される鍵で、どちらも固定されています。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を生成できます。これは、PSK または PMK が攻撃者によって侵害された場合、それらを使用して PTK で暗号化さ

れたすべてのトラフィックを復号化できることも意味します。PTK (Pairwise Temporal Key) は PMK から派生したキー、ANonce AuthenticatorNonce (ANonce) は認証子 (AP などのネットワーク 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、SNonce Supplicant Nonce (SNonce) はサプリカント (STA などのネットワーク リソースにアクセスするデバイス) によって生成される乱数、AA Authenticator Address (AA) は認証子の MAC アドレス、SA Supplicant Address (SA) は疑似乱数関数 (PRF) を使用するサプリカントの MAC アドレスです。PTK は 4 つのサブキーで構成されます: KCK キー確認キー (KCK) はメッセージの整合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 メッセージ整合性コード (MIC) キーが使用されます。
その他のオプションは、以下の理由により弱点ではありません。
証明機関によって生成された X 509 証明書を使用します。: WPA2 パーソナルは認証に X 509 証明書も証明機関も使用しないため、このオプションは false です。X 509 証明書と証明機関は、802.1X と EAP を使用する WPA2 エンタープライズ モードで使用されます。拡張認証プロトコル (EAP) は、パスワード、証明書、トークン、生体認証などの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、ワイヤレス ネットワークやポイントツーポイント接続で使用され、サプリカント (ネットワークにアクセスするデバイス) と認証サーバー (サプ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 サーバーによるユーザー認証用 RADIUS (リモート認証ダイヤルイン ユーザー サービス) 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的な認証、承認、アカウンティング (AAA) 管理を提供するネットワーク プロトコルです。
Pairwise Temporal Key（PTK）はセッションごとに固有です :このオプションは無効です。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、通信中に時間や送信パケット数に基づいて定期的にPTKが変更されることを意味します。これにより、リプレイ攻撃を防ぎ、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 :WPA2-Personalは鍵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、このオプションは無効です。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を生成するプロセスです。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することもできます。
参考資料: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management
https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf

質問: **75**
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?

正解:



説明

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 でデータのない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: 通常制御の接続が確立されます。

参考資料: 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

質問: **76**

Clearpass OnGuard についての説明は何ですか? (2 つ選択してください。)

A. Onguard は各デバイスに固有の ID を割り当てます。

B. ゲストデバイスの自己登録に使用されます。

C. OnGuard はクライアント システム上で実行されるエージェントです。

D. OnGuard はクライアント システムのポスチャ チェックを実行しています。

E. ユーザーがデバイスを安全に構成するための直感的なポータルです。

正解: **(**正解を表示します**)**

ClearPass OnGuardは、ClearPass Policy Managerのコンポーネントであり、デバイスの健全性とセキュリティポスチャのチェックを実行し、ネットワークへのアクセスを許可する前に、デバイスの健全性とセキュリティポスチャのチェックを行い、組織のコンプライアンス要件を満たしていることを確認します。クライアントシステム上でエージェントとして動作し、これらのチェックを実行します。

質問: **77**

信号強度を測定する場合、dBm が一般的に使用され、0 dBm は 1 mW の電力に相当します。

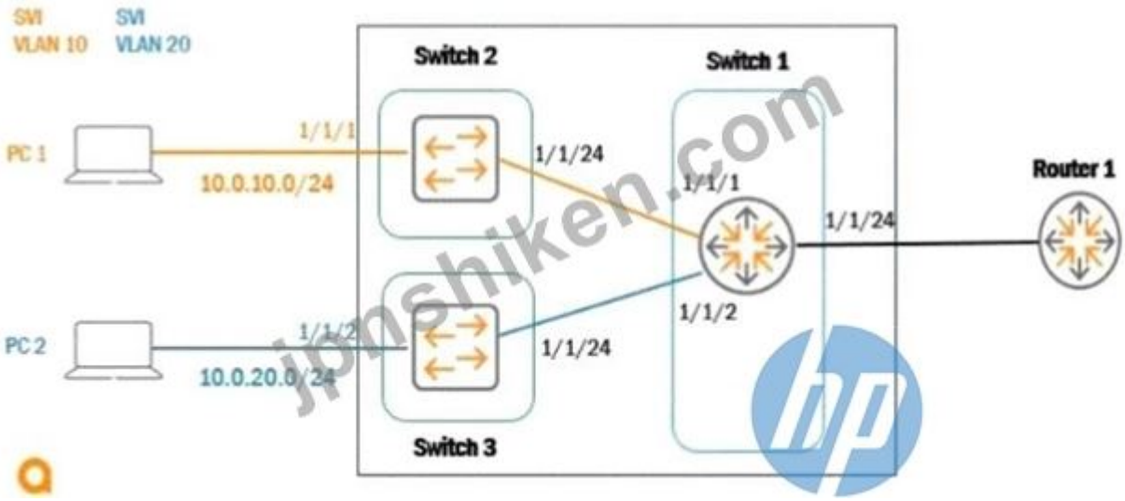
-20 dBm は何に相当しますか?
A. .-1 mW
B. 0.01 MW
C. 10mW
D. 1mW
正解: **B (**コメントを発表する**)**
dBmは、1mWに対する所定の電力レベルの比率を測定する電力単位です。dBmをmWに変換する式は、P(mW) = 1mW * 10^(P(dBm)/10)です。したがって、-20dBmは0.01mWに相当し、P(mW) = 1mW * 10^(-20/10) = 0.01mWとなります。参考 :https://www.rapidtables.com/convert/power/dBm_to_mW.html dBmは、1ミリワット(mW)を基準とした電力の対数単位です。-20dBmは、信号強度が1mWより20デシベル低いことを意味します。mWに換算すると、0.01mWです。10dBの減少は、電力が10分の1に減少することを意味します。したがって、-20 dBm は 10-210-2 または 0.01 mW になります。

質問: **78**
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 トラフィックをどのように確立するのでしょうか。
A. Aruba 6300M ではルーティングがデフォルトで有効になっています。
B. ルート リークはデフォルトの VRF で設定する必要があります。
C. SVI インターフェイスから 〝ルーティングなし」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。
正解: **(**正解を表示します**)**
Aruba CX 6300M スイッチでは、スイッチ仮想インターフェイス (SVI) 間のルーティングがデフォルトで有効になっています。
したがって、SVI に 〝ルーティングなし」設定が存在しない限り、120 と 130 などの SVI 間のトラフィックは、ルート リークや静的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。

質問: **79**
Aruba 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用して RF 計画および最適化サービスを集中化できますか?
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
正解: **(**正解を表示します**)**
AirMatchは、Aruba無線ネットワーク向けにRFプランニングと最適化を一元的に提供する機能です。クラウドベースのアルゴリズムと機械学習を用いて、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。参考 :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）トポロジーとして、デイジーチェーン＋マルチアクティブ検出（MAD）とリングトポロジーが挙げられます。MADを備えたデイジーチェーントポロジーは、複数のスイッチを直列に接続す

る簡単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MADが検出して処理できるようにします。リングトポロジーは、VSFメンバー間にループ接続パターンを作成することで冗長性を提供し、ネットワークの復元力と信頼性を向上させます。

質問: **80**



指定されたトポロジに基づいて、ルータ 1 で LLDP が有効になっている場合に、スイッチ 1 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の Aruba スイッチの要件は何ですか。

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 の有効化

C. int 1/1/24、lldp受信

D. int 1/1/24、CDPなし

正解: **(**正解を表示します**)**

Arubaスイッチでは、Link Layer Discovery Protocol（LLDP）がすべてのポートでデフォルトで有効になっています。このプロトコルは業界標準のネットワーク検出プロトコルであり、ネットワークデバイスがローカル管理ネットワーク（IEEE 802ネットワークに代表される）上で自身のID、機能、およびネイバーをアドバタイズするために使用されます。これは、ネットワークマッピングやトラブルシューティングに役立ちます。LLDPはデフォルトで有効になっているため、ポートでLLDPが無効になっていない限り、スイッチ1のポート1/1/24でルータ1からのLLDPメッセージを受信するために追加の設定を行う必要はありません。

質問: **81**

ハッカーは、ユーザーのセッションにアクセスするために、ユーザーの 3 ウェイ ハンドシェイクを変更しました。

どのセキュリティ メカニズムがこのトラフィックをインテリジェントに拒否するでしょうか?

A. 帯域外管理 (00BM)

B. ステートレスファイアウォール

C. アクセス制御リスト (ACL)

D. ステートフルファイアウォール

正解: **(**正解を表示します**)**

ステートフルファイアウォールは、ユーザーの3ウェイハンドシェイクを改ざんしてセッションにアクセスしようとするハッカーからのトラフィックをインテリジェントに拒否します。ステートフルファイアウォールはアクティブな接続の状態を追跡し、受信パケットが確立済みのセッションの一部であるかどうかを認識できます。これにより、既知の接続状態と一致しない不正アクセスの試みを検出し、ブロックすることができます。

質問: **82**
無線帯域と AP 無線間の負荷分散を実現する Aruba テクノロジーはどれですか?
A. アルバ ESP
B. アルバクライアントマッチ
C. アルバ エアウェーブ
D. アルバセントラル
正解: **(**正解を表示します**)**
Aruba ClientMatchは、クライアントの行動を継続的に監視し、クライアント接続を自動調整してWi-Fiパフォーマンスを最適化するテクノロジーです。これにより、クライアントをWLAN上で最も混雑の少ないアクセスポイントと最適な無線に誘導し、異なる無線帯域やAP無線間で効果的な負荷分散を実現します。

質問: **83**
セキュアなエンタープライズ モード WLAN に接続すると、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
正解: **B (**コメントを発表する**)**
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アソシエーションを完了した後、WPA 4ウェイハンドシェイクの前に開始されます。これは、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するEAP（拡張認証プロトコル）プロセスの一部です。

質問: **84**
AP 信号強度 0.0000001 ミリワットは何 dBm に相当しますか?
A. -90 dBm
B. -60 dBm
C. -70 dBm
D. -80 dBm
正解: **(**正解を表示します**)**
AP信号強度が0.0000001ミリワットの場合、-80dBmに相当します。dBmは対数スケールで、10dBmごとに電力が10倍に増加または減少します。1ミリワット（mW）の信号強度は0dBmなので、0.0000001mWの信号強度は1mWより80デシベル低い−80dBmとなります。

質問: **85**
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. ペアワイズ一時鍵 (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（ノンス）
正解: **(**正解を表示します**)**
データの暗号化や復号化に使用されるWPA キー階層の部分は、Pairwise Temporal Key (PTK) です。PTK は PMK から派生したキーです。Pairwise Master Key (PMK) は PSK から派生したキーです。Pre-shared Key (PSK) は通信を開始する前に 2 者間で共有されるキーです。ANonce Authenticator Nonce (ANonce) は認証子 (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 (AP など) によって生成される乱数です。SNonce Supplicant Nonce (SNonce) はサプリカント (ネットワーク リソースにアクセスするデバイス (STA など) によって生成される乱数です。AA Authenticator Address (AA) は認証子の MAC アドレスです。SA Supplicant Address (SA) は疑似乱数関数 (PRF) を使用するサプリカントの MAC アドレスです。PTK は 4 つのサブキーで構成されます。
KCK キー確認キー（KCK）はメッセージの整合性チェックに使用されます。
KEKキー暗号化キー（KEK）は暗号化キーの配布に使用されます
TK一時鍵（TK）はデータの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 Temporal Key (TK) です。TK は Pairwise Transient Key (PTK) とも呼ばれます。TK は、通信中に時間または送信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、次の理由により 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 を導出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、メッセージの整合性チェックに使用されます。
Nonce: Nonce は WPA キー階層の一部ではなく、PTK を導出するための入力です。

質問: **86**
Aruba の Captive Portal ではどの認証が使用されますか?
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
正解: **A (**コメントを発表する**)**
Aruba の Captive Portal 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 リクエストをインターセプトし、クライアントが資格情報を入力できる Web ページにリダイレクトします。その後、資格情報は RADIUS サーバーまたはローカル データベースによって検証され、ネットワーク アクセスが許可されます。
参照: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/captive-portal/captive-portal-auth.htm Aruba の Captive Portal は主にネットワーク層で動作するレイヤー 3 認証を使用します。ユーザーが Captive Portal を使用してネットワークに接続すると、認証のために Web ページにリダイレクトされます。このプロセスでは、ユーザーがネットワークへのフル アクセスを取得する前に、Web インターフェイスで資格情報を入力するか、利用規約に同意する必要があります。Captive Portal はレイヤー 3 で

ユーザーの Web トラフィックをインターセプトし、続行する前に認証を要求するため、レイヤー 3 認証の一種と見なされます。

質問: **87**
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 ヘッダーに渡されるものはどれですか?
A. チェックサム
B. 生存時間
C. プロトコル
D. 宛先IP
正解: **(**正解を表示します**)**
レイヤー 3 ルート ループを軽減するために使用されるレイヤー 3 IPv4 パケット ヘッダー内のフィールドは、Time To Live (TTL) です。
TTL は、パケットが破棄されるまでに通過できるホップの最大数を示す 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によって 1 ずつ減ります。TTL が 0 に達するとパケットは破棄され、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、ソース 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。メッセージが送信元デバイスに送り返されます。 TTLは、ループしたネットワークトポロジ内でパケットが無期限に循環するのを防ぐため、レイヤー3のルートループを軽減するために使用されます。また、TTLはネットワークリソースを節約し、ループしたパケットによる輻輳を回避するのにも役立ちます。
その他のオプションは、次の理由により、レイヤー 3 IPv4 パケット ヘッダー内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ルートループを軽減することはできません。
* 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 などの、データ転送に 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) 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、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。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、ウィンドウ処理を使用してデータ配信とフロー制御を保証します。また、TCP は、再送、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を処理します。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。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形式を持ちます。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、

質問: **88**
Aruba の Captive Portal ではどの認証が使用されますか?
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
正解: **A (**コメントを発表する**)**
ArubaのCaptive Portal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。入力された認証情報は、RADIUSサーバーまたはローカルデータベースによって検証された後、ネットワークアクセスを許可します。参考：
https://www.
arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/captive-portal/captive-portal-auth.htm
Arubaのキャプティブポータルは、主にネットワーク層で動作するレイヤー3認証を使用します。ユーザーがキャプティブポータルを使用してネットワークに接続すると、認証用のWebページにリダイレクトされます。このプロセスでは、ユーザーはWebインターフェースを通じて資格情報を入力するか、利用規約に同意した後、ネットワークへのフルアクセスが可能になります。キャプティブポータルは、ユーザーのWebトラフィックをレイヤー3で傍受し、操作を続行する前に認証を要求するため、レイヤー3認証の一種と考えられています。

質問: **89**
ArubaOS-CX スイッチを介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ことを保証する必要があります。
このタスクに使用する最適なスケジューリング テクノロジーは何ですか?
A. QoSシェーピング
B. レート制限
C. 厳密なキューイング
D. DWRRキューイング
正解: **(**正解を表示します**)**
ストリクトキューイングは、遅延の影響を受けやすい音声トラフィックを他のトラフィックよりも優先させるのに最適なスケジューリング技術です。この方式により、音声トラフィックがキューイングされた他のトラフィックよりも先に送信されるため、遅延の可能性が効果的に低減されます。

質問: **90**
データリンク層 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
正解: **B (**コメントを発表する**)**
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を使用してネットワーク層PDU（パケット）をカプセル化するデータリンク層PDUです。フレームは、イーサネット、Wi-Fiなどの物理メディアを介して送信されます。参考：
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/networking-basics.htm

質問: **91**
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) 層と一致させます。

正解:

質問: **92**
各 AAA サービスを正しい定義と一致させます (一致は複数回使用される場合やまったく使用されない場合があります)

正解:

説明

AAA 認証、認可、アカウンティング (AAA) 認証、認可、アカウンティング (AAA) は、ネットワーク アクセス制御のためのセキュリティ サービスを提供するフレームワークです。AAA は次の 3 つのコンポーネントで構成されます。

認証: ユーザー名とパスワード、証明書、トークンなどの資格情報に基づいて、ネットワークにアクセスするユーザーまたはデバイスの ID を確認するプロセス。認証では、PAP 、CHAP 、EAP 、RADIUS 、TACACS+ などのさまざまなプロトコルを使用できます。

認可 :ユーザーまたはデバイスのIDと権限に基づいて、ネットワークリソースへのアクセスを許可または拒否するプロセス。認可には、ACL、RBAC、MAC、DACなど、さまざまな方法を使用できます。

アカウンティング :ユーザーまたはデバイスによるネットワークリソースのアクティビティと使用状況を記録し、報告するプロセス。アカウンティングでは、syslog、SNMP、NetFlowなど、さまざまな形式を使用できます。

サービス。私の答えはこうです。

各 AAA サービスとその定義の正しい組み合わせは次のとおりです。

会計 :C. ネットワーク上のユーザーアクティビティの追跡

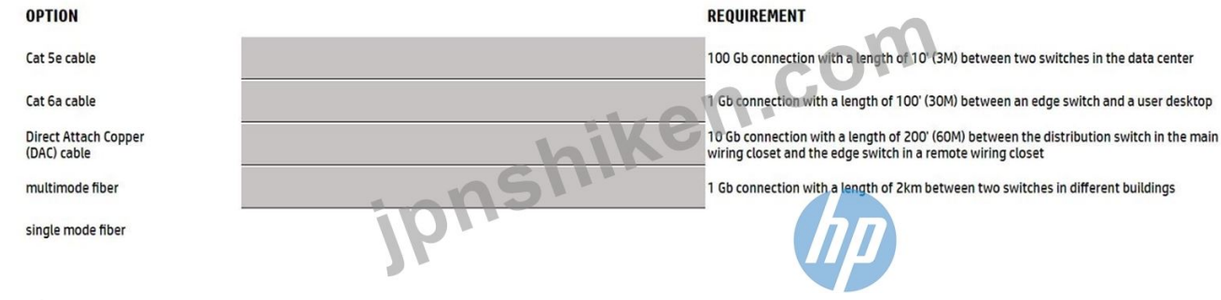
認証: D. 資格情報/証明書に基づいてネットワークにアクセスできるユーザー 承認: B. ネットワーク上のユーザー アクセスを制御する その他のオプションは、次の理由により正しく一致しません。

アクセスを許可または拒否するエンティティを指定するルールのリスト: このオプションは、アクセス制御リスト (ACL) の定義です。アクセス制御リスト (ACL) アクセス制御リスト (ACL) は、ルータ、スイッチ、ファイアウォール、サーバなどのネットワーク リソースへのアクセスを許可または拒否するエンティティを指定するルールのリストです。ACL は、送信元と宛先の IP アドレス、ポート番号、プロトコル タイプ、時刻などのさまざまな基準に基づくことができます。ACL は、着信または発信などのさまざまなインターフェイスや方向に適用できます。ACL は、AAA サービスではなく、 show access-lists、show ip access-lists、debug ip packet などのコマンドを使用して確認できます。

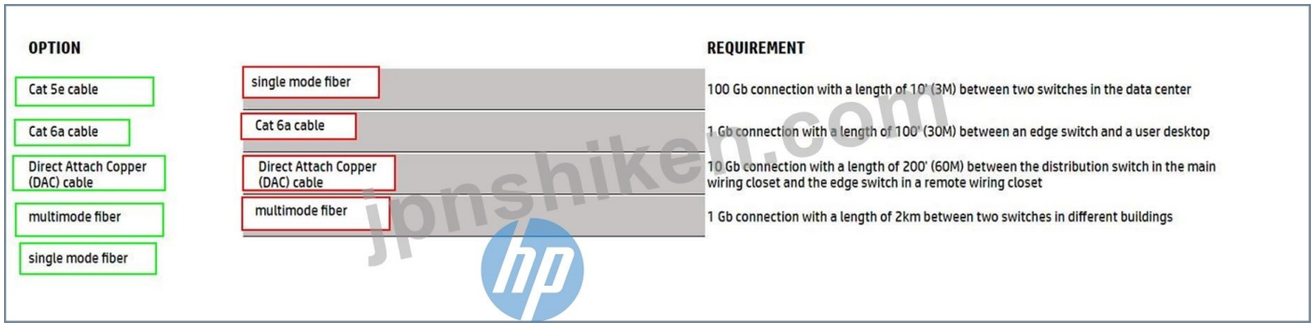
資格情報/証明書に基づいてネットワークにアクセスできるユーザー :このオプションは認証の定義であり、認可ではありません。認可とは、資格情報/証明書ではなく、ユーザーまたはデバイスのIDと権限に基づいてネットワークリソースへのアクセスを許可または拒否するプロセスです。
参考資料: https://en.wikipedia.org/wiki/AAA_(computer_security)
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-1

質問: **93**
UXI の 2 つの利点は何ですか? (2 つ選択してください)
A. UXIはインターネット接続なしでも使用できます
B. UXIは遠隔地の最適なWiFiチャンネルを計算するのに役立ちます
C. UXIはクライアント/ユーザーのように動作します
D. UXI 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。
正解: **C,E (**コメントを発表する**)**
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指標を測定できます。
参考資料: https://www.arubanetworks.com/products/networking/user-experience-insight/

質問: **94**
各要件に応じて、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ます。 すべての長さは、パッチ ケーブル、サービス ループなど（使用されている場合）を含むケーブルの合計長さを示します。）



正解:



質問: **95**

次のうち、Aruba スイッチでサポートされている主なセキュリティ機能はどれですか?
A. 侵入防止システムが組み込まれています。
B. すべて正解です。
C. Web コンテンツのフィルタリング。
D. ロールベースのアクセス制御。
正解: **(**正解を表示します**)**

質問: **96**
顧客は、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。
ネットワークへの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. ピープ
正解: **(**正解を表示します**)**
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法です。
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。
参考文献:
https://www.arubanetworks.com/techdocs/ClearPass/6.9/Guest/Content/CPPM_UserGuide/EAP-TL

質問: **97**
グループ作成時にユーザーが Aruba Central で定義できるデバイス構成グループ タイプはどれですか? (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
正解: **(**正解を表示します**)**
説明
Aruba Centralでは、デバイス設定グループを作成し、各グループ内のデバイスに共通の設定を定義できます。ネットワーク要件や管理設定に応じて、さまざまな種類のグループを作成できます。Aruba Centralでグループ作成時に定義できる2種類のグループは次のとおりです。
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、複数のデバイスまたはデバイスグループに適用できる変数と式を使用して、構成テンプレートを作成できます。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。

参考資料: 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

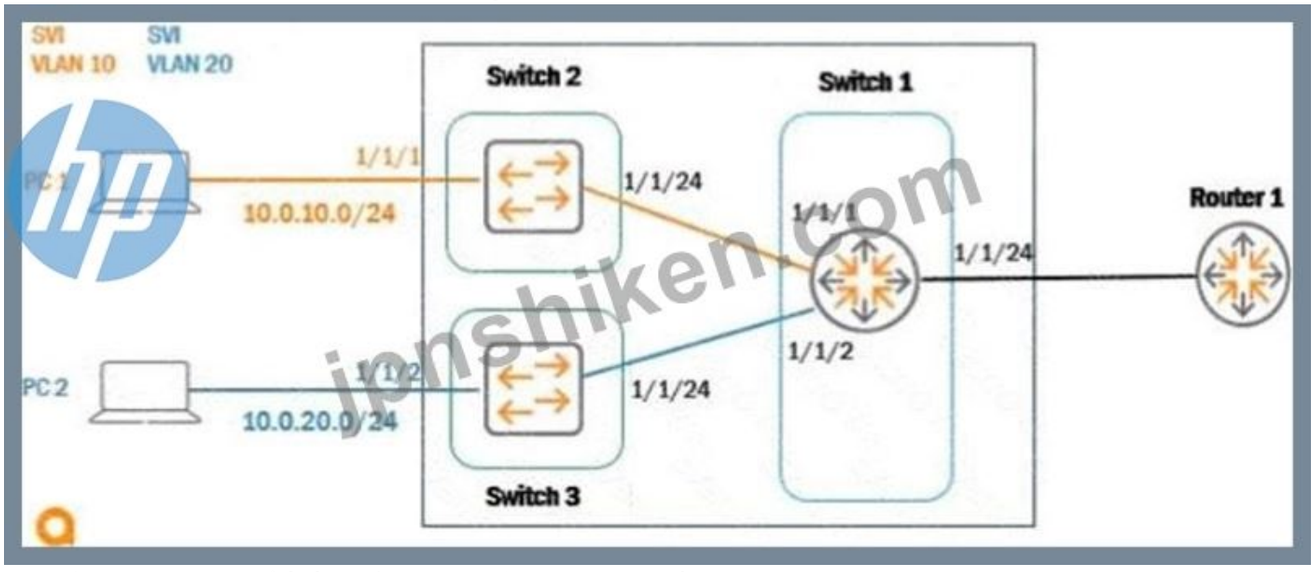
質問: **98**
ネットワーク技術者が支社向けに新しいSSIDをテストしています。接続、IPアドレスの取得、DNS名解決は可能ですが、インターネットを閲覧できません。
ブランチの既存のSSIDでは、新しいSSIDと同じVLAN上でインターネットへの接続が期待どおりに機能します。ワイヤレスクライアントには、インターネットアクセスを許可するための新しいロールが割り当てられているはずです。
両方の SSID が同様に機能することを確認するために、ネットワーク技術者は何を検証する必要がありますか?
A. 各 SSID の認証および暗号化パラメータが有効になっており、同じであることを確認します。
B. 暗黙的な すべて拒否」がファイアウォール ポリシーの最後のエントリであることを確認します。
C. 新しい SSID がブランチ オフィスのすべての AP で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。
正解: **(**正解を表示します**)**
ネットワーク技術者が、接続とDNS解決は成功しているにもかかわらず、新しいSSIDでインターネットアクセスが許可されないという問題に遭遇した場合、新しいSSIDに関連付けられた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、意図したとおりに適用されるように正しい順序で配置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、2つ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手段となります。

質問: **99**
管理距離の目的を説明する
A. 管理距離が大きいほど優先されます
B. 管理距離はルートエントリの信頼度評価として使用されます。
C. 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管理距離が長くなります。
D. スタティックルートの管理距離は10です
正解: **(**正解を表示します**)**

質問: **100**
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。
接続が成功するためにはどの RADIUS メッセージに注意する必要がありますか?
A. 承認済み
B. アクセス許可
C. 成功
D. 認証済み

正解: (正解を表示します)
802.1X経由の接続が成功した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サーバがサプリカント（ネットワークへのアクセスを希望するデバイス）を認証・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ます。これらの属性は、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）がサプリカントのトラフィックをどのように処理すべきかを指定します。
その他のオプションは、次の理由により RADIUS メッセージではありません。
- 承認済み: これは RADIUS メッセージではありませんが、認証と承認が成功した後、認証子のポートがサプリカントからのトラフィックを渡すことができ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）がパスワード、証明書、トークン、生体認証などの複数の認証方法をサポートする認証フレームワークであることを示すステータスです。EAPは、ワイヤレスネットワークやポイントツーポイント接続で使用され、サプリカント（ネットワークへのアクセスを要求するデバイス）と認証サーバー（サプリカントの資格情報を検証するデバイス）間の安全な認証を提供します。サプリカントと認証サーバー間の交換が正常に完了しました。
- 認証済み: これは RADIUS メッセージではありませんが、サプリカントの認証が成功した後、認証子のポートが認証サーバーから EAP 成功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#アクセス承認
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-https://en.wikipedia.org/wiki/IEEE_802.1X#Port-based_network_access_control
https://en.wikipedia.org/wiki/拡張認証プロトコル#EAP_exchange

質問: **101**
指定されたトポロジに基づいて、スイッチ 1 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の Aruba スイッチの要件は何ですか。



ルータ 1 で LLDP が有効になっているのはいつですか?

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 の有効化
C. int 1/1/24、lldp受信
D. int 1/1/24、CDPなし
正解: **(**正解を表示します**)**
Aruba スイッチが特定のポート上で LLDP メッセージを受信するには、そのポート上で LLDP を有効にする必要があります。
通常、Aruba スイッチのデフォルト設定ではすべてのポートで 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。
つまり、ルータ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、追加の設定なしでメッセージを受信できるはずです。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、LLDPを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）と似ています。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ArubaスイッチでLLDPを有効にする一般的な方法ではありません。オプションDはCisco Discovery Protocol（CDP）に関連していますが、LLDPの動作とは無関係です。

質問: **102**
ネットワーク技術者は、キャプティブポータルの完了後、顧客がゲストネットワークに正常に接続できたことを確認しています。ネットワーク技術者はClearPassのアクセストラッカーを確認しています。
顧客のセッションの OUTPUT タブを確認するときに、どのロールが表示される必要がありますか?
A. ゲストが認証されました
B. キャプティブポータルログイン
C. キャプティブポータルリダイレクト
D. ゲストログオン
正解: **(**正解を表示します**)**
ClearPassのアクセストラッカーでは、顧客がキャプティブポータルを介してゲストネットワークに正常に接続した後、出力タブに、ユーザーが認証されていることを示すロールが表示されます。
「ゲストが認証されました。」このロールは、ユーザーが認証プロセスに合格し、アクセスが許可されたことを確認します。

質問: **103**
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 ヘッダーに渡されるものはどれですか?
A. チェックサム
B. 生存時間
C. プロトコル
D. 宛先IP
正解: **B (**コメントを発表する**)**
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まで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によって 1 ずつ減算されます。TTL が 0 に達すると、パケットは破棄され、ICMP が送信されます。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を持ちます。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はレイヤーを緩和するために使用されます
3 ルートループは、ループしたネットワークトポロジ内でパケットが無期限に循環するのを防ぐため、ルートループを防ぎます。また、TTLはネットワークリソースを節約し、ループしたパケットによる輻輳を回避するのにも役立ちます。
その他のオプションは、次の理由により、レイヤー 3 IPv4 パケット ヘッダー内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16ビットのフィールドで、IPヘッダーの整合性を検証するために使用されます。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ルートループを軽減することはできません。
- 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などのIPを使用してデータ転送を行う上位層プロトコルを識別します。TCP（Transmission Control Protocol）は、異なるデバイス上のアプリケーション間で、信頼性が高く、順序付けされ、エラーチェックされたデータ転送を提供するコネクション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、ウィンドウ処理を使用してデータ配信とフロー制御を保証します。また、TCPは、再送、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、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 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、

質問: **104**
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アドレスを一致させます
B. クライアント側での設定は必要ありません
C. MAC許可リストは時間の経過とともに簡単に維持されます
D. MAC識別子は偽装が難しい
正解: **(**正解を表示します**)**
レイヤー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、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、スイッチは割り当てられたロール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、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-overview/mac-authentication.htm

質問: **105**
スパニング ツリー (STP) 設定を備えた 2 つの独立した ArubaOS-CX 6300 スイッチが、ポート 1/1/1 と 1/1/2 の間で 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」および「no routing」コマンドがあります。STP はこれらのポートでどのようにトラフィックを転送または破棄しますか?
A. MACアドレスが低いスイッチは両方のポートで転送し、MACアドレスが高いスイッチは両方のポートで転送します。
B. MACアドレスの低いスイッチは両方のポートで転送し、MACアドレスの高いスイッチは1つのポートで破棄します。
C. MACアドレスの低いスイッチは1つのポートで破棄し、MACアドレスの高いスイッチは両方のポートで転送します。
D. MACアドレスの低いスイッチは1つのポートで破棄し、MACアドレスの高いスイッチは1つのポートで破棄します。
正解: **D (**コメントを発表する**)**
STP（スパニングツリープロトコル）は、スイッチまたはブリッジ間の冗長パスがループを発生させ、ブロードキャストストーム、多重フレーム送信、MACテーブルの不安定化を引き起こすのを防ぐことで、ブリッジ型イーサネットローカルエリアネットワークにおいてループフリーの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、ツリーに含まれない冗長リンクによるデータパケットの転送をブロックします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、2つのスイッチのブリッジID（プライオリティ値とMACアドレスで構成される）に基づいてルートブリッジを選択します。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、すべてのポートでトラフィックを転送します。
* STPは、両方のスイッチの各ポートに、ポートID（優先度とポート番号から構成される）に基づいて役割と状態を割り当てます。ポートIDが小さいポートが指定ポートとなり、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、両スイッチ間には2つのパスが存在する可能性があり、ループが発生します。このループを防ぐため、STPは各スイッチのポートの1つでトラフィックを破棄することで、これらのパスの1つをブロックします。
* 両方のスイッチのプライオリティ値が同じ（デフォルトは32768）であると仮定すると、MACアドレスが小さい方のスイッチのブリッジ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。

* 両ポートの優先度が同じ値（デフォルトは128）であると仮定すると、ポート1/1/1はポート番号が小さいため、両スイッチともポート1/1/2よりも低いポートIDを持ちます。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、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 アドレスが低いスイッチは 1 つのポート (ポート 1/1/2) のトラフィックを破棄し、MAC アドレスが高いスイッチも 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。
参考文献: 3 https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

質問: **106**
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
正解: **(**正解を表示します**)**
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。
参考資料:https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/iap-dhcp/iap-dhc

質問: **107**
ARP の機能について説明します。
A. クライアントには ARP キャッシュがないため、常にデフォルト ゲートウェイを要求します。
B. ARP は MAC アドレスをスイッチ ポートにマッピングします。
C. ARP はレイヤー 3 IP アドレスをレイヤー 2 MAC アドレスにマッピングします。
D. ARP はマルチキャストを使用して ARP テーブルを構築します。
正解: **(**正解を表示します**)**
アドレス解決プロトコル（ARP）は、レイヤー3のIPアドレスをレイヤー2のMACアドレスにマッピングするために使用されます。ネットワーク上のデバイスが他のデバイスと通信する場合、ARPを使用して通信先のIPアドレスに対応するMACアドレスを見つけ、ローカルネットワーク用のフレームを構築します。

質問: **108**
Aruba のロールベース アクセス制御機能は何を提供しますか?
A. ネットワーク デバイスの展開を自動化します。
B. デバイスの種類に基づいて、ユーザーを特定のネットワーク セグメントに制限します。
C. ユーザー ID に基づいて動的なファイアウォール ルールを提供します。
D. VLAN をユーザー ロールに割り当てます。
正解: **C (**コメントを発表する**)**

質問: **109**
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アドレスを一致させます
B. クライアント側での設定は必要ありません
C. MAC許可リストは時間の経過とともに簡単に維持されます
D. MAC識別子は偽装が難しい
正解: **(**正解を表示します**)**
レイヤー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、スイッチは割り当てられたロール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、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

質問: **110**
Aruba CX スイッチのハードリセットを実行するにはどうすればいいですか?
A. リセットボタンを押し、クリアボタンを 5 秒間押したままリセットボタンを放します。
B. リセットボタンを 5 秒間押し続けてから放します。
C. リセットボタンとクリアボタンを同時に押します。
D. リセットボタンを3回押します。
正解: **B (**コメントを発表する**)**
Aruba CXスイッチでハードリセットを実行するには、通常、リセットボタンを5秒など一定時間押し続け、その後放します。この操作によりスイッチが再起動し、認証情報を含む工場出荷時の設定に戻ります。

質問: **111**
Aruba Mobility Controller は、キャンパス ネットワーク内のレイヤー 3 モビリティをどのように処理しますか?
A. 各ワイヤレス クライアントに一意の IP サブネットを割り当てます。
B. 各アクセス ポイントへのトンネルを維持することで、シームレスなユーザー遷移を実現します。
C. ユーザーの位置と動きを追跡する集中型データベースを通じて。
D. モビリティでは、レイヤー 3 での特別な処理は必要ありません。
正解: **C (**コメントを発表する**)**