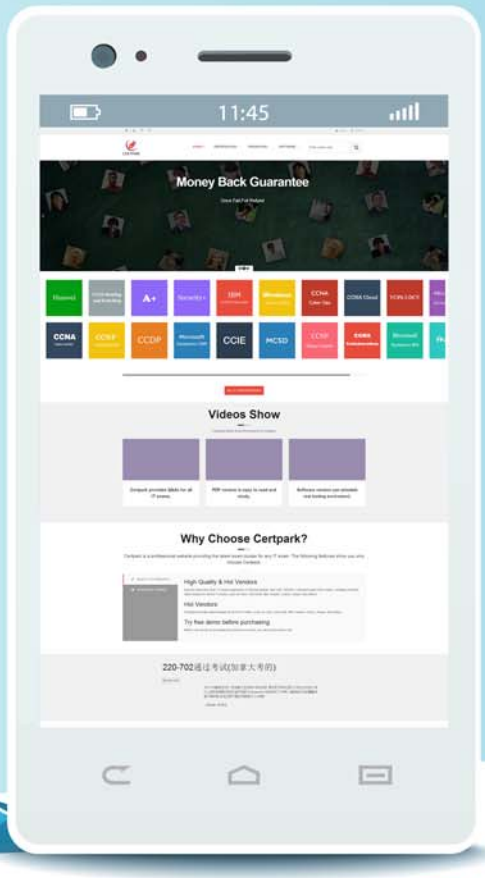
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **200-105J**

Title : Interconnecting Cisco Networking Devices Part 2 (ICND2 v3.0)

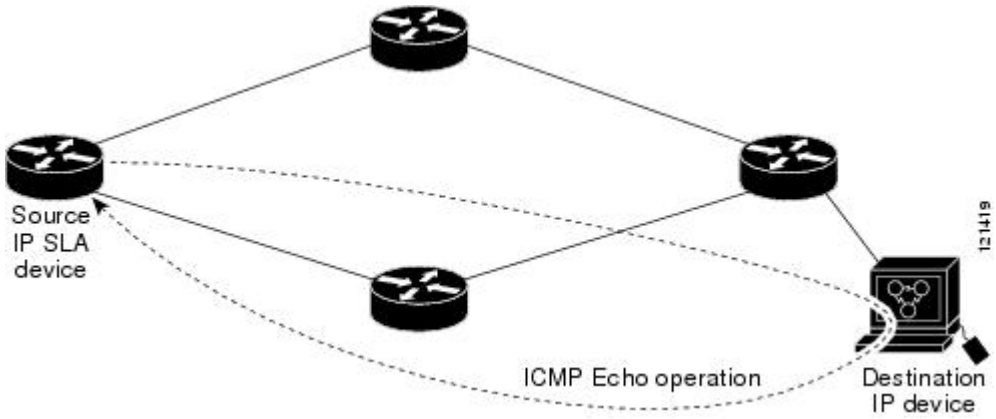
Version : DEMO

1. トピック **1**、新しいセットの質問セット **1**

どのプロトコルが LAN にアクセスする前に接続されたデバイスを認証するのですか?
802.1d
802.11
802.1w
802.1x
Answer: D
Explanation:
802.1X 認証には、サプリカント、オーセンティケータ、および認証サーバの 3 つの関係者が必要です。サプリカントは、LAN / WLAN に接続するクライアントデバイス（ラップトップなど）です。また、「サプリカント」という用語は、認証者に資格情報を提供するクライアント上で実行されているソフトウェアを指すために交換可能に使用されます。オーセンティケータは、イーサネットスイッチやワイヤレスアクセスポイントなどのネットワークデバイスです。認証サーバは、典型的には、RADIUS および EAP プロトコルをサポートするソフトウェアを実行するホストである。
オーセンティケータは、保護されたネットワークへのセキュリティガードのように動作します。サプリカント（すなわち、クライアントデバイス）は、サプリカントのアイデンティティが検証され、認可されるまで、オーセンティケータを介してネットワークの保護された側へのアクセスが許可されない。これに類推すると、入国を許可される前に、到着空港で有効なビザが提供されます。 802.1X ポートベースの認証では、サプリカントはユーザー名/パスワードやデジタル証明書などの資格情報をオーセンティケータに提供し、オーセンティケータは認証のために資格情報を認証サーバーに転送します。認証サーバーが資格情報が有効であると判断した場合、サプリカント（クライアントデバイス）はネットワークの保護された側にあるリソースにアクセスできます。

2.AAA の TACACS +と RADIUS の違いは何ですか?
A. TACACS +だけが別個の認証を可能にします。
B. RADIUS のみがアクセス要求パケット全体を暗号化します。
C. RADIUS だけが TCP を使用します。
D. TACACS +だけが認証と承認を結合します。
Answer: A
Explanation:
認証と認可
RADIUS は、認証と承認を組み合わせたものです。 RADIUS サーバからクライアントに送信された access-accept パケットには、認可情報が含まれています。これにより、認証と認可を切り離すことが困難になります。
TACACS +は AAA を分離する AAA アーキテクチャを使用します。これにより、認証とアカウンティングに TACACS +を引き続き使用できる個別の認証ソリューションが可能になります。たとえば、TACACS +では、Kerberos 認証と TACACS +許可とアカウンティングを使用できます。 NAS が Kerberos サーバで認証されると、TACACS +サーバから認証情報が要求され、再認証は必要ありません。 NAS は TACACS +サーバに Kerberos サーバで正常に認証されたことを通知し、サーバは認証情報を提供します。
セッション中に、追加の権限チェックが必要な場合、アクセスサーバーは TACACS +サーバーを調べて、ユーザーに特定のコマンドの使用許可が与えられているかどうかを判断します。これにより、認証メカニズムから切り離しながらアクセスサーバー上で実行できるコマンドをより詳細に制御できます。.

3.IP SLA ICMP Echo オペレーションに関する正しい記述はどれですか?
A.操作の頻度はミリ秒単位で指定します。
B.トラフィックを送信するための最適な送信元インターフェイスを特定するために使用されます。
C.イネーブルモードで構成されています。
D. ICMP パケットの頻度を決定するために使用されます。
Answer: D
Explanation:
このモジュールでは、IPv4 または IPv6 を使用する Cisco ルータとデバイス間のエンドツーエンド応答時間をモニタするために、IP SLA（Service Level Agreements）インターネット制御メッセージプロトコル（ICMP）エコー動作を設定する方法について説明します。 ICMP Echo は、ネットワーク接続の問題のトラブルシューティングに役立ちます。 また、このモジュールは、ICMP エコー操作の結果を表示および分析して、ネットワーク IP 接続がどのように実行されているかを判断する方法を示します。
ICMP エコー操作
ICMP エコー操作は、Cisco ルータと IP を使用するすべてのデバイス間のエンドツーエンドの応答時間を測定します。 応答時間は、ICMP Echo 要求メッセージを宛先に送信してから ICMP Echo 応答を受信するまでの時間を測定することによって計算されます。
下の図では、ping は ICMP Echo 操作でソース IP SLA デバイスと宛先 IP デバイス間の応答時間を測定するために使用されます。 多くの顧客は、IP SLA ICMP ベースのオペレーション、社内の ping テスト、または応答時間測定のための ping ベースの専用プローブを使用します。
図 1. ICMP エコー操作



IP SLA ICMP エコー操作は、ICMP ping テストのための同じ IETF 仕様に準拠しており、2 つの方法は同じ応答時間になります。
ソースデバイスでの基本 ICMP エコー操作の設定
要約手順
1.有効にする
2.端末の設定
3. ip sla operation-number
4. icmp-echo {宛先 IP アドレス| 宛先 - ホスト名} [source-ip {ip-address | ホスト名} | ソースインターフェイスインターフェイス名]
5.周波数秒
6.終了

4.どのタイプのインターフェイスが PPPoE クライアントの IP アドレスをネゴシエートできますか?
A.イーサネット

B.ダイヤラー
C.シリアル
D.フレームリレー
Answer: B

5.スイッチスタッキングの利点はどれですか?
A.リソースの使用に影響を与えずに冗長性を提供します。
B.ホストの追加と削除を簡単にします。
C.高いニーズのアプリケーションのパフォーマンスを向上させます。
D.より高いリソース密度でより高いポート密度を提供します。
Answer: D
Explanation:
スタッカブルスイッチは、完全に機能するスタンドアロンのネットワークスイッチですが、1 つ以上の他のネットワークスイッチと一緒に動作するように設定することもできます。このスイッチグループは単一のスイッチの特性を示しますが、 組み合わされたスイッチの合計。