# HP.HPE6-A85.v2025-04-23.q90

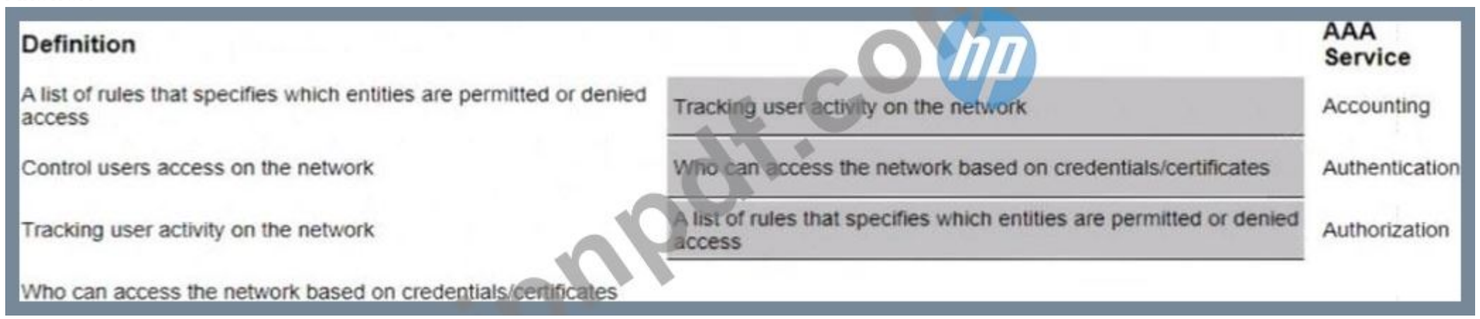
| | |
|---|---|
| 試験コード: | HPE6-A85 |
| 試験名称: | Aruba Campus Access Associate Exam |
| 認定資格: | HP |
| 無料問題数: | 90 |
| バージョン: | v2025-04-23 |
| アクセス数: | 498 |
| ページビュー数: | 900 |
| https://www.jpnpdf.com/HP.HPE6-A85.v2025-04-23.q90-mondaishu.html | |

最新問題: **1**
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.** .01 メガワット
**C.** 10mW
**D.** 1mW
**Answer: B (メーッセージを残す)**
説明
dBm は、与えられた電力レベルを 1 mW に対してどれだけの比率で表すかを表す電力の単位です。dBmを mW に変換する式は、P(mW) = 1mW * 10^(P(dBm)/10) です。したがって、-20 dBm は 0.01 mW に相当し、次の式で表されます。P(mW)
1mW * 10^(-20/10) = 0.01 mW 参考:https://www.rapidtables.com/convert/power/dBm_to_mW.html

最新問題: **2**
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。
**Answer: C (メーッセージを残す)**
アドレス解決プロトコル (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するために使用されます。
ネットワーク上のデバイスが別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 ネットワークのフレームを構築できます。

最新問題: **3**
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)


**Answer:**




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一致は次のとおりです。
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/証明書に基づいてネットワークにアクセスできるユーザー。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。

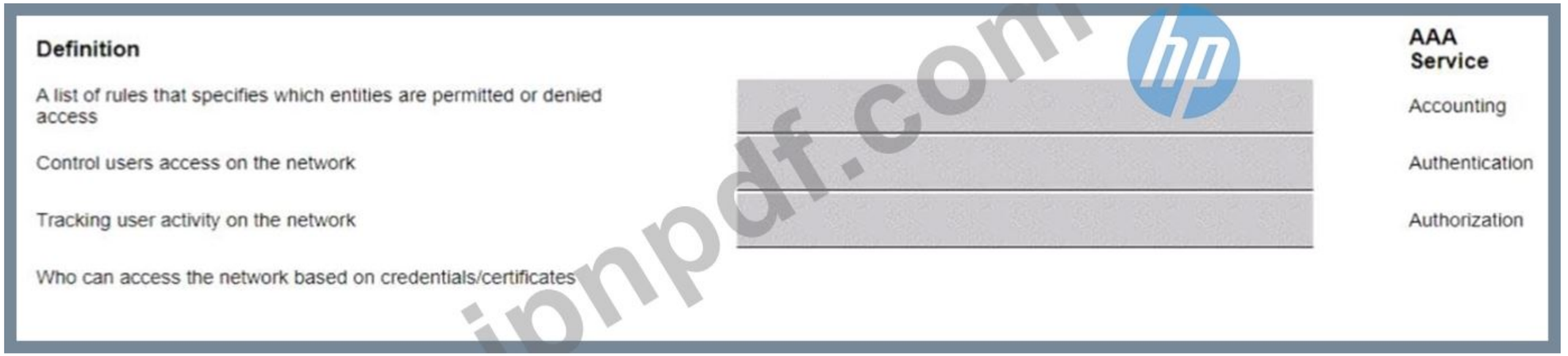
最新問題**: 4**
どのプロトコル データ ユニット (PDU) がデータ リンク層 PDU を表しますか?
**A.** PDU1 - 信号
**B.** PDU2 - フレーム
**C.** PDU3 - パケット
**D.** PDU4 - セグメント
**Answer: B (**メーッセージを残す**)**
フレームは、送信元および宛先 MAC アドレス、フレーム タイプ、エラー検出などの情報を含むヘッダーとトレーラーを使用してネットワーク層 PDU (パケット) をカプセル化するデータ リンク層 PDU です。フレームは、イーサネット、Wi-Fi などの物理メディアを介して送信されます。
参考資料: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos- solutions/1-ov

最新問題**: 5**
正しく起動できない Aruba CX 6200 4 ノード VSF スタック スイッチのトラブルシューティングを行う必要があります。スイッチにアクセスして、OS イメージと ServiceOS で使用可能な起動オプションを確認できるオプションを選択します。
**A.** メンバー 2 RJ-45 コンソール ポート
**B.** メンバー2スイッチ管理ポート
**C.** コンダクターUSB-Cコンソールポート

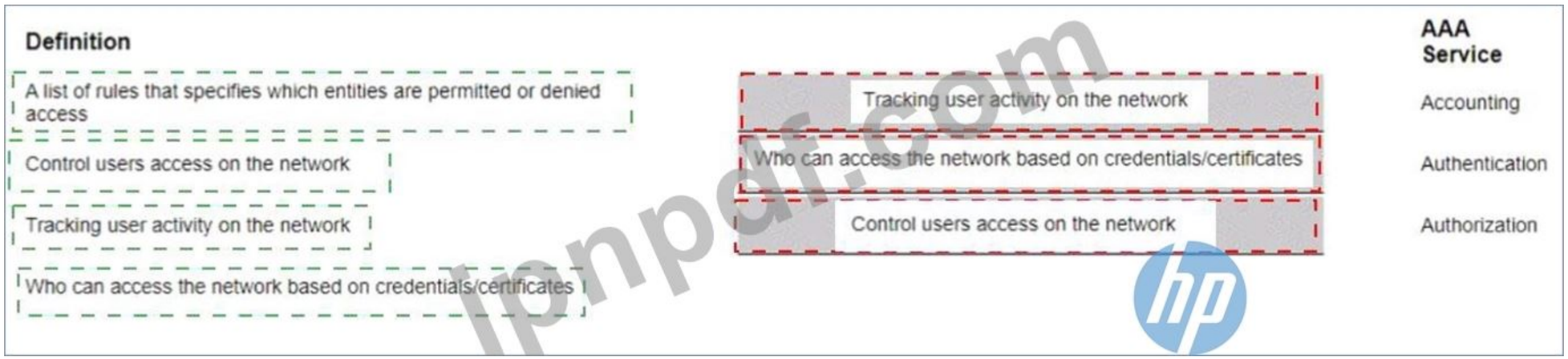
**D.** SSH を使用した Conductor 管理ポート
**Answer: C (**メーッセージを残す**)**
説明
スイッチにアクセスし、OS イメージと ServiceOS で使用可能なブート オプションを確認できるオプションは、Conductor USB-C コンソール ポートです。このオプションでは、AOS-CX とは独立して Aruba CX スイッチで実行されるオペレーティング システムである ServiceOS に直接アクセスできます。Aruba Operating System CX (AOS-CX) は、Aruba CX スイッチで実行されるオペレーティング システムです。ServiceOS は、ブート、ファームウェア アップグレード、パスワード回復、ハードウェア診断、スイッチ スタッキング、システム回復などの低レベルの機能を提供します。ServiceOS には、次の 2 つの方法のいずれかでアクセスできます。
Conductor USB-C コンソール ポート: この方法では、USB-C ケーブルを使用して、PC またはラップトップを VSF スタック内の任意のメンバー スイッチの USB-C コンソール ポートに接続できます。この方法では、AOS-CX での構成や認証を必要とせずに、ServiceOS に直接アクセスできます。
AOS-CX CLI: この方法では、SSH または Telnet プロトコルを使用して AOS-CX CLI 経由で ServiceOS にアクセスできます。この方法では、AOS-CX で IP アドレスを設定し、ユーザー名とパスワードで認証する必要があります。
OS イメージと ServiceOS で使用可能なブート オプションを表示するには、Conductor USB-C コンソール ポートを介して ServiceOS にアクセスし、ServiceOS プロンプトでブート メニュー コマンドを入力する必要があります。
他のオプションでは、次の理由により、スイッチにアクセスして OS イメージおよび ServiceOS で使用可能なブート オプションを確認することはできません。
メンバー 2 RJ-45 コンソール ポート: このオプションを使用すると、RJ-45 ケーブルを使用して、VSF スタック内の任意のメンバー スイッチの RJ-45 コンソール ポートに PC またはラップトップを接続できます。このオプションでは、ServiceOS ではなく AOS-CX CLI に直接アクセスできます。
メンバー 2 スイッチ管理ポート: このオプションを使用すると、イーサネット ケーブルを使用して、PC またはラップトップを VSF スタック内の任意のメンバー スイッチのスイッチ管理ポートに接続できます。このオプションでは、ServiceOS ではなく、SSH または Telnet プロトコルを介して AOS-CX CLI に間接的にアクセスできます。
SSH を使用したコンダクタ管理ポート: このオプションを使用すると、イーサネット ケーブルを使用して、PC またはラップトップを VSF スタック内の任意のメンバー スイッチの管理ポートに接続できます。このオプションは、ServiceOS ではなく SSH プロトコルを介して AOS-CX CLI への間接アクセスを提供します。
参考文献:
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/serviceos/serviceos-overv
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/serviceos/access-serviceo
https://www.arubanetworks.com/techdocs/AOS-CX_10_08/NOSCG/Content/cx-noscg/serviceos/boot-menu.htm

最新問題**: 6**
ネットワーク技術者は、キャプティブ ポータルを完了した後、顧客がゲスト ネットワークに正常に接続したかどうかを確認しています。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
**Answer: (**解答を表示する**)**
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、OUTPUT タブに 「ゲストが認証されました」など、ユーザーが認証されたことを示すロールが表示されます。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。

最新問題**: 7**
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)




**Answer:**




説明

AAA 認証、許可、アカウンティング (AAA) 認証、許可、アカウンティング (AAA) は、ネットワーク アクセス制御のセキュリティ 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。

承認: 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。承認では、ACL、RBAC、MAC、DAC などの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 などのさまざまな形式を使用できます。

サービス。これが私の答えです:

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。

アカウンティング: 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 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、着信や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、承認ではなく認証の定義です。承認とは、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: 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

最新問題: **8**
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
**Answer: B,E (**メーッセージを残す**)**
説明
のみ: デイジー チェーンと MAD およびリングの組み合わせは、Aruba スイッチに推奨される VSF トポロジです。これらは、VSF スタックに高い可用性と冗長性を提供します。MAD (Multiple Active Detection) は、VSF スタック内のスプリット ブレイン シナリオを検出して解決するメカニズムです。
参考資料:https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6790/GUID-D6EF042E-EEE

最新問題: **9**
UXI の利点を 2 つ挙げてください。(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。
**Answer: C,E (**メーッセージを残す**)**
説明
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、遅延、ジッター、パケット損失、スループットなどのメトリックを測定できます。
参考資料:https://www.arubanetworks.com/products/networking/user-experience-insight/

最新問題: **10**
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、クライアントに同じ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、クライアントに同じスループットを提供します。
**D.** 5GHz チャネルは 6GHz チャネルと比較して移動距離が異なり、クライアントに提供するスループットも異なります。
**Answer: (**解答を表示する**)**

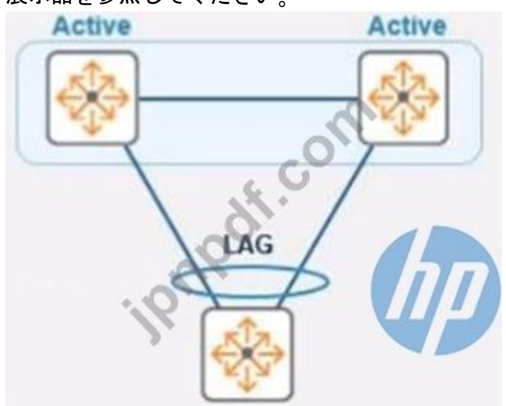
最新問題: **11**

SVI を使用したインバンド管理が使用されている場合、Aruba CX スイッチでデフォルト ルートを 10.4.5.1 に設定するにはどのコマンドを使用しますか?
**A.** iP デフォルトゲートウェイ 10.4.5.1
**B.** ip ルート 0 0 0.070 10.4 5.1 vrf 管理
**C.** IPルート0.0 0 0/0 10.4.5.1
**D.** デフォルトゲートウェイ 10.4.5.1
**Answer: C (メーッセージを残す)**
説明
SVI を使用したインバンド管理が使用されている場合に、Aruba CX スイッチでデフォルト ルートを 10.4.5.1 に設定するために使用されるコマンドは、ip route 0.0 0 0/0 10.4.5.1 です。このコマンドは、スイッチに直接接続されていないネットワークに到達するための宛先ネットワーク アドレス (0.0 0 0)、プレフィックス長 (/0)、およびネクストホップ アドレス (10.4.5.1) を指定します。デフォルト ルートは、デフォルトの VRF 仮想ルーティングおよび転送に適用されます。
VRF は、ルーティング テーブルの複数のインスタンスを同じルータ内で同時に共存できるようにするテクノロジです。VRF は通常、セキュリティ、プライバシー、または管理上の目的でネットワーク トラフィックをセグメント化するために使用されます。これは、SVI スイッチ仮想インターフェイスを通過するインバンド管理トラフィックに使用されます。
SVIはスイッチ上の仮想インターフェイスであり、スイッチが同じスイッチ上の異なるVLAN間またはトランクリンクで接続された異なるスイッチ間でパケットをルーティングできるようにします。SVIはVLANに関連付けられており、IPアドレスとサブネットマスクが割り当てられています。
https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i-6000-6100-6200/Content/Ch
2
https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i-6000-6100-6200/Content/Ch

最新問題**: 12**
顧客との会議で、ネットワーク冗長機能である Multiple Spanning Tree (MSTP) について説明するよう求められています。この機能に関する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.** MSTP 構成 ID リビジョンはデフォルトでスイッチのシリアル番号として使用されます。
**Answer: B (メーッセージを残す)**
説明
MSTP マルチスパニングツリープロトコル。MSTP は、複数の VLAN を持つネットワークで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、
MSTP リージョンを識別する 32 バイトの ASCII 文字列。MSTP リージョンは、同じ構成 ID と VLAN からインスタンスへのマッピングを共有するスイッチのグループです。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。これは、スイッチの 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 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、ネットワーク セグメント内の通信でネットワーク アドレスとして使用されます。
参考資料:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mstp/

最新問題**: 13**
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ています。
この機能の正しい説明は何ですか?
**A.** VRRPはメッセージングにBPDUを使用する
**B.** VRRPはメッセージングにマルチキャストを使用する
**C.** VRRPはメッセージングにユニキャストを使用する
**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

**Answer: B (メーッセージを残す)**
仮想ルータ冗長プロトコル (VRRP) は、参加ホストに利用可能なインターネット プロトコル (IP) ルータを自動的に割り当てるネットワーク プロトコルです。VRRP は、マスターの選択プロセスと仮想 IP アドレスの通知のために、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。

最新問題: **14**
展示品を参照してください。


指定されたトポロジでは、アクティブ ゲートウェイを使用する VSX スタックに Aruba CX 8325 スイッチのペアが存在します。クライアントが VSX をデフォルト ゲートウェイとして使用してアクセス スイッチに接続されている場合、VSX ペアの仮想 IP の性質と動作はどのようなものですか。
**A.** プライマリVSXスイッチで仮想IPがアクティブです
**B.** 障害が発生した場合、仮想フローティングIPはフェイルオーバーします
**C.** 両方のCXスイッチで仮想IPがアクティブです
**D.** 仮想IPはVSXと同期されたSVI IPアドレスを使用します
**Answer: (**解答を表示する**)**
仮想スイッチング拡張 (VSX) スタックでは、仮想 IP (VIP) は、アクセス スイッチに接続されたクライアントに単一のデフォルト ゲートウェイ IP アドレスを提供します。この VIP は、プライマリ VSX スイッチでアクティブなフローティング IP です。プライマリ スイッチに障害が発生した場合、VIP はセカンダリ スイッチにフェールオーバーし、クライアント トラフィックが中断することなくルーティングされ続けるようにします。

最新問題: **15**
AruDaCX 8400 の「show ip route」出力に基づきます。「10.1 20 0/24、vrf default via 10.1.12.2. [1/0]」はどのようなタイプのルートですか?
**A.** ローカル
**B.** 静的
**C.** OSPF
**D.** 接続済み
**Answer: B (**メーッセージを残す**)**
スタティック ルートは、ルータまたはスイッチ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にトラフィックが到達する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、スタティック ルートの一般的な値であるため、スタティック ルートです。参考: https://en.wikipedia.org/wiki/Static_routing https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/show-ip-route.htm

最新問題: **16**
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ました。スタッキングモードが選択されていません。
**C.** スタッキングを同期しています。お待ちください
**D.** スタッキングモードが選択されました
**Answer: A** (メーッセージを残す)



最新問題: **17**
ユースケースを適切な認証技術に合わせてください

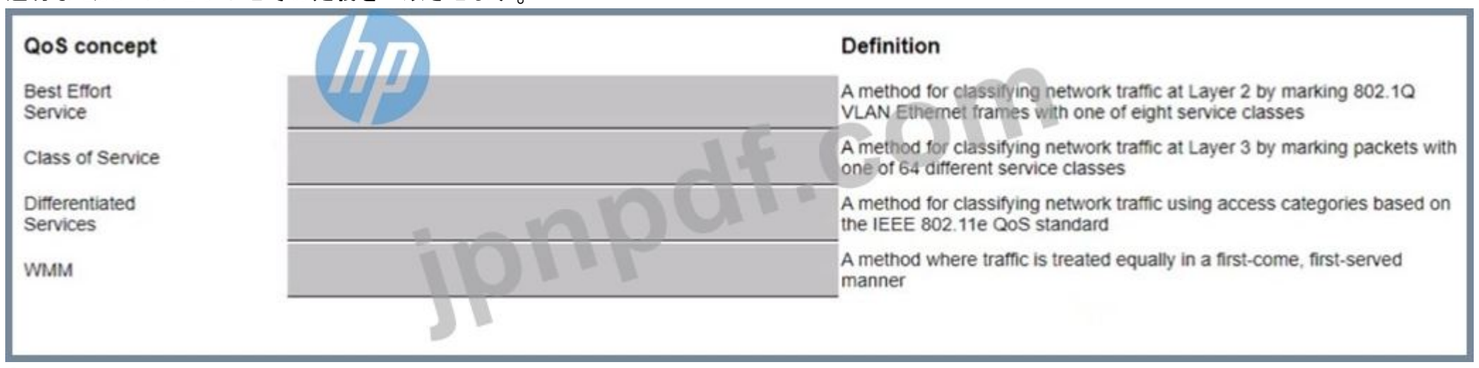

**Answer:**


最新問題: **18**
ノイズフロアは 000000001 ミリワットで、受信機の信号強度は -65dBm です。信号対雑音比とは何ですか?
**A.** 35 dBm
**B.** 15 dBm
**C.** 45dBm
**D.** 25 dBm
**Answer:** (解答を表示する)
信号対雑音比 (SNR) は、目的の信号のレベルを背景雑音のレベルと比較する尺度です。SNR は信号電力と雑音電力の比として定義され、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、信号が雑音によって破損または不明瞭になっており、識別や復元が困難な場合があることを意味します3。SNR を dB で計算するには、次の式を使用します。

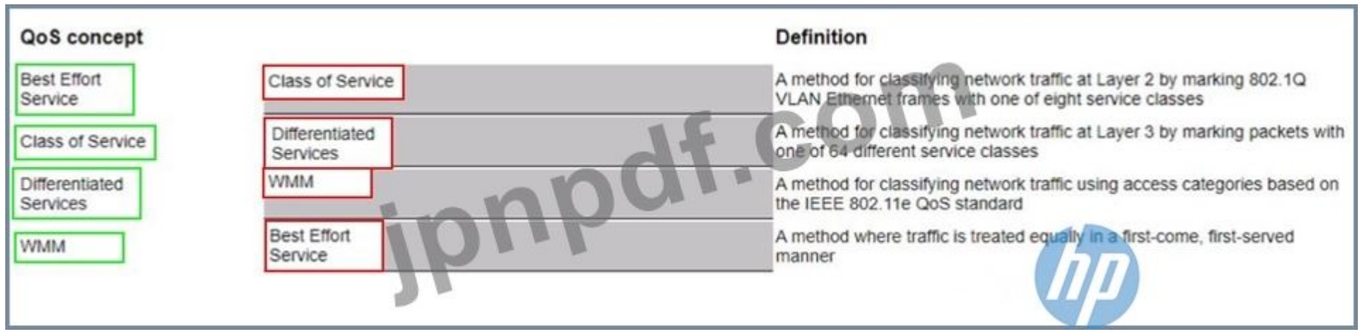
SNR (dB) = 信号電力 (dBm) - ノイズ電力 (dBm)
この問題では、ノイズ フロアが -90 dBm (0.000000001 ミリワット)、受信機の信号強度が -65 dBm (0.000316 ミリワット) であることが示されています。したがって、これらの値を式に代入すると、次のようになります。
SNR (dB) = -65 dBm - (-90 dBm) SNR (dB) = -65 dBm + 90 dBm SNR (dB) = 25 dBm したがって、正解は SNR が 25 dBm であるということです。

最新問題**: 19**
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.** .01 メガワット
**C.** 10mW
**D.** 1mW
**Answer: B (**メーッセージを残す**)**
dBm は、特定の電力レベルと 1 mW の比率を測定する電力単位です。dBm を mW に変換する式は、P(mW) = 1mW * 10^(P(dBm)/10) です。したがって、-20 dBm は 0.01 mW に相当し、次のようになります。P(mW) = 1mW * 10^(-20/10) = 0.01 mW 参照: https://www.rapidtables.com/convert/power/dBm_to_mW.html

最新問題**: 20**
適切な QoS コンセプトとその定義を一致させます。




**Answer:**




最新問題**: 21**

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。
接続が成功することを確認するには、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
**Answer: (**解答を表示する**)**
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る必要がある RADIUS メッセージは、Access-Accept です。このメッセージは、RADIUS サーバーがサプリカント (ネットワークへのアクセスを希望するデバイス) を認証および承認し、ネットワーク リソースへのアクセスを許可したことを示します。Access-Accept メッセージには、認証者 (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処理する方法を指定する VLAN ID、セッション タイムアウト、またはフィルタ ID などの追加属性も含まれる場合があります。
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通過できることを示す状態です。
- 成功: これは RADIUS メッセージではありませんが、EAP 拡張認証プロトコル (EAP) は、パスワード、証明書、トークン、生体認証など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 ネットワークおよび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。サプリカントと認証サーバーの間で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#Access-Accept
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/Extensible_Authentication_Protocol#EAP_exchange

最新問題**: 22**
Aruba Central を使用する場合、ネットワークの健全性の問題を解決するための推奨手順を特定し、サポート担当者と詳細情報を共有できるのは何ですか?
**A.** 概要ダッシュボード
**B.** OAIOps
**C.** アラートとイベント
**D.** 監査証跡
**Answer: (**解答を表示する**)**
OAIOps は、人工知能と機械学習を使用してネットワークの健全性の問題を解決するための推奨手順を特定し、サポート担当者と詳細情報を共有できるようにする Aruba Central の機能です。OAIOps は、ネットワーク パフォーマンス、根本原因分析、異常検出、プロアクティブなアラート、自動修復アクションに関する洞察を提供します。また、OAIOps は Aruba User Experience Insight (UXI) センサーと統合して、有線および無線ネットワーク全体のユーザー エクスペリエンスを測定および改善します。参照: https://www.arubanetworks.com/assets/ds/DS_ArubaCentral.pdf

最新問題**: 23**
要求どおりにエッジ スイッチ アップリンクを構成した後、同僚からコアへの ping に失敗したと言われました。同僚に、接続が差し込まれ、スイッチの電源がオンになっていることを確認するように依頼しました。同僚は、両方とも正しいことを確認しました。コア スイッチへの ping を試行し、ping が失敗していることを確認しました。
この展開の性質を理解した上で、この問題のトラブルシューティングにどのようなコマンドを使用すればよいでしょうか？
**A.** ping 10.11 1 - コアに ping を実行して接続を確認します。トランクの表示 - LAG インターフェイスがスイッチに正しく追加されたかどうかを確認します。スパニング ツリーの表示 - スパニング ツリーのブロック状態を確認します。ポート アクセス クライアント インターフェイスのすべてを表示します - すべてのインターフェイスでポート アクセスのブロック状態または失敗した認証試行を表示します。実行インターフェイス vlan20 の表示 - レイヤー 3 svi 構成が l_3 接続に対して正しいかどうかを再確認します。lldp ネイバーの表示 - コアを L2 ネイバーとして表示できるかどうかを確認し、正しいリンクが正しいポートに接続されているかどうかを確認します。

**B.** 診断 diag ケーブル ディアグ 1/1/51 diag ケーブル ディアグ 1/1/52 - 物理リンクの診断情報を表示して、レイヤー 1 接続の中断のステータスを取得します。show ip route - デフォルト ゲートウェイがルーティング テーブルに存在することを確認します。show ip ospf - レイヤー 3 ルーティング プロトコルが有効になっているかどうかを確認します。show ip dns - 有効な DNS ソースがあるかどうかを表示します。
**C.** 10.1.1.1 の ping - コアに ping を実行して接続を確認します。show lacp agg - どのリンク アグリゲーションがどの物理ポートを使用して現在設定されているかを確認します。show lacp int - LACP ステータスと、トポロジ内でブロックされているリンクがあるかどうかを確認します。show lldp neighors - コアを L2 ネイバーとして表示できるかどうかを確認し、正しいリンクが正しいポートに接続されているかどうかを確認します。show run interface 1/1/51.1/1/52 - 物理インターフェイスが no-shut であり、lag のメンバーであることを確認します。show run interface lag 1 - 論理インターフェイスに正しい VLAN トランキング設定が適用されていることを確認します。show run int vlan 20 - L3 SVI が no shut であり、正しいサブネットに設定されていることを確認します。
**D.** Show run - スイッチの実行中の設定を表示します。Show run | begin 20 "vlan 20" - VLAN 20 がデータベースに正しく追加されたことを確認します。show run | begin 20 'interface vlan 20' - L3 SVI 設定を表示します。Show run interface 1/1/51.1/1/52 - 物理インターフェイスが no shut であり、LAG 1 のメンバーとして追加されたことを確認します。Show run int lag 1 - LACP ブロッキング状態を排除するために LACP モード アクティブが設定されたことを確認します。
**Answer: (**解答を表示する**)**
これらのコマンドは、レイヤー 3 の到達可能性、レイヤー 2 の隣接関係、LACP の構成とステータス、VLAN トランキングの構成、インターフェイスのステータスなど、エッジ スイッチとコア スイッチ間の接続のさまざまな側面をチェックするため、この問題のトラブルシューティングに役立つ可能性があります。参考: https://www.arubanetworks.com/techdocs/AOS-CX_10_04/CLI/GUID-8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

最新問題**: 24**
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して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
**Answer: A (**メッセージを残す**)**
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すべてのタイプのアラートとイベントが表示されます。構成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 のアラートと通知を構成できます。また、リスト ビューと概要ビュー2 でアラートとイベントを表示することもできます。
参考文献:
1 https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/cconfiguring-alerts.htm
2 https://www.arubanetworks.com/techdocs/central/latest/content/nms/alerts/viewing-alerts.htm

最新問題**: 25**
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
**Answer: C (**メッセージを残す**)**
AirMatch は、Aruba ワイヤレス ネットワークの集中 RF 計画および最適化サービスを提供する機能です。クラウドベースのアルゴリズムと機械学習を使用して、RF パフォーマンスとユーザー エクスペリエンスを最適化します。
参考資料: https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdf

最新問題**: 26**
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。

**EDGE1# TROUBLESHOOTING - SHOW COMMANDS OUTPUT**

```
EDGE1# show span vlan 20
Port          Role           State
    TCN-Tx      TCN-Rx
------------ -------------- ----------
--- ---------- ----------
lag1          Disabled       Blocking
    2           2
EDGE1# show run int 1/1/51
interface 1/1/51
    no shutdown
    description Uplink_To_Core1
    lag 1
    exit
EDGE1# show run int 1/1/52
interface 1/1/52
    no shutdown
    description Uplink_To_Core1
    lag 1
    exit
EDGE1# show run int lag1
interface lag 1
    no shutdown
    no routing
    vlan trunk native 20
    vlan trunk allowed all
    lacp mode active
    exit
EDGE1# show lacp int
Actor details of all interfaces:
-------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
-------------------------------------------------------------------------------
1/1/51     lag1       52    1     ALFOE   b8:d4:e7:b5:22:80 65534  1    lacp-block
1/1/52     lag1       53    1     ALFOE   b8:d4:e7:b5:22:80 65534  1    lacp-block
```

**CORE1# TROUBLESHOOTING - SHOW COMMANDS OUTPUT**

```
CORE1# show span vlan 20
Port          Role           State
Rx    TCN-Tx      TCN-Rx
------------ -------------- ----------
----- ---------- ----------
lag1          Designated     Forwarding
    2           2

CORE1# show run int 1/1/51
interface 1/1/51
    no shutdown
    lag 1
    exit
CORE1# show run int 1/1/52
interface 1/1/52
    no shutdown
    lag 1
    exit
CORE1# show run int lag 1
interface lag 1
    no shutdown
    no routing
    vlan trunk native 20
    vlan trunk allowed all
    exit
CORE1# show lacp int
Actor details of all interfaces:
```

CORE1# show lacp int

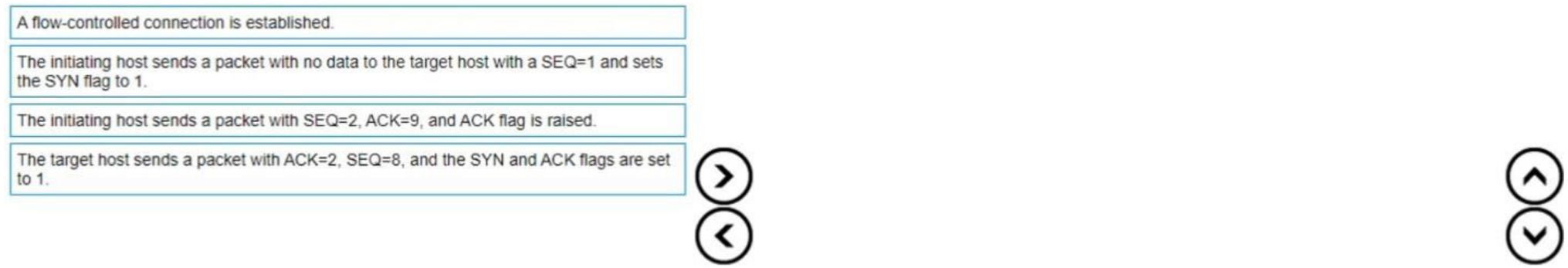
Actor details of all interfaces:

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

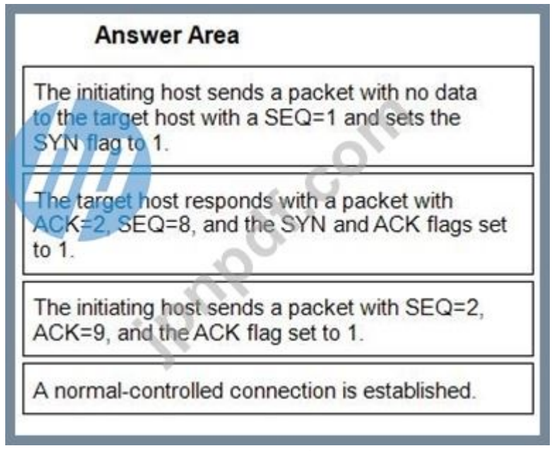


**A.** 物理インターフェースが正しい LAG のメンバーではありません。
**B.** スパニングツリーのブロック状態により、コアアップリンクがエッジに接続できなくなっています
**C.** コアが間違った物理インターレースに接続されています
**D.** コアアップリンクにLACPが設定されていません
**Answer: D** (メーッセージを残す)
説明
LACP は、複数の物理リンクを 1 つの論理リンクに集約して帯域幅と冗長性を向上させるプロトコルです。LACP が適切に機能するには、リンクの両端で設定する必要があります。この場合、EDGE1 のアップリンク ポート チャネル 1 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、リンクが起動できなくなります。
参考資料:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-ove

最新問題: **27**
TCP 3ウェイハンドシェイクシーケンスの正しい順序は何ですか?

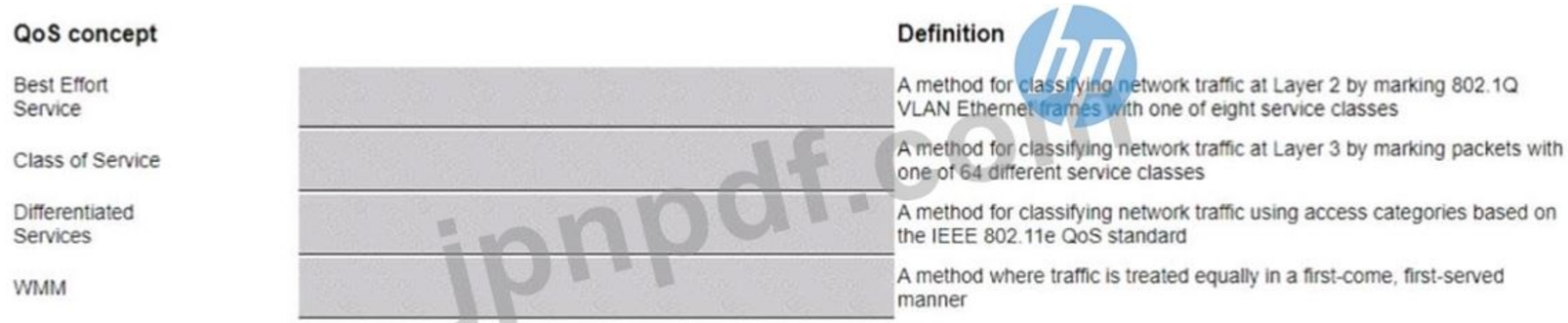



**Answer:**

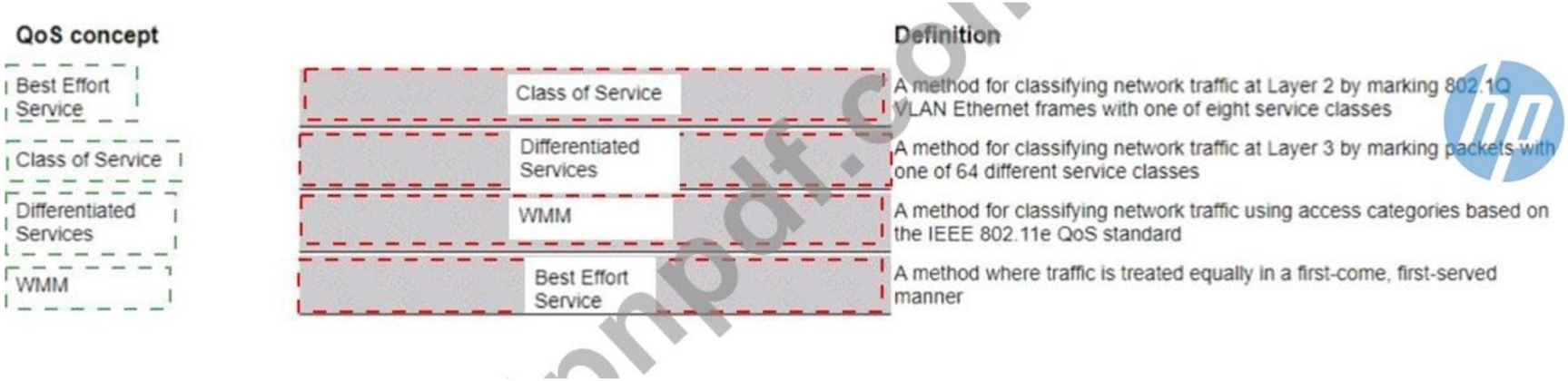



1 - 開始ホストは、SEQ=1 でデータなしのパケットをターゲット ホストに送信し、SYN フラグを 1 に設定します。
2 - ターゲット ホストは、ACK=2、SEQ=8、SYN および ACK フラグが 1 に設定されたパケットで応答します。
3 - 開始ホストは、SEQ=2、ACK=9、ACK フラグが 1 に設定されたパケットを送信します。
4 - 通常制御の接続が確立されます。

最新問題: **28**
適切な QoS コンセプトとその定義を一致させます。




**Answer:**




説明

QoS サービス品質 (QoS) は、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さまざまなレベルのサービスを提供する一連の技術です。QoS により、ネットワーク パフォーマンスが向上し、待ち時間が短縮され、スループットが増加し、輻輳が防止されます。概念とその定義。これが私の答えです。

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で平等に扱われる方法 a) 802.1Q VLAN イーサネット フレームを 8 つのサービス クラスのいずれかで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) パケットを 64 の異なるサービス クラスのいずれかで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、トラフィックが優先順位付けや差別化なしに先着順で平等に処理される方法です。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およびアプリケーションのデフォルトのサービス レベルです。ベスト エフォート サービスでは、帯域幅、遅延、ジッター、パケット損失は保証されません。

サービスクラス: これは、802.1Q VLANイーサネットフレームを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、レイヤー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。

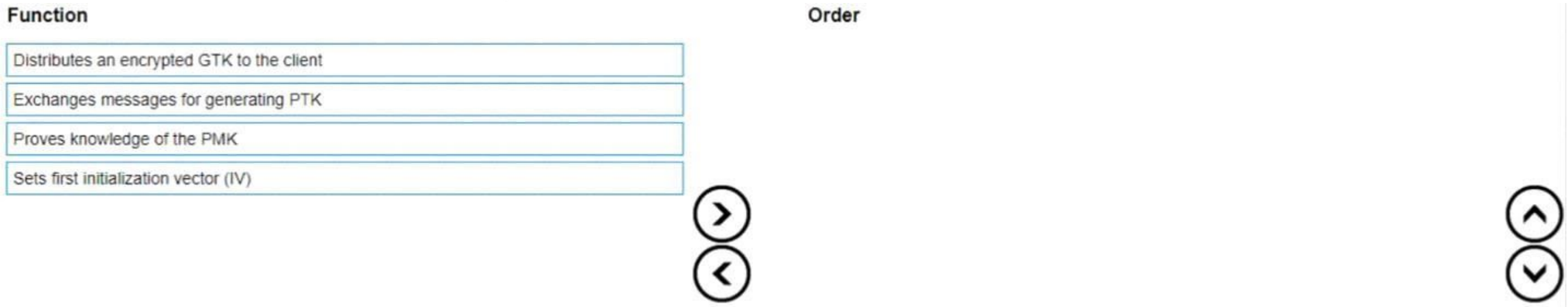
802.1p の優先度値または PCP 優先度コード ポイント (PCP) は、802.1Q VLAN タグ内の 3 ビット フィールドで、イーサネット フレームの優先度レベルを示します。サービス クラスにより、ネットワーク デバイスは優先度レベルに基づいてさまざまな種類のトラフィックを識別して処理できます。サービス クラスは通常、LAN で使用されます。ローカル エリア ネットワーク (LAN) は、家庭、オフィス、建物などの限られた地理的領域内でデバイスを接続するネットワークで、レイヤ 2 スイッチングが主流です。
差別化サービス: これは、64 の異なるサービス クラス (0 ～ 63) のいずれかを使用して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、パケットのサービス クラスを示す IP ヘッダー内の 6 ビット フィールドです。差別化サービスにより、ネットワーク デバイスはサービス クラスに基づいてさまざまな種類のトラフィックを識別して処理できます。差別化サービスは、通常、WAN で使用されます。ワイド エリア ネットワーク (WAN) は、国や大陸などの広い地理的領域にわたってデバイスを接続するネットワークで、レイヤー 3 ルーティングが主流の環境です。
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 標準。WMM は Wi-Fi Multimedia の略で、ワイヤレス ネットワークの QoS を強化するために Wi-Fi Alliance によって開発された認定プログラムです。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、ワイヤレス トラフィックのさまざまな優先度レベルと競合パラメータに対応しています。WMM を使用すると、ワイヤレス デバイスはアクセス カテゴリに基づいてさまざまな種類のトラフィックを識別して処理できます。
参考: 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-dfsr
https://www.cisco.com/c/en/us/support/docs/wireless-Mobility/wireless-lan-wlan/81831-qos-wlan.html
https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm

最新問題**: 29**
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。
**Answer: C (**メッセージを残す**)**
Aruba CX 6300M スイッチでは、スイッチ仮想インターフェイス (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。

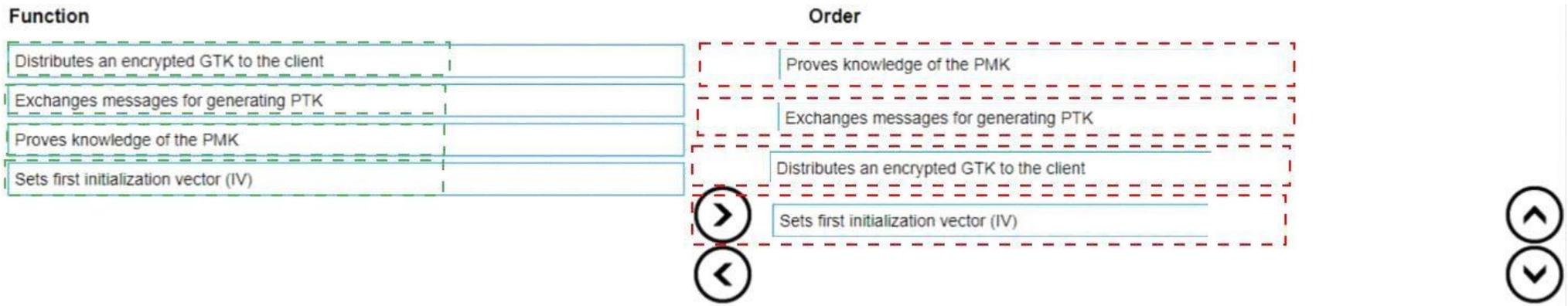
最新問題**: 30**
配布ラックあたり 200 ～ 380 台のクライアント、プリンター、AP にコスト効率よく接続するための理想的な Aruba アクセス スイッチは何ですか?
**A.** アルバ CX 6400
**B.** アルバ CX 6200
**C.** アルバ CX 6300
**D.** アルバ CX 6000
**Answer: B (**メッセージを残す**)**
説明
ディストリビューション ラックあたり 200 ～ 380 台のクライアント、プリンター、AP へのコスト効率の高い接続に最適な Aruba アクセス スイッチは、Aruba CX 6200 です。このスイッチ シリーズは、クラウド管理可能でスタック可能なアクセス スイッチ シリーズであり、企業のブランチ オフィスやキャンパス ネットワーク、および SMB に最適です。CX 6200 シリーズには、次の利点があります。
エンタープライズクラスの接続: CX 6200 シリーズは、ACL、堅牢な QoS、静的ルーティングやアクセス OSPF ルーティングなどの一般的なプロトコルをサポートします。
ユーザーとIoTのためのパワーとスピード :CX 6200シリーズは、1/10GbEアップリンクと30Wを内蔵し、
AP やカメラなどのデバイスに電力を供給するためのクラス 4 ～ クラス 6 PoE の 60W。

スケーラブルな拡張が簡単に: CX 6200 シリーズは、高性能の内蔵 10G SFP ポートを使用して、単一スタックでネットワークを 8 つのメンバーに迅速に拡張できる Aruba Virtual Switching Framework (VSF) をサポートしています。
管理の柔軟性: CX 6200 シリーズは、クラウドベースおよびオンプレミスの Central、CLI、スイッチ Web GUI、AOS-CX オペレーティング システムによるプログラミング機能、REST API などの管理の選択肢をサポートします。
他のオプションは、次の理由から理想的ではありません。
Aruba CX 6400: このスイッチ シリーズは、データ センター展開への多目的エッジ アクセスに最適な高可用性モジュラー スイッチ シリーズです。CX 6200 シリーズよりも優れたパフォーマンス、拡張性、モジュール性を備えていますが、展開と管理がより高価で複雑です。分散ラックごとに 200 ～ 380 のクライアントを接続する場合、コスト効率が良くない可能性があります。
Aruba CX 6300: このスイッチ シリーズは、スマート レートと高出力 PoE を提供するレイヤー 3 スタッカブル アクセスおよびアグリゲーション スイッチ シリーズです。CX 6200 シリーズよりも多くの機能とパフォーマンスを提供しますが、価格も高く、分散ラックごとに 200 ～ 380 のクライアントを接続するのには必要ない場合もあります。
Aruba CX 6000: このスイッチ シリーズは、PoE を提供するレイヤー 2 アクセス スイッチ シリーズです。CX 6200 シリーズよりも機能とパフォーマンスが低く、VSF スタッキングやルーティング プロトコルをサポートしていません。分散ラックごとに 200 ～ 380 のクライアントを接続するには不十分な場合があります。
参考資料: https://www.arubanetworks.com/products/switches/access/
https://www.arubanetworks.com/products/switches/access/6200-series/
https://www.arubanetworks.com/products/switches/access/6400-series/
https://www.arubanetworks.com/products/switches/access/6300-series/
https://www.arubanetworks.com/products/switches/access/6000-series/

最新問題: **31**
WPA 4 ウェイ ハンドシェイク機能を正しい順序でリストします。




**Answer:**




PMKに関する知識を証明する
PTKを生成するためのメッセージを交換する
暗号化されたGTKをクライアントに配布する
最初の初期化ベクトル (IV) を設定する



最新問題: **32**
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。
**Answer: C,D** (メーッセージを残す)
ClearPass OnGuard は、ClearPass Policy Manager のコンポーネントであり、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実行して、デバイスの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。

最新問題: **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ーはどれですか?
**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

**Answer: (**解答を表示する**)**
Aruba AirMatch は、RF 無線周波数を最適化する機能です。RF は、電波伝搬に関連する電磁スペクトル内の任意の周波数です。RF 電流がアンテナに供給されると、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。
参考文献:
https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdf https://www.arubanetworks.com/techdocs/Ar ubaOS

最新問題**: 34**
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.** PEAP
**Answer: B (**メーッセージを残す**)**
EAP-TLS は、ネットワークへの認証時にクライアント証明書を必要とする認証方法です。
公開鍵暗号化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

最新問題**: 35**
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
**Answer: (**解答を表示する**)**
スタック LED がゆっくりとオレンジ色に点滅している場合は、スイッチでスタッキング モードが選択されていることを示します。これは、スイッチがスタックに参加する準備ができているか、他のスイッチが存在しない場合は新しいスタックを形成する準備ができていることを意味します。参照: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/stacking-leds.htm

最新問題**: 36**
IP 通信に関連するエラー情報や動作情報を送信するためにネットワーク デバイスが使用するものは何ですか?
**A.** フレームチェックシーケンス (FCS)
**B.** ユーザー データグラム プロトコル (UDP)
**C.** 巡回冗長検査 (CRC)
**D.** インターネット制御メッセージ プロトコル (ICMP)
**Answer: D (**メーッセージを残す**)**
ICMP (インターネット制御メッセージプロトコル) は、ネットワークデバイスが IP 通信に関連するエラーや動作情報を送信するために使用されます。IP 通信に問題がある場合に、 宛先に到達できません」や 時間超過」などのメッセージを送信するために使用されます。

最新問題: **37**
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何が起こりますか?
**A.** APは結合チャネルを使用してクライアントへの遅延を減らします
**B.** 信号対雑音比 ($SNR) が増加する
**C.** 信号対雑音比 ($SNR) が減少する
**D.** Aruba Centralはクライアントを近隣のAPに動的に移動します
**Answer: C (**メーッセージを残す**)**
説明
信号対雑音比 (SNR) は、目的の信号のレベルを背景雑音のレベルと比較する尺度です。SNR は、信号電力と雑音電力の比として定義され、多くの場合デシベル (dB) で表されます。SNR が高いということは、信号が明瞭で検出や解釈が容易であることを意味します。一方、SNR が低いということは、信号が雑音によって破損または不明瞭になっており、識別や回復が困難な場合があることを意味します1。AP アクセス ポイントからの信号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、ワイヤレス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 やデバイスなどの他のソースからの干渉によって増加する場合もあります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/信号対雑音比 2
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_%28SNR%29

最新問題: **38**
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 shut」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アドレスの小さいスイッチは両方のポートで転送し、MACアドレスの大き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アドレスの小さいスイッチは1つのポートで破棄し、MACアドレスの大き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。
**Answer:** (解答を表示する**)**
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 ネットワークのループのないトポロジを保証するネットワーク プロトコルです。
STP は、拡張ネットワーク内のすべてのスイッチにまたがる論理ツリー構造を作成し、ツリーの一部ではない冗長リンクがデータ パケットを転送するのをブロックします3。
これらのポートでトラフィックを転送または破棄する方法は次のとおりです。
- STP は、優先順位値と MAC アドレスで構成されるブリッジ ID に基づいて、2 つのスイッチの中からルート ブリッジを選択します。ブリッジ ID が低いスイッチがルート ブリッジになり、すべてのポートでトラフィックを転送します。
- STP は、優先順位値とポート番号で構成されるポート ID に基づいて、両方のスイッチの各ポートに役割と状態を割り当てます。ポート ID が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、それらの間のパスは 2 つ存在し、ループが発生します。このループを防ぐために、STP は各スイッチのポートの 1 つでトラフィックを破棄して、これらのパスの 1 つをブロックします。
- 両方のスイッチの優先度の値が同じ (デフォルトは 32768) であると仮定すると、MAC アドレスが低いスイッチのブリッジ ID が低くなり、ルート ブリッジになります。ルート ブリッジは、ポート 1/1/1 と 1/1/2 の両方でトラフィックを転送します。
- 両方のポートの優先度の値が同じ (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、両方のスイッチでポート 1/1/2 よりもポート ID が低くなります。ポート 1/1/1 は指定ポートになり、トラフィックを転送しますが、ポート 1/1/2 は代替ポートになり、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

最新問題: **39**
ディストリビューションおよびレイヤー 3 サービスに使用される 6300M スイッチのスタック ペア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。これに類似した複数の VLAN/サブネットを作成し、複数のアクセス スタックで使用します。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イスを構成する正しい方法は何ですか。
**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。
**Answer:** (解答を表示する)
この VLAN に関連付けられるサブネットのルーティング可能なインターフェイスを正しく設定するには、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 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 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 (例: vlan 10) に従って番号が付けられ、VLAN のサブネット内で IP アドレスが割り当てられます。SVI は、interface vlan、ip address、no shut down 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、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。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 内のユーザーのゲートウェイとして機能し、異なるサブネット間の VLAN 間ルーティングが可能になります。また、6300M スタックのサブネットに SVI を作成すると、ルーティングに必要な物理インターフェイスとケーブルの数が減り、ネットワークの設計と管理が簡素化されます。
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。
- ダウンストリーム スイッチごとに 6300M スタック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。このオプションは正しくありません。ダウンストリーム スイッチごとに 6300M スタックのサブネットに物理的にルーティングされたインターフェイスを作成すると、ダウンストリーム スイッチごとに 1 つの物理ポートとケーブルを使用する必要があり、インターフェイス リソースが消費され、ケーブル コストが増加します。また、ダウンストリーム スイッチごとに 6300M スタックのサブネットに物理的にルーティングされたインターフェイスを作成すると、インターフェイスごとに個別のルーティング設定とポリシーが必要になるため、ネットワークの設計と管理が複雑になります。
- 各ダウンストリーム スイッチのサブネットに SVI を作成します。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 を作成しても、各ダウンストリーム スイッチは自身の 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、同じサブネットに重複した IP アドレスが作成され、IP の競合やルーティング エラーが発生します。
- 6300M スタックのサブネットに 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、同じサブネットに不要な IP アドレスも作成され、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。
参考文献:
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/index.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-ov
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7295/cx-noscg/l3-routing/l3-routing-co

最新問題: **40**
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。

**Answer: B (**メーッセージを残す**)**
与えられたオプションの中で当てはまる 6 GHz 帯域の主な特性は、北米では 5 GHz 帯域の 40 MHz チャネルよりも多くの 80 MHz チャネルが 6 GHz 帯域で提供されることです。この特性により、Wi-Fi 6E をサポートするワイヤレス デバイスでは、スペクトルの可用性が高まり、干渉が減り、スループットが向上します。Wi-Fi Enhanced (Wi-Fi 6E) は、Wi-Fi 6 (802.11ax) 標準の拡張であり、6 GHz 付近の新たに利用可能になったライセンス不要の周波数スペクトルと、それ以下の既存の帯域で動作します。この特性に関するいくつかの事実は次のとおりです。
北米では、新しいスペクトルの無認可部分全体 (5925 ～ 7125 MHz) において、3 つのチャネル幅 (20 MHz、40 MHz、80 MHz) のそれぞれで、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 個あることになります。
これと比較すると、北米では、既存のスペクトルのライセンス不要部分全体 (2400 ～ 2483 MHz および 5150 ～ 5825 MHz) の 2 つのチャネル幅 (20 MHz および 40 MHz) で、それぞれ 9 つの重複しないチャネルしか利用できません。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 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は、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) では、それ以下の既存のスペクトルの 40 MHz 幅 (3) よりも 2 倍以上の重複しない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。
6 GHz 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、長距離伝送時や物体または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、6 GHz WLAN の RF 信号は、低周波 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 帯域は既存の帯域と完全に下位互換性があります。Wi-Fi デバイスは、6 GHz 付近の新しいスペクトルで動作するために Wi-Fi 6E 標準をサポートする必要があるため、このオプションは false です。Wi-Fi 6E 標準をサポートしていない既存の Wi-Fi デバイスはこのスペクトルを使用できず、それ以下の既存の帯域でのみ動作できます。
低電力デバイスは屋内および屋外での使用が許可されています: 低電力屋内デバイス (LPI) は、特定の電力制限および登録要件の下で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 (連邦通信委員会 (FCC) は、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する米国政府の独立機関) 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、特定の電力制限の下で、登録要件なしで許可される場合があります。

最新問題**: 41**
ゲートウェイ経由でクラス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？
172.16.1.1?
**A.** IPルート 10.2.10.0/24 172.16.1.1
**B.** ip ルート 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
**Answer: A (**メーッセージを残す**)**
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 に静的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)、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、静的ルートを追加するための構文が正しくないか、パラメーターが正しくありません。
参考資料: https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip- routing/sta

最新問題**: 42**
UXI の利点を 2 つ挙げてください。(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。
**Answer: (**解答を表示する**)**

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、遅延、ジッター、パケット損失、スループットなどのメトリックを測定できます。
参考資料: https://www.arubanetworks.com/products/networking/user-experience-insight/

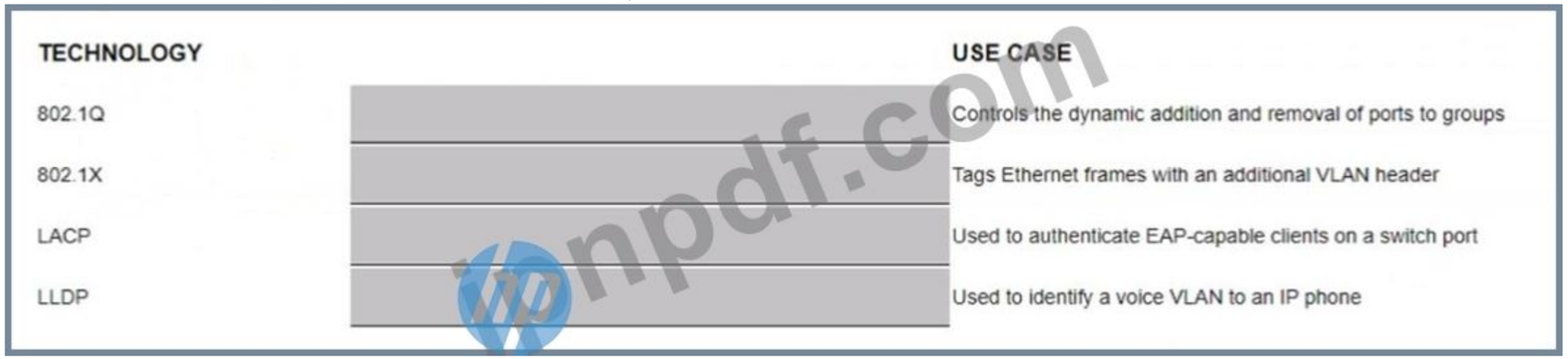
最新問題: **43**
AruDaCX 8400の 「show ip route」出力に基づきます。「10.1 20 0/24、vrf default via」はどのようなルートですか？
10.1.12.2. [1/0]"?
**A.** ローカル
**B.** 静的
**C.** OSPF
**D.** 接続済み
**Answer: B (**メーッセージを残す**)**
説明
スタティック ルートは、ルータまたはスイッチ上で手動で設定されるルートであり、管理者によって変更されない限り変更されません。スタティック ルートは、デバイスに直接接続されていない、またはダイナミック ルーティング プロトコルでは到達できない特定の宛先にトラフィックがどのように到達するかを指定するために使用されます。Aruba CX スイッチでは、グローバル コンフィギュレーション モードで ip route コマンドを使用してスタティック ルートを設定できます。Aruba CX 8400 スイッチの 「show ip route」出力に基づくと、ルート 「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 であるため、静的ルートです。これらは、静的ルートの一般的な値です。参照: https://en.wikipedia.org/wiki/Static_routing
https://www.arubanetworks.com/techdocs/AOS-CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.h

最新問題: **44**
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.** グローバル設定 lldp の有効化
**B.** int 1/1/24、lldp 受信
**C.** int 1/1/24、CDPなし
**D.** LLDPはデフォルトで有効になっています
**Answer: (**解答を表示する**)**

最新問題: **45**
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
**Answer: (**解答を表示する**)**
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モデルを幅広く取り揃えています。200 ～ 380 台のクライアント、プリンター、AP をサポートする分散ラックの場合、CX 6300 は、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機能を提供します。このシリーズはコスト効率に優れ、信頼性の高い接続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 などのその他のオプションは、過剰仕様で高価 (CX 6400)、必要なポート密度が提供されない (CX 6200)、または製品ラインに存在しない (CX 6000) 場合があります。

最新問題: **46**

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。




**Answer:**

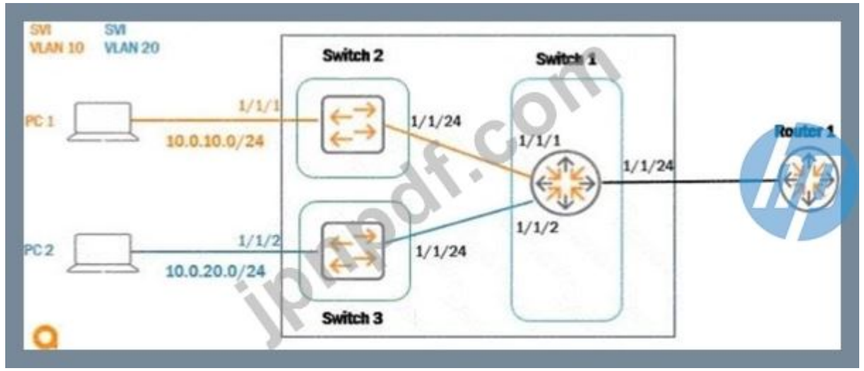



最新問題: **47**
無線帯域と AP 無線間で負荷分散を提供する Aruba テクノロジーはどれですか?
**A.** アルバ ESP
**B.** アルバ クライアントマッチ
**C.** アルバ エアウェーブ
**D.** アルバ セントラル
**Answer: B** (メーッセージを残す)
Aruba ClientMatch は、クライアントの動作を継続的に監視し、クライアント接続を自動的に調整して Wi-Fi パフォーマンスを最適化するテクノロジーです。これには、クライアントを WLAN 上の最も混雑の少ないアクセス ポイントと最適な無線に誘導することが含まれており、さまざまな無線帯域と AP 無線間で負荷分散が効果的に行われます。

最新問題: **48**

Aruba Central を使用する場合、ネットワークの健全性の問題を解決するための推奨手順を特定し、サポート担当者と詳細情報を共有できるのは何ですか?
**A.** 概要ダッシュボード
**B.** OAIOps
**C.** アラートとイベント
**D.** 監査証跡
**Answer: B (**メーッセージを残す**)**
OAIOps は、人工知能と機械学習を使用してネットワークの健全性の問題を解決するための推奨手順を特定し、サポート担当者と詳細情報を共有できる Aruba Central の機能です。OAIOps は、ネットワーク パフォーマンス、根本原因分析、異常検出、プロアクティブなアラート、自動修復アクションに関する洞察を提供します。また、OAIOps は Aruba User Experience Insight (UXI) センサーと統合して、有線および無線ネットワーク全体のユーザー エクスペリエンスを測定および改善します。
参考資料: https://www.arubanetworks.com/assets/ds/DS_ArubaCentral.pdf

最新問題**: 49**
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 が LLDP で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
**Answer: A (**メーッセージを残す**)**
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。
Aruba スイッチのデフォルト設定では通常、すべてのポートで LLDP が有効になっているため、ほとんどの場合、追加の設定は必要ありません。
つまり、ルータ 1 が LLDP メッセージを送信している場合、そのポートで LLDP が無効になっていない限り、スイッチ 1 ポート 1/1/24 は追加の設定なしでそのメッセージを受信するはずです。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、それ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) に似ている可能性があります。オプション B は、Aruba スイッチで LLDP を有効にする一般的な方法ではないグローバル設定コマンドを提案しているためです。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。

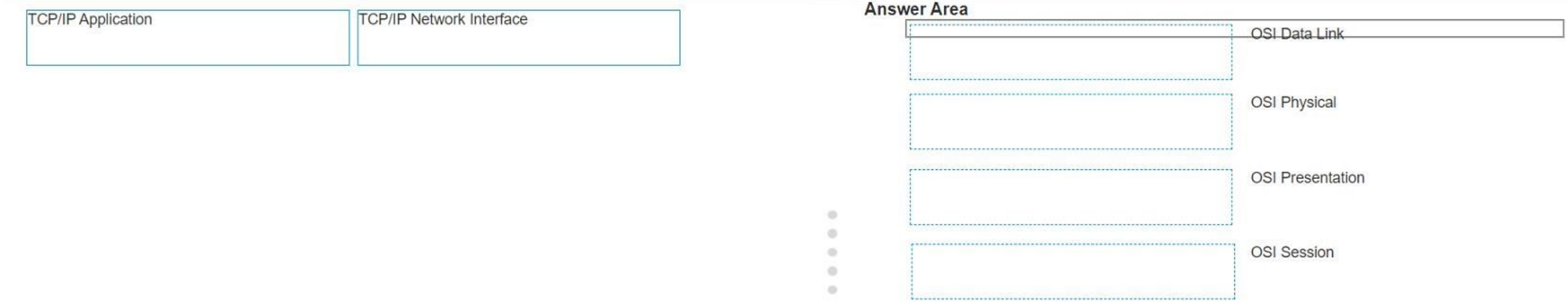
最新問題**: 50**
AP 信号強度 0.0000001 ミリワットは何 dBm に相当しますか?
**A.** -90 dBm
**B.** -60 dBm

**C.** -70 dBm
**D.** -80 dBm
**Answer: (**解答を表示する**)**
AP 信号強度 0.0000001 ミリワットは -80 dBm に相当します。dBm スケールは対数で、10 dBm 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 0 dBm なので、信号強度 0.0000001 mW は 1 mW より 80 デシベル低く、-80 dBm になります。

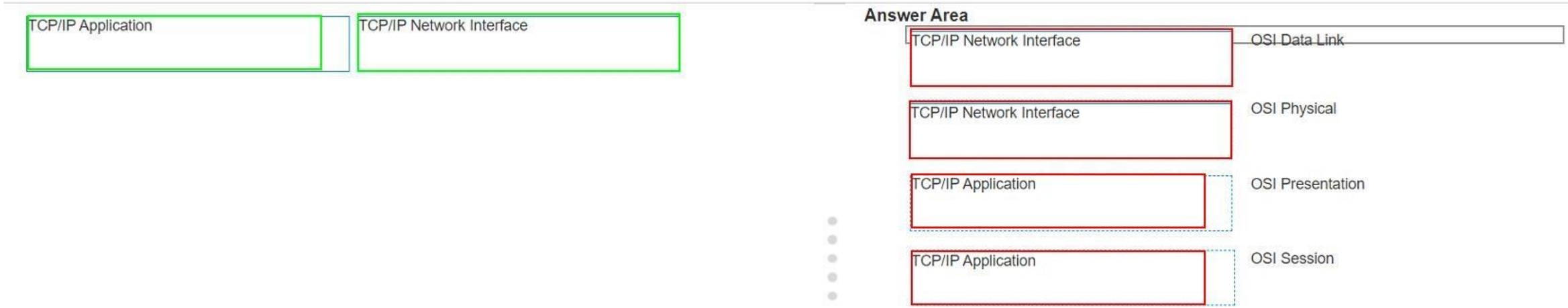
最新問題**: 51**
ネットワーク技術者が、ブランチ オフィスにある 1 つの新しい AP のトラブルシューティングを行っています。この AP は Aruba Central から構成を受信しません。ブランチにある他の AP は期待どおりに動作しています。「show ap debug cloud-server コマンド」の出力には、「cloud conflg received」が FALSE であることが示されています。
新しい AP がインターネットにアクセスできることを確認した後、次に何を確認しますか?
**A.** プロビジョニングの更新をトリガーするためにアクティブ化を無効にしてから有効にする
**B.** APがarubanetworks.com上のデバイスにpingできることを確認します。
**C.** APにライセンスが割り当てられていることを確認する
**D.** Aruba Central を無効にしてから有効にすると、構成の更新がトリガーされます。
**Answer: A (**メーッセージを残す**)**
Aruba AP が Aruba Central から構成を受信しておらず、その場所にある他の AP が正常に機能している場合、一般的なトラブルシューティング手順は、AP のアクティベーション プロセスを無効にしてから再度有効にすることです。このアクションによりプロビジョニングの更新がトリガーされ、AP が Aruba Central から構成を再度取得するように促されます。この手順は、AP と管理プラットフォーム間の通信またはプロビジョニングの問題を解決するのに効果的です。

最新問題**: 52**
管理距離の目的を説明する
**A.** 外部BGP経由でチーム化されたルートは、OSPF経由で学習されたルートよりも管理距離が長くなります。
**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.** 静的ルートの管理距離は10です
**D.** 管理距離が大きいほど優先されます
**Answer: B (**メーッセージを残す**)**
管理距離は、ルート エントリ (B) の信頼度評価として使用されます。これは、2 つの異なるルーティング プロトコルから同じ宛先への 2 つ以上の異なるルートがある場合に、ルータが最適なパスを選択するために使用するメトリックです。管理距離の値が低いほど、ルートのソースの信頼性が高くなります。たとえば、直接接続されたネットワークは、ルーティング情報の最も信頼できるソースであるため、管理距離は 0 になります。対照的に、異なるルーティング プロトコルから学習されたルートは、相対的な信頼性を反映して、管理距離が高くなります。

最新問題**: 53**
オープン システム インターコネクション (OSI) 層を、TCP/IP スタックの同等のメンバーと一致させます。(オプションは複数回使用できます。)




**Answer:**




最新問題: **54**

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も必要
**Answer: (**解答を表示する**)**
手動プロビジョニングは、DHCP または 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、および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構成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

最新問題**: 55**
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X 509証明書を使用します
**B.** ペアワイズテンポラルキー (PTK) は各セッションに固有のものです
**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
**Answer: C (**メッセージを残す**)**
WPA2-Personal をセキュリティに使用すると、WLAN 環境に導入される弱点は、PMK ペアワイズ マスター キー (PMK) が PSK 事前共有キー (PSK) から派生したキーであり、通信開始前に 2 者間で共有されるキーであり、どちらも固定されていることです。つまり、PSK を知っているすべてのユーザーは、認証プロセスなしで PMK を生成できます。これはまた、PSK または PMK が攻撃者によって侵害された場合、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 から派生したキーです。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です。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) は疑似ランダム関数 (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ています: 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 パーソナルでは認証に X 509 証明書も証明機関も使用されないため、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の場合、リモート認証ダイヤルイン ユーザー サービス (RADIUS) は、ネットワーク サービスに接続して使用するユーザーに対して集中的な認証、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) は各セッションに固有です。このオプションは false です。PTK が各セッションに固有であることは WPA2-Personal の弱点ではなく強みです。PTK が各セッションに固有であるということは、通信中に時間または送信されたパケット数に基づいて定期的に変更されることを意味します。これにより、リプレイ攻撃が防止され、データ暗号化のセキュリティが向上します。
WPA 4 ウェイ ハンドシェイクを使用しません: WPA2-Personal はキー ネゴシエーションに WPA 4 ウェイ ハンドシェイクを使用するため、このオプションは false です。WPA 4 ウェイ ハンドシェイクは、ステーションとアクセス ポイントが ANonce と SNonce を交換し、PMK から PTK を導出できるようにするプロセスです。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もできます。

最新問題**: 56**
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
**Answer: B,C (**メーッセージを残す**)**
Aruba Central を使用すると、各グループ内のデバイスの共通設定を定義するデバイス構成グループを作成できます。ネットワーク要件と管理設定に応じて、さまざまなタイプのグループを作成できます。
グループ作成時に Aruba Central で定義できるグループには次の 2 種類があります。
- テンプレート グループ: テンプレート グループを使用すると、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、同様の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

最新問題**: 57**
大規模物流施設に推奨されるUXI監視ソリューションは何ですか?
**A.** 特殊な耐久性のある UXI センサーを使用します。
**B.** Windows CE で実行されているすべてのハンドヘルド デバイスで UXI アプリを使用します。
**C.** 物流スペースのすべての通路に UXI センサーを追加します。
**D.** Android で実行されている Zebra スキャン デバイスで UXI アプリを直接使用します。
**Answer: C (**メーッセージを残す**)**
大規模な物流施設では、包括的な監視とパフォーマンス分析を確実に行うために、各通路に User Experience Insight (UXI) センサーを設置することをお勧めします。これにより、施設の広範囲にわたるネットワーク パフォーマンスを詳細かつ具体的に監視できます。

最新問題**: 58**
Aruba モビリティ コントローラーは、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。
**B.** 各ワイヤレス クライアントに固有の IP サブネットを割り当てます。
**C.** 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。
**D.** 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。
**Answer: D (**メーッセージを残す**)**

最新問題**: 59**
ネットワーク技術者が、本社の倉庫に「ヘッドレス」デバイスを導入しています。これまで、802.1X の SSID が設定されていました。しかし、これらの新しいデバイスには 802.1X のサポートがありません。
これらのデバイスのセキュリティを強化するにはどのオプションが最適ですか?
**A.** WPA3-パーソナル
**B.** マルチ事前共有キー (mPSK)
**C.** WPA2-エンタープライズ
**D.** 無線暗号化 (OWE)

**Answer: (**解答を表示する**)**
802.1X をサポートしていない 「ヘッドレス」デバイスの場合、マルチ事前共有キー (mPSK) は、単一の事前共有キーを使用する WPA2-Personal よりも安全な代替手段となります。mPSK を使用すると、デバイスまたはデバイス グループに固有の PSK を割り当てることができるため、複数のデバイス間で単一の PSK を共有せずにセキュリティを強化できます。

最新問題**: 60**
SVI を使用したインバンド管理が使用されている場合、Aruba CX スイッチでデフォルト ルートを 10.4.5.1 に設定するにはどのコマンドを使用しますか?
**A.** iP デフォルトゲートウェイ 10.4.5.1
**B.** ip ルート 0 0 0.070 10.4 5.1 vrf 管理
**C.** IPルート0.0 0 0/0 10.4.5.1
**D.** デフォルトゲートウェイ 10.4.5.1
**Answer: C (**メーッセージを残す**)**
SVI を使用したインバンド管理が使用されている場合に、Aruba CX スイッチでデフォルト ルートを 10.4.5.1 に設定するコマンドは、ip route 0.0 0 0/0 10.4.5.1 です。このコマンドは、スイッチに直接接続されていないネットワークに到達するための宛先ネットワーク アドレス (0.0 0 0)、プレフィックス長 (/0)、およびネクストホップ アドレス (10.4.5.1) を指定します。デフォルト ルートは、デフォルトの VRF (仮想ルーティングおよび転送) に適用されます。VRF は、ルーティング テーブルの複数のインスタンスを同じルータ内に同時に共存させるテクノロジです。VRF は通常、セキュリティ、プライバシー、または管理上の目的でネットワーク トラフィックをセグメント化するために使用されます。は、SVI スイッチ仮想インターフェイスを通過するインバンド管理トラフィックに使用されます。SVI は、スイッチ上の仮想インターフェイスであり、スイッチは、同じスイッチ上の異なる VLAN 間またはトランク リンクで接続された異なるスイッチ間でパケットをルーティングできます。SVI は VLAN に関連付けられており、IP アドレスとサブネット マスクが割り当てられています12。参考: 1 https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i-6000-6100-6200/Content/Chp_StatRoute/def-rou.htm 2 https://www.arubanetworks.com/techdocs/AOS-CX/10_08/HTML/ip_route_4100i-6000-6100-6200/Content/Chp_VRF/vrf-overview.htm

最新問題**: 61**
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ように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
**Answer: C (**メーッセージを残す**)**
厳密なキューイングは、遅延の影響を受けやすい音声トラフィックを他の種類のトラフィックよりも優先させるための最適なスケジューリング技術です。この方法により、音声トラフィックがキューに入れら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。

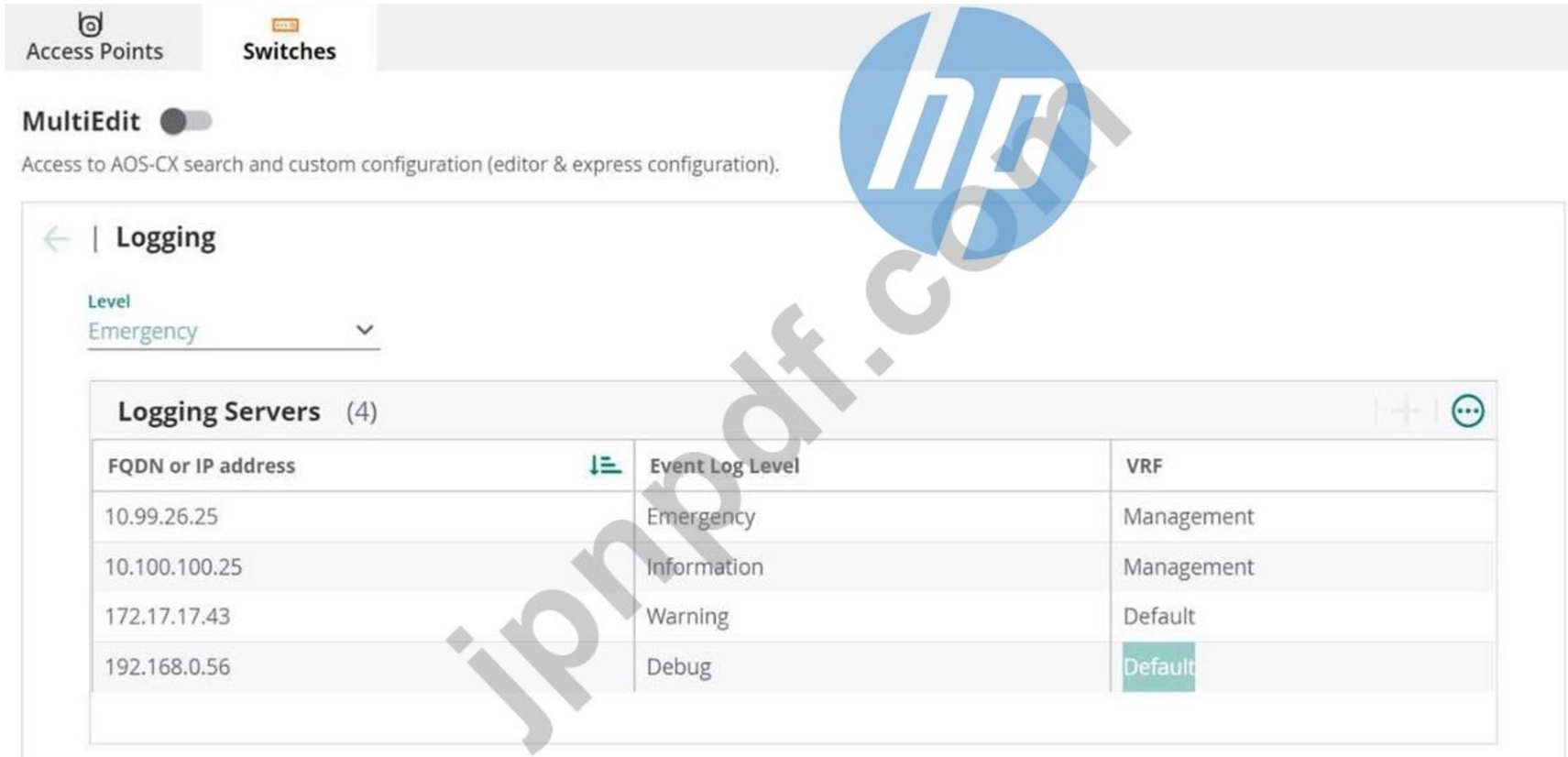


最新問題**: 62**
Aruba の ClearPass Policy Manager にはどのような機能が含まれていますか? (2 つ選択してください)
**A.** デバイスのプロファイリングとフィンガープリンティング。
**B.** カスタマイズ可能な Web ポータルを使用したゲスト アクセス管理。
**C.** 直接的なクラウド管理統合。
**D.** 高度な暗号化モジュールの検証。

**Answer: A,B (メーッセージを残す)**

最新問題**: 63**
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 ルート 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
**Answer: A (メーッセージを残す)**
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。参照: 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 「/24」で示されるクラス C サブネット マスクで正しく指定し、ネクスト ホップ IP アドレスとして 「172.16.1.1」を指定します。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 システムで静的ルートを追加するための標準構文に従っています。他のオプションは構文が間違っているか、静的ルートを追加するための標準コマンドに通常は含まれない不要なパラメータが追加されています。

最新問題**: 64**
別紙を参照してください。




どのサーバーが最も少ない量のデータを受信するでしょうか?

**A.** 172.17.17.43

**B.** 10.100.100.25

**C.** 10.99.26.25

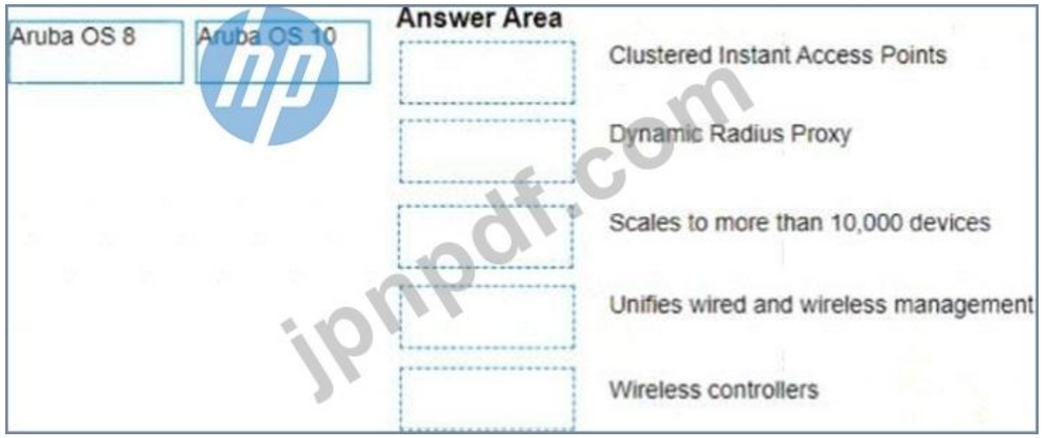
**D.** 192.168.0.56

**Answer: (**解答を表示する**)**

ログ サーバーの構成を示す図に基づくと、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、受信するデータ量は最小になります。つまり、警告またはそれ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、情報」、デバッグ」、緊急」などの重大度が低いレベルよりも頻度が低くなります。

最新問題: **65**

機能を Aru ba 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)。




**Answer:**


Explanation:

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

ArubaOS 8 の機能の一部は次のとおりです。

- クラスター化されたインスタント アクセス ポイント: この機能により、複数のインスタント AP がクラスターを形成し、構成と状態情報を共有できるようになります。これにより、クライアントのシームレスなローミング、負荷分散、および高速フェイルオーバーが可能になります2。
- ダイナミック RADIUS プロキシ: この機能により、MC はクライアントまたは AP からの RADIUS 認証要求のプロキシとして機能できます。これにより、RADIUS サーバーの構成と管理が簡素化され、MC と RADIUS サーバー間のネットワーク トラフィックが削減されます3。
- ワイヤレス コントローラー: Aruba ワイヤレス コントローラーは、ワイヤレス ネットワークを集中的に管理および制御するデバイスです。AP のプロビジョニング、構成、セキュリティ、ポリシーの適用、ネットワークの最適化などの機能を提供します。

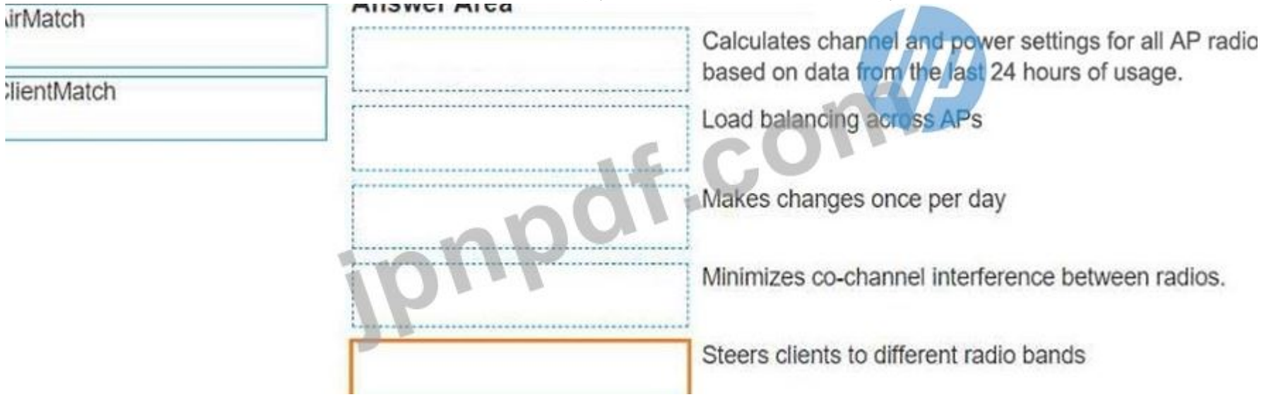
ArubaOS 10 は、クラウドベースのネットワーク管理プラットフォームである Aruba Central と連携する次世代のオペレーティング システムです。ArubaOS 10 は、大規模なキャンパス、ブランチ、リモート ワーク環境全体で、優れたスケーラビリティ、セキュリティ、AI を活用した最適化を実現します。ArubaOS 10 の機能の一部は次のとおりです。
- 10,000 台を超えるデバイスに拡張可能: ArubaOS 10 は、クラスターあたり最大 10,000 台のデバイスをサポートできます。これは、ArubaOS 8 の 10 倍です。これにより、パフォーマンスや信頼性を損なうことなく、ネットワークを拡張できます。
- 有線と無線の管理を統合: ArubaOS 10 は、ネットワーク全体の有線デバイスと無線デバイスの両方を管理するための単一のプラットフォームを提供します。お客様は、Aruba Central を使用して、どこからでもデバイスの構成、監視、トラブルシューティング、更新を行うことができます。
ArubaOS 8 と ArubaOS 10 には、次のような共通機能がいくつかあります。
- 有線と無線の管理を統合: 両方のオペレーティング システムは、Aruba スイッチと AP を使用するお客様に統合された有線と無線のアクセスを提供します。お客様は、単一のインターフェイスを使用してネットワーク インフラストラクチャ全体を管理できます1。
参考文献:
1 https://www.arubanetworks.com/resource/arubaos-8-fundamental-guide/
2 https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/iap-maintenance/clus
3 https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1- 概要
https://www.arubanetworks.com/products/networking/controllers/
https://www.arubanetworks.com/products/network-management-operations/arubaos/
https://blogs.arubanetworks.com/solutions/making-the-switch/
https://www.arubanetworks.com/products/network-management-operations/aruba-central/

最新問題**: 66**
ネットワーク技術者が 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
**Answer: (**解答を表示する**)**
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すべてのタイプのアラートとイベントが表示されます。構成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 のアラートと通知を構成できます。また、リスト ビューと概要ビュー2 でアラートとイベントを表示することもできます。参照: 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

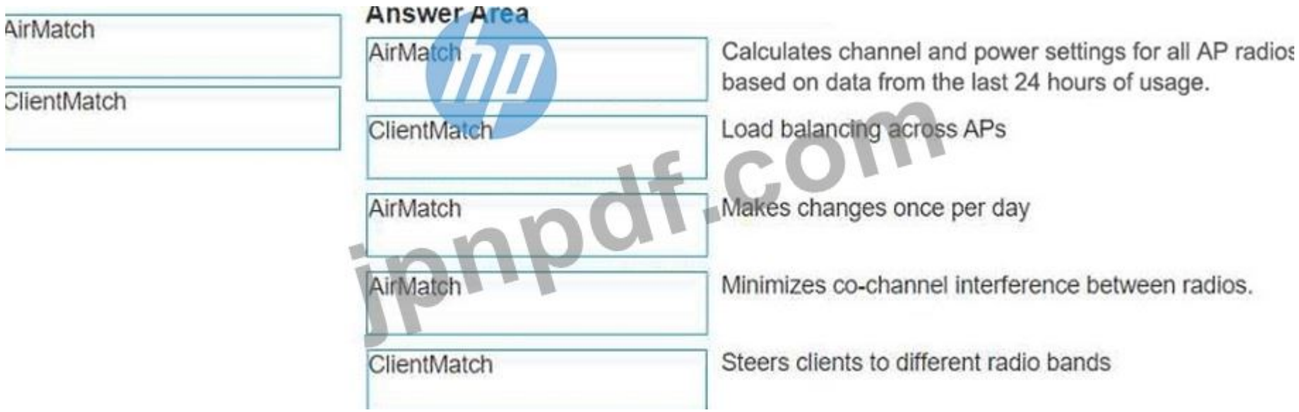
最新問題**: 67**
病院では、診断や患者データの記録に多くのモバイル機器を使用しています。
単一の VSF スタックに 400 を超えるポートを備えた配布ラックを備えたこの大規模病院に最適なアクセス スイッチは何ですか?
**A.** OCX 6300
**B.** OCX 6400
**C.** OCX 6200
**D.** OCX 6100
**Answer: (**解答を表示する**)**
単一の VSF スタックに 400 を超えるポートを備えた配布ラックを備えた大規模病院に最適なアクセス スイッチは、CX 6300 です。
このスイッチには次の利点があります。

- 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 個のスイッチをサポートし、1 つのスタックで合計 480 個のポートを使用できます。これにより、1 つの VSF スタックに 400 個を超えるポートを配置するという要件が満たされます。
- CX 6300は、最大960Gbpsのスイッチング容量と最大
714 Mpps の転送速度。これにより、モバイル機器と患者データの高スループットと低遅延の要件が満たされます。
- CX 6300 は、動的セグメンテーション、ポリシーベースのルーティング、ロールベースのアクセス制御などの高度な機能をサポートしています。これらの機能により、さまざまなタイプのデバイスやユーザーに異なるポリシーとロールを適用することで、ネットワークのセキュリティと柔軟性が向上します。
- CX 6300 は、ネットワークの管理と自動化を簡素化するネットワーク構成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メンテナンスに伴う複雑さと人的エラーが軽減されます。
他のオプションは、次の理由から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に役立つ動的セグメンテーションやポリシー ベース ルーティング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、スイッチング容量と転送速度が CX 6300 よりも低いため、ネットワークのパフォーマンスに影響す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、スイッチング容量と転送速度は CX 6300 よりも低いため、ネットワークのパフォーマンスに影響する可能性があります。
参考文献:
https://www.arubanetworks.com/assets/ds/DS_CX6300Series.pdf
https://www.arubanetworks.com/assets/ds/DS_OC6400Series.pdf
https://www.arubanetworks.com/assets/ds/DS_OC6200Series.pdf
https://www.arubanetworks.com/assets/ds/DS_OC6100Series.pdf

最新問題: **68**
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ます。(一致は複数回使用できます。)




**Answer:**




最新問題: **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)。


**Answer:**


説明

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/licensing-guide.pdf

最新問題: **70**
複数の 20MHz 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.** 可用性の高い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
**Answer: B (**メッセージを残す**)**
複数の 20MHz 幅の 802.11 チャネルを結合することは、より高速なデータ転送をサポートするより広い帯域幅のチャネルを作成する技術です。これにより、より多くのスペクトル リソースを使用し、干渉を減らすことで、クライアントと AP 間のスループットを向上させることができます。
参考文献: https://ieeexplore.ieee.org/document/9288995

最新問題: **71**
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できる
**D.** MAC識別子は偽装が難しい
**Answer: B (**メッセージを残す**)**
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、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に認証を行います。
参考資料:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-ove

最新問題: **72**
セキュアなエンタープライズ モード WLAN に接続するときに、802.1x 認証プロセスはいつ開始されますか?
**A.** ファイアウォールポリシーがセッションに適用された後
**B.** クライアントが802.11アソシエーションを完了した後
**C.** キャプティブポータル認証が完了した後
**D.** WPA 4ウェイハンドシェイクが完了した後
**Answer: (**解答を表示する**)**
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、完全なネットワーク 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。

最新問題: **73**
WPA3-Personal は、ステーションがワイヤレス ネットワークに接続するたびに異なるペアワイズ マスター キー (PMK) を生成するソースとして何を使用しますか?
**A.** キー暗号化キー (KEK)
**B.** セッション固有の情報 (MAC と nonce)
**C.** 同時同等認証 (SAE)

**D.** 無線暗号化 (OWE)
**Answer: C (**メーッセージを残す**)**

最新問題**: 74**
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
**Answer: A (**メーッセージを残す**)**
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 要求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。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てから、ネットワーク アクセスを許可します。参照: https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/instant-ug/captive-portal/captive-portal-auth.htm Aruba の Captive Portal は主にレイヤー 3 認証を使用します。これはネットワーク層で動作します。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、ユーザーが資格情報を入力するか、Web インターフェイスを介して利用規約に同意してから、ネットワークへのフル アクセスを取得します。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。

最新問題**: 75**
「show lacp interface」で LACP をチェックしたときの 「ALFOE」のステータスは何を意味しますか?
**A.** ローカルスイッチのインターフェースは静的LAGとして設定されています
**B.** LACPは問題なく動作しています
**C.** ピア側でLACPが設定されていません
**D.** LACP は同期処理中です
**Answer: C (**メーッセージを残す**)**

最新問題**: 76**
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。このタスクに使用する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
**Answer: A (**メーッセージを残す**)**
ArubaOS-CX スイッチへの入力時に過剰なブロードキャスト トラフィックをドロップするのに最適なテクノロジは、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) 攻撃を軽減できます。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と、ArubaOS-CX スイッチへの入力時にブロードキャスト トラフィックにレート制限を適用できます。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または 1 秒あたりのパケット数の割合を指定できます。ブロードキャスト トラフィックが指定されたしきい値を超えると、スイッチは過剰な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 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順位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な帯域幅の割り当てを取得し、優先順位の低いキューの不足を回避できるようにします。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さまざまな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、使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順位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、帯域幅要件や重みに関係なく、優先順位の高いキューが常に優先順位の低いキューよりも先に処理されます。ストリクト キューイングでは、入力時に過剰なブロードキャスト トラフィックがドロップされるのではなく、出力時に送信トラフィックがスケジュールされます。

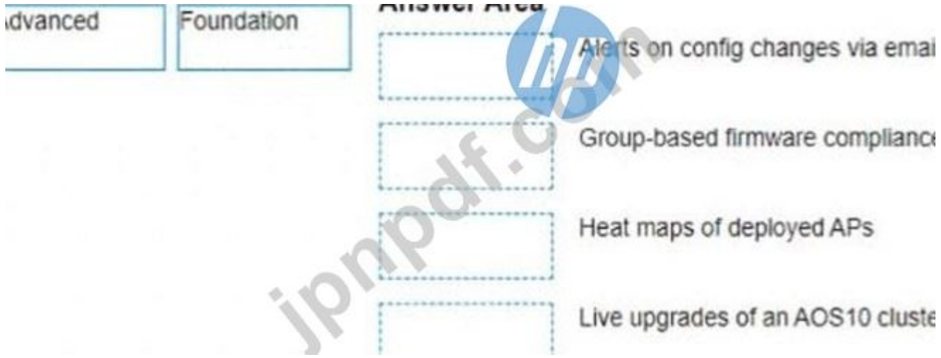


最新問題**: 77**
セキュリティのために WPA2-Personal を使用すると、WLAN 環境にどのような脆弱性が生じますか?
**A.** 認証局によって生成されたX 509証明書を使用します
**B.** ペアワイズテンポラルキー (PTK) は各セッションに固有のものです
**C.** ペアワイズマスターキー (PMK) はすべてのユーザーによって共有されます
**D.** WPA 4ウェイハンドシェイクを使用しません
**Answer: C** (メーッセージを残す)
WPA2-Personal をセキュリティに使用すると、WLAN 環境に導入される弱点は、PMK ペアワイズ マスター キー (PMK) が PSK 事前共有キー (PSK) から派生したキーであり、通信開始前に 2 者間で共有されるキー (両方とも固定) であることです。つまり、PSK を知っているすべてのユーザーは、認証プロセスなしで PMK を生成できます。これはまた、PSK または PMK が攻撃者によって侵害された場合、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) は疑似ランダム関数 (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ています: 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-Personal は認証に X 509 証明書または証明機関を使用しないため、このオプションは false です。X 509 証明書と証明機関は、802.1X および EAP を使用する WPA2-Enterprise 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、または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 ネットワークおよび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の場合、リモート認証ダイヤルイン ユーザー サービス (RADIUS) は、ネットワーク サービスに接続して使用するユーザーに対して集中的な認証、承認、およびアカウンティング (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) は各セッションに固有です: このオプションは false です。PTK が各セッションに固有であることは WPA2-Personal の弱点ではなく強みです。PTK が各セッションに固有であるということは、通信中に時間または送信されたパケット数に基づいて定期的に変更されることを意味します。これにより、リプレイ攻撃が防止され、データ暗号化のセキュリティが向上します。
- WPA 4 ウェイ ハンドシェイクを使用しません: WPA2-Personal はキー ネゴシエーションに WPA 4 ウェイ ハンドシェイクを使用するため、このオプションは false です。WPA 4 ウェイ ハンドシェイクは、ステーションとアクセス ポイントが ANonce と SNonce を交換し、PMK から PTK を導出できるようにするプロセスです。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もできます。
参考文献: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA_key_hierarchy_and_management https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf

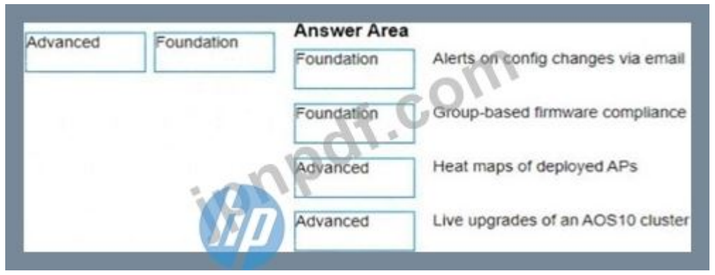
最新問題**: 78**
Aruba モビリティ マスター アーキテクチャを使用する場合、ネットワーク管理者はどの機能を使用して RF 計画および最適化サービスを集中化できますか?

**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
**Answer: C (メーッセージを残す)**
説明
AirMatch は、Aruba ワイヤレス ネットワークの集中 RF 計画および最適化サービスを提供する機能です。クラウドベースのアルゴリズムと機械学習を使用して、RF パフォーマンスとユーザー エクスペリエンスを最適化します。参考資料:https://www.arubanetworks.com/assets/ds/DS_AirMatch.pdf

最新問題**: 79**
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)。




**Answer:**

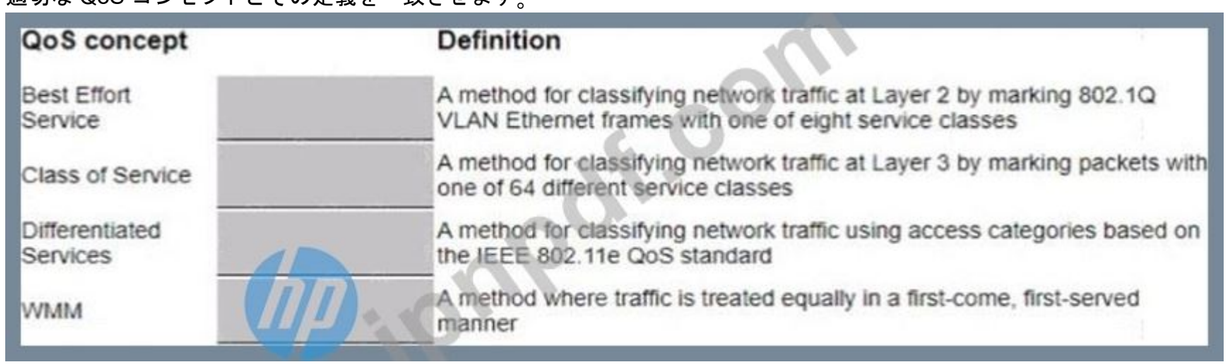



Explanation:
a) 電子メールによる設定変更のアラート - Foundation
b) グループベースのファームウェアコンプライアンス - Foundation
c) 展開された AP のヒートマップ - 上級
d) AOS10 クラスターのライブアップグレード - 上級
Aruba Central ライセンス ガイド1 によれば、Foundation ライセンスでは、構成、監視、アラート、レポート、ファームウェア管理などの基本的なデバイス管理機能が提供されます。Advanced ライセンスでは、AI インサイト、WLAN サービス、NetConductor Fabric、ヒート 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/licensing-guide.pdf

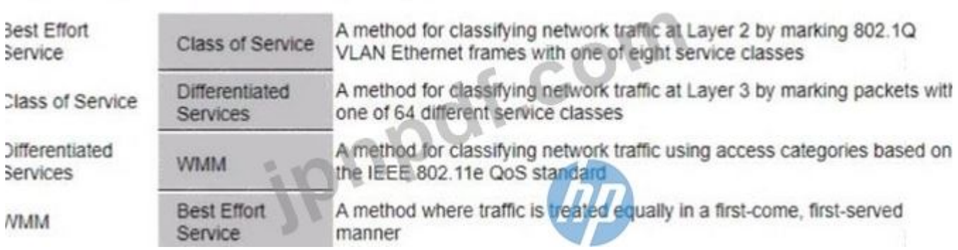
最新問題**: 80**

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.** 静的ルートの管理距離は10です
**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.** 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
**Answer: D (**メーッセージを残す**)**

最新問題**: 81**
適切な QoS コンセプトとその定義を一致させます。




**Answer:**




Explanation:
QoS サービス品質 (QoS) は、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さまざまなレベルのサービスを提供する一連の技術です。QoS により、ネットワーク パフォーマンスが向上し、待ち時間が短縮され、スループットが増加し、輻輳が防止されます。概念とその定義。
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で平等に扱われる方法 a) 802.1Q VLAN イーサネット フレームを 8 つのサービス クラスのいずれかで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) パケットを 64 の異なるサービス クラスのいずれかで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回答: 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、トラフィックが優先順位付けや差別化なしに先着順で平等に処理される方法です。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およびアプリケーションのデフォルトのサービス レベルです。ベスト エフォート サービスでは、帯域幅、遅延、ジッター、パケット損失は保証されません。
- サービス クラス: これは、802.1Q VLAN イーサネット フレームを 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、レイヤー 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 802.1p 優先度値または PCP とも呼ばれます。優先度コード ポイント (PCP) は、イーサネット フレームの優先度レベルを示す 802.1Q VLAN タグの 3 ビット フィールドです。サービス クラスにより、ネットワーク デバイスは優先度レベルに基づいてさまざまな種類のトラフィックを識別して処理できます。サービス クラスは通常、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、建物環境など、レイヤー 2 スイッチングが主流である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、64 の異なるサービス クラス (0 ～ 63) のいずれかを使用して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、パケットのサービス クラスを示す IP ヘッダー内の 6 ビット フィールドです。差別化サービスにより、ネットワーク デバイスは、サービス クラスに基づいてさまざまな種類のトラフィックを識別して処理できます。差別化サービスは、通常、WAN で使用されます。ワイド エリア ネットワーク (WAN) は、国や大陸などの広い地理的領域にわたってデバイスを接続するネットワークで、レイヤー 3 ルーティングが主流の環境です。
- 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 標準。WMM は Wi-Fi Multimedia の略で、ワイヤレス ネットワークの QoS を強化するために Wi-Fi Alliance によって開発された認証プログラムです。WMM では、次の 4 つのアクセス カテゴリ (AC) が定義されています。音声、ビデオ、ベスト エフォート、およびバックグラウンド。これらのアクセス カテゴリは、ワイヤレス トラフィックのさまざまな優先レベルと競合パラメータに対応しています。WMM を使用すると、ワイヤレス デバイスはアクセス カテゴリに基づいてさまざまな種類のトラフィックを識別して処理できます。
参考文献:
https://en.wikipedia.org/wiki/Quality_of_service
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_dfsrv/configuration/xe-16/qos-dfsrv-xe-16-book/qos-dfs
https://www.cisco.com/c/en/us/support/docs/wireless-Mobility/wireless-lan-wlan/81831-qos-wlan.html
https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm

最新問題: **82**
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
**Answer: B (**メーッセージを残す**)**
説明
プロファイリングは、Aruba スイッチが、MAC アドレス、DHCP オプション、LLDP 情報などのさまざまな属性に基づいて、接続されているデバイスを自動的に識別および分類できるようにする機能です。プロファイリングを使用すると、デバイス 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。
たとえば、IP カメラは、プリンターや PC よりも高い PoE 優先度を持つ場合があります。プロファイリングを使用すると、デバイス プロファイルに基づいて、VLAN、ACL、QoS などの他の構成設定を適用することもできます。
参考資料:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-ove

最新問題: **83**
WPA 4 ウェイ ハンドシェイク機能を正しい順序でリストします。

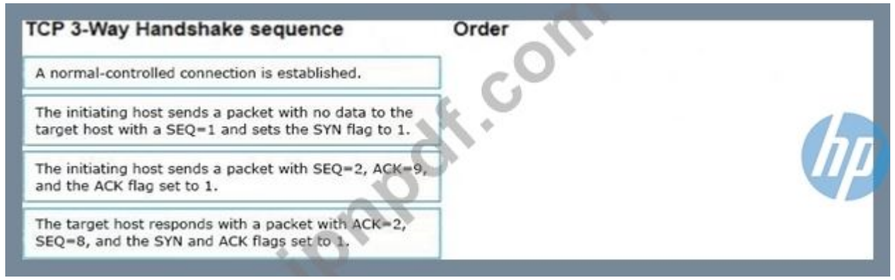

**Answer:**

**Answer Area**

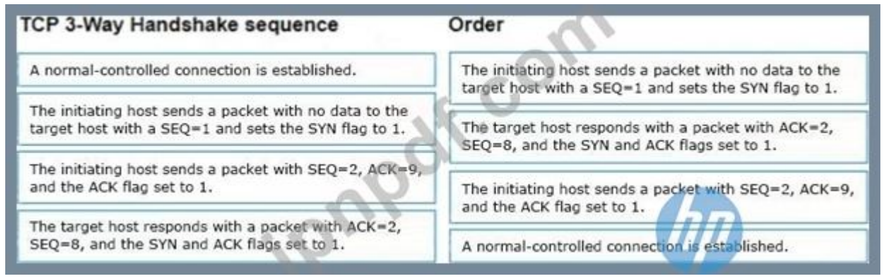
- Proves knowledge of the PMK
- Exchanges messages for generating PTK
- Distributes an encrypted GTK to the client
- Sets first initialization vector (IV)

1 - PMKに関する知識を証明する
2 - PTKを生成するためのメッセージを交換する
3 - 暗号化されたGTKをクライアントに配布する
4 - 最初の初期化ベクトル (IV) を設定します

最新問題: **84**
TCP 3ウェイハンドシェイクシーケンスの正しい順序は何ですか?




**Answer:**




Explanation:
TCP 3ウェイハンドシェイクシーケンスは次のとおりです。
ステップ 1: 開始ホストは、SEQ=1 でデータなしのパケットをターゲット ホストに送信し、SYN フラグを 1 に設定します。
ステップ2: ターゲットホストはACK=2、SEQ=8、SYNおよびACKフラグが設定されたパケットで応答します。
1.
ステップ 3: 開始ホストは、SEQ=2、ACK=9、ACK フラグが 1 に設定されたパケットを送信します。
ステップ 4: 通常制御の接続が確立されます。
参考文献:
https://en.wikipedia.org/wiki/Transmission_Control_Protocol
https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

最新問題: **85**
支社のネットワーク技術者が、新しく構成された AOS-CX スイッチに VoIP 電話機を接続しています。ユーザーから、音声品質が本社ほど良くないとの苦情が寄せられています。さらに調査すると、支社のローカル プライオリティ値は 1 であるのに対し、本社では 5 であることがわかりました。
AOS-CX スイッチのデフォルトの QoS 動作に関する問題を説明するものは何ですか?
**A.** QoS 信頼はデフォルトで DSCP に設定され、VoIP 電話のローカル優先度値は 1 にマッピングされます。
**B.** QoS 信頼はデフォルトで CoS に設定され、VoIP 電話のローカル優先度値は 1 にマッピングされます。
**C.** QoS 信頼はデフォルトでなしに設定されており、各 VoIP 電話のローカル プライオリティは CoS マップ エントリ 1 に対して設定されます。
**D.** QoS 信頼はデフォルトでなしに設定されており、各 VoIP 電話のローカル プライオリティは CoS マップ エントリ 0 に設定されます。
**Answer: C** (メッセージを残す)
AOS-CX スイッチでは、QoS 信頼モードが設定されていない場合、デフォルトで none に設定されます。VoIP 電話はトラフィックをローカル プライオリティ値でマークします。QoS 信頼モードが none の場合、この値はデフォルトで CoS マップ エントリ 1 に対応します。ブランチ オフィスのローカル プライオリティ値が 1 であることは、本社と比較してトラフィックの優先順位が正しく設定されていないことを示している可能性があります。本社では、ローカル プライオリティ値が 5 であることは、音声トラフィックの優先順位が高いことを示しています。

最新問題: **86**
ネットワーク技術者が 802 1X 経由で従業員の SSID に正常に接続しました。接続が成功したことを確認するには、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
**Answer: B** (メッセージを残す)

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る必要がある RADIUS メッセージは、Access-Accept です。このメッセージは、RADIUS サーバーがサプリカント (ネットワークへのアクセスを希望するデバイス) を認証および承認し、ネットワーク リソースへのアクセスを許可したことを示します。Access-Accept メッセージには、認証者 (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るかを指定する VLAN ID、セッション タイムアウト、またはフィルタ ID などの追加属性も含まれる場合があります。
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通過できることを示す状態です。
成功: これは RADIUS メッセージではありませんが、EAP 拡張認証プロトコル (EAP) は、パスワード、証明書、トークン、生体認証など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 ネットワークおよび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) 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。

最新問題**: 87**
レイヤー 2 MAC 認証を使用する利点は何ですか?
**A.** MAC 許可リストは、時間の経過とともに簡単に維持できます。
**B.** クライアント側での設定は必要ありません。
**C.** ユーザー名と MAC アドレスを照合します。
**D.** MAC 識別子は偽装が困難です。
**Answer: B (**メーッセージを残す**)**
レイヤー 2 MAC 認証の利点は、クライアント デバイスでセットアップや構成を行う必要がないことです。ネットワーク デバイス (スイッチやアクセス ポイントなど) は、ネットワークに接続しようとすると、デバイスの MAC アドレスに基づいて自動的に認証を実行します。

最新問題**: 88**
Aruba CX スイッチで OSPF ダイナミック ルーティング プロトコルを使用する場合、ルートを交換するために隣接デバイスで一致する必要があるものは何ですか?
**A.** こんにちはタイマー
**B.** DR構成
**C.** ECMPメソッド
**D.** BDR構成
**Answer: A (**メーッセージを残す**)**
説明
OSPF (Open Shortest Path First)。OSPF は、階層構造を使用して IP ネットワークのルーティング トポロジを作成するリンク ステート ルーティング プロトコルです。OSPF ルータは、各インターフェイスで定期的に送信される Hello パケットを使用して、ネイバーとルーティング情報を交換します。隣接関係を確立するには、OSPF ルータは、インターフェイスで Hello パケットが送信される頻度を指定する Hello タイマーなど、いくつかのパラメータについて合意する必要があります。隣接ルータ間で Hello タイマーが一致しない場合は、隣接関係は形成されず、ルートも交換されません。
参考資料:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/osfp/o

最新問題**: 89**
レイヤ 3 ルート ループを軽減するために、レイヤ 3 IPv4 パケット ヘッダーで使用されてい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
**Answer: B (**メーッセージを残す**)**

説明
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 ヘッダーのフィールドは、Time To Live (TTL) です。
TTL は、パケットが破棄される前に通過できるホップの最大数を示す 8 ビットのフィールドです。TTL はソース 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。メッセージがソース デバイスに送り返されます。TTL は、ループしたネットワーク 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 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、IP ヘッダー内のすべてのフィールドの値に基づいて宛先デバイスによって検証されます。チェックサムは、パケットが通過できるホップの数を制限しないため、レイヤー 3 ルート ループを軽減しません。
プロトコル: プロトコルは、IP データグラムによって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 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、順序付けられた、エラー チェック済みの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、再送信、輻輳回避、高速回復などのメカニズムを使用して、パケット損失や輻輳を処理します。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、緊急ポインター、オプション、データなどのフィールドを含む特定の形式を持ちます。 TCPセグメントは、telnet、ftp、ssh、debug ip tcptransactionsなどのコマンドを使用して検証できます。UDPユーザーデータグラムプロトコル（UDP）ユーザーデータグラムプロトコル（UDP）は、コネクションレストランスポート層プロトコルであり、

最新問題: **90**
不明または紛失した資格情報を使用して、Aruba CX-Switch に物理的にアクセスできます。
資格情報を再構築するにはどのような手順がありますか? (2 つ選択してください。)
**A.** コンソール経由でスイッチを接続します。次に、スイッチの電源を入れ直します。
**B.** クリア ボタンを押し続けます。次に、スイッチの電源を入れ直します。
**C.** クリアボタンを押し続けます。次に、リセットボタンを 2 秒間押し、両方のボタンを放します。
**D.** ワンタイム パスワードについては、Aruba サポートにお問い合わせください。
**E.** ブート プロファイル 0 を使用します。
**Answer: B,E (**メーッセージを残す**)**
資格情報が不明または紛失した場合に Aruba CX スイッチへのアクセスを回復するには、クリア ボタンを長押しし、スイッチの電源を入れ直してパスワードをリセットします。さらに、ブート ローダー メニューでブート プロファイル 0 を使用すると、不明な資格情報が含まれている可能性のある現在のスタートアップ構成をバイパスできます。