Cisco.350-401.v2023-11-06.q182

試験コード:	350-401
試験名称:	Implementing Cisco Enterprise Network Core Technologies (350-401 ENCOR)
認定資格:	Cisco
無料問題数:	182
バージョン:	v2023-11-06
アクセス数:	1566
ページビュー数:	1820
https://www.jpnpdf.com/Cisco.350-401.v2023-11-06.q182-mondaishu.html	

最新問題: **1**

展示を参照してください。ネットワーク エンジニアは show コマンドを設定して設定を確認します。出力によって何を確認できますか?

A. 最初のポケットが NAT をトリガーして NAT テーブルにエントリを追加しました

B. 160.1.1 1 から 10.1.1.10 への Telnet が開始されました。

C. R1 には NAT オーバーロード パラメータが設定されています

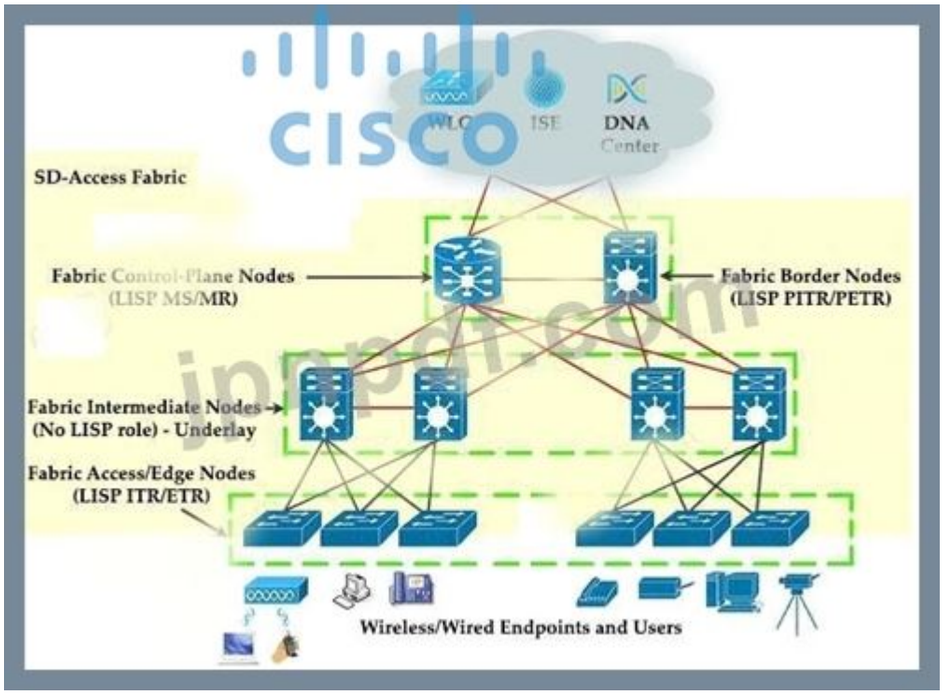
D. PAT オーバーロード パラメータを使用して設定される R1

Answer: A (メーッセージを残す**)**

最新問題: **2**

SD-Access 導入環境でファブリック エッジ ノードはどの機能を実行しますか?

A. SD-Access ファブリックを別のファブリックまたは外部レイヤ 3 ネットワークに接続します。
B. エンドポイントをファブリックに接続し、トラフィックを転送します。
C. ファブリック アンダーレイに到達可能境界ノードを提供します
D. エンドユーザー データ トラフィックを LISP にカプセル化します。
Answer: (解答を表示する**)**
説明
ファブリック オーバーレイには、次の 5 つの基本的なデバイスの役割があります。
+ コントロール プレーン ノード: このノードには、ファブリック オーバーレイのエンドポイントからロケーション (EID から RLOC) へのマッピング システムを提供するための設定、プロトコル、およびマッピング テーブルが含まれています。
+ ファブリック境界ノード: このファブリック デバイス (コア層デバイスなど) は外部層に接続します
SDA ファブリックへの 3 つのネットワーク。
+ ファブリック エッジ ノード: このファブリック デバイス (アクセス レイヤ デバイスやディストリビューション レイヤ デバイスなど) は、有線エンドポイントを SDA ファブリックに接続します。
+ ファブリック WLAN コントローラー (WLC): このファブリック デバイスは、AP とワイヤレス エンドポイントを SDA ファブリックに接続します。
+ 中間ノード: これらは、アンダーレイ サービス以外の SD-Access ファブリックの役割を一切提供しない中間ルーターまたは拡張スイッチです。



最新問題**: 3**
展示を参照してください。

DSW1 が VLAN 10 および 20 のルート ブリッジになることを保証する 2 つのコマンドはどれですか?

A. スパニングツリー mst 1 優先度 1

B. スパニングツリー mst 1 ルート プライマリ

C. スパニングツリー mstp vlan 10,20 ルート プライマリ

D. スパニングツリー MST VLAN 10,20 優先ルート

E. スパニングツリー mst 1 優先度 4096

Answer: B,E (メーッセージを残す)

Priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

最新問題**: 4**

展示を参照してください。

エンジニアは SW1 でモニタリングを設定し、show コマンドを入力して動作を確認します。出力は何を確認しますか?

A. SPAN セッション 1 は、リモート スイッチの VLAN 50 上のアクティビティを監視します。

B. RSPAN セッション 1 はモニタリング用に不完全に構成されています

C. SPAN セッション 2 は、ポート FastEthernet 0/15 に出入りするすべてのトラフィックを監視します。

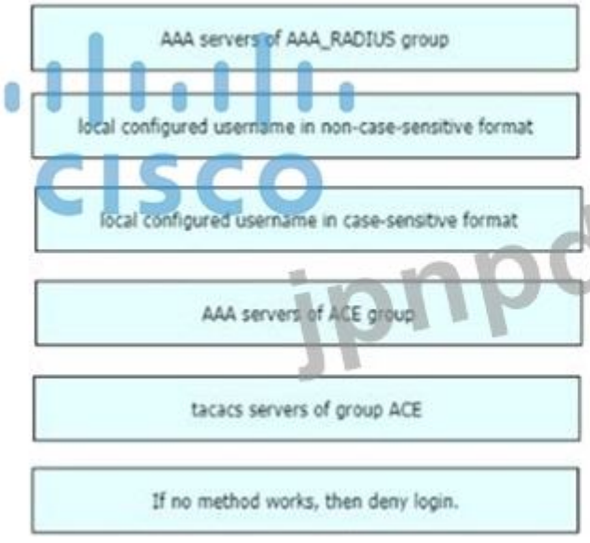
D. SPAN セッション 2 は、ポート FastEthernet 0/14 から出る出力トラフィックのみを監視します。

Answer: C (メーッセージを残す)

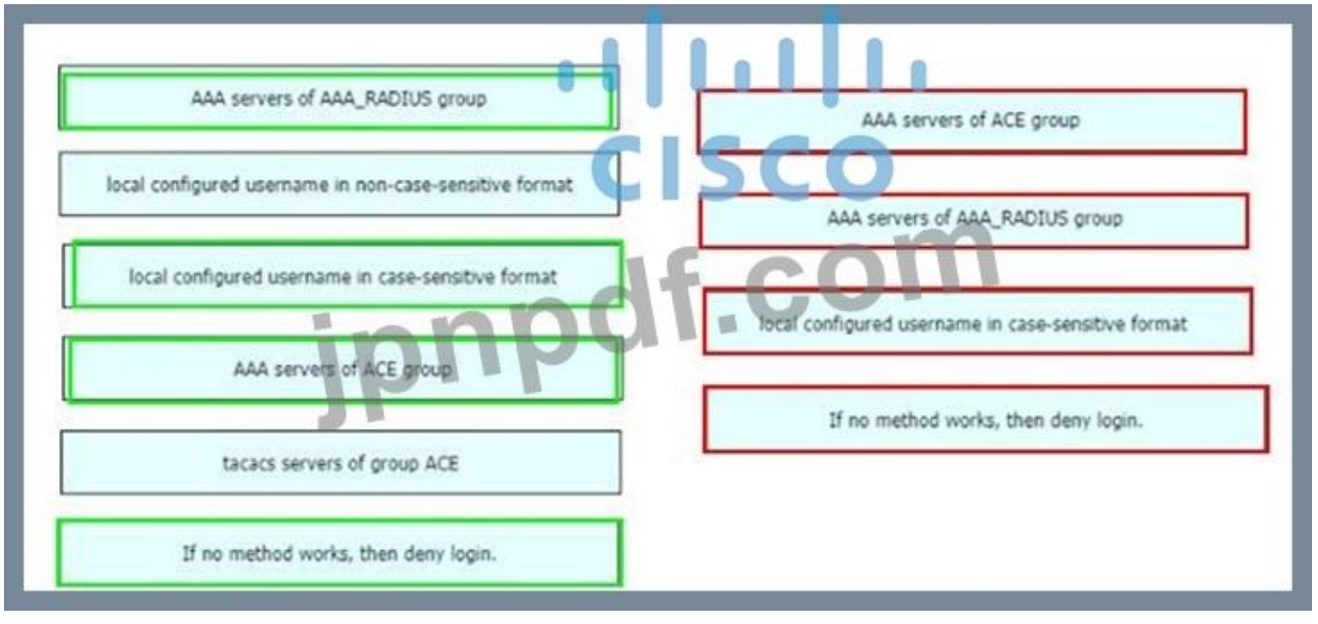
最新問題**: 5**

エンジニアは以下の構成を作成します。左側の認証方式を右側の優先順位にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。

```
R1#sh run | i aaa
aaa new-model
aaa authentication login default group ACE group AAA_RADIUS local-case
aaa session-id common
R1#
```



Answer:



最新問題**: 6**

NETCONF 経由で YANG データ モデルを操作するために使用される Python ライブラリはどれですか?

A. いいえ

B. cURL

C. 郵便配達員

D. リクエスト

Answer: A (メーッセージを残す**)**

最新問題**: 7**

展示を参照してください。

ネットワーク管理者は、すべての RADIUS サーバーが到達不能な場合に構成変更を実行できる必要があります。ユーザーが正常に認証された場合、すべてのコマンドを許可できる構成はどれですか?

A. aaa 認証ログイン デフォルト グループ radius local none
B. aaa authorization exec デフォルト グループ半径 なし
C. aaa authorization exec のデフォルトのグループ半径
D. aaa authorization exec デフォルト グループ半径 if-authenticated
Answer: (解答を表示する**)**

最新問題**: 8**
キャンパス ネットワークに QoS を実装する必要があることを示す 2 つのネットワーク問題はどれですか? (2 つお選びください)

A. ポートのフラッピング
B. 過剰なジッター
C. 誤ってルーティングされたネットワーク パケット
D. IP アドレスが重複しています
E. 帯域幅関連のパケット損失
Answer: B,D (メーッセージを残す**)**

最新問題**: 9**
展示を参照してください。

トランクは、Switch1 インターフェイス Giq1/0/20 と Switch2 インターフェイス Gig1/0/20 の間のバックツーバック リンクでは機能しません。どの構成で問題が解決しますか?

A)

```
Switch1(config)#interface gig1/0/20
Switch1(config-if)#switchport mode dynamic auto
```

B)

```
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic desirable
```

C)

```
Switch1(config)#interface gig1/0/20
Switch1(config-if)#switchport trunk native vlan 1
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport trunk native vlan 1
```

D)

```
Switch2(config)#interface gig1/0/20
Switch2(config-if)#switchport mode dynamic auto
```

A. オプション B
B. オプション C
C. オプション A
D. オプション D
Answer: A (メーッセージを残す**)**

最新問題**: 10**
Cisco DNA Center が提供する Intent API を定義する 2 つの特性はどれですか? (2つお選びください。)
A. ノースバウンド API
B. ビジネス成果重視
C. デバイス指向
D. サウスバウンド API

E. 手続き型

Answer: A,B (メーッセージを残す)

説明

Intent API は、Cisco DNA Center プラットフォームの特定の機能を公開する Northbound REST API です。Intent API は、ポリシーベースのビジネス意図の抽象化を提供し、個々のメカニズムのステップに苦労するのではなく、結果に集中できるようにします。

最新問題: **11**

DMVPN ソリューションでは、GRE トンネルの送信元と宛先が自動的に生成できるコンポーネントはどれですか?

A. QoS マーキング

B. 事前共有キー

C. ポリシー マップ

D. 暗号化 ACL

Answer: D (メーッセージを残す)

説明/参照:

最新問題: **12**

展示を参照してください。

データを形成する JSON 構文は何ですか?

A. 名前: ボブ、ジョンソン、年齢: 76、生きている: 本当、好きな食べ物。[シリアル、"マスタード」、"オニオン」}}

B. 名前'、'ボブ ジョンソン'、'年齢'、76、'生きている'、本当、'好きな食べ物' 'シリアル マスタード'、'玉ねぎ'}

C. {"名前":"ボブ ジョンソン","年齢":76,"生存":true,"お気に入り

食品":["シリアル","マスタード","玉ねぎ"]}正しい

D. 名前"、"ボブ ジョンソン"、"年齢"、76、"生きている"、true、"好きな食べ物"、["シリアル、"マスタード"、玉ねぎ"}}

E. 名前」、"ボブ ジョンソン」、"年齢」: 76 歳、"生きている」は本当、"好きな食べ物」、[シリアル]、[マスタード] "玉ねぎ"}}

Answer: C (メーッセージを残す)

説明

JSON データは、名前と値のペアとして書き込まれます。

名前と値のペアは、フィールド名 (二重引用符で囲んだ)、コロン、値で構成されます。

"名前":"マーク"

JSON では配列を使用できます。配列値は、文字列、数値、オブジェクト、配列、ブール値、または null 型である必要があります。
例えば：
{
"名前":"ジョン",
「年齢」:30、
「生きている」:本当、
"車":["フォード"、"BMW"、"フィアット"]
}

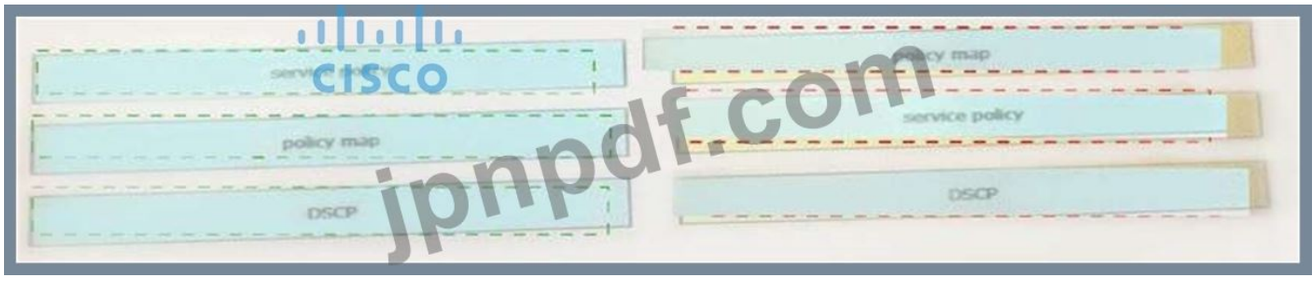
最新問題: **13**
Cisco DNA Center で、同様のネットワーク設定を持つデバイスに適用できる汎用設定を構築するために使用されるツールはどれですか?
A. テンプレートエディター
B. 認証テンプレート
C. コマンドランナー
D. アプリケーションポリシー
Answer: (解答を表示する**)**

最新問題: **14**
Cisco SD-Access ファブリックのファブリック データ プレーンはどのプロトコルまたはテクノロジーに基づいていますか?
A. LISP
B. IS-IS
C. Cisco TrustSec
D. VXLAN
Answer: (解答を表示する**)**
説明
ファブリック データ プレーンに使用されるトンネリング テクノロジーは、Virtual Extensible LAN (VXLAN) に基づいています。VXLAN カプセル化は UDP ベースです。つまり、任意の IP ベースのネットワーク (レガシーまたはサードパーティ) によって転送でき、SD-Access ファブリックのオーバーレイ ネットワークを作成できます。LISP は SD-Access ファブリックのコントロール プレーンですが、データ プレーンに LISP データ カプセル化を使用しません。代わりに、VXLAN カプセル化を使用します。これは、LISP では元のイーサネット ヘッダーをカプセル化して MAC-in-IP カプセル化を実行できるためです。VXLAN を使用すると、SD-Access ファブリックがレイヤ 2 およびレイヤ 3 の仮想トポロジ (オーバーレイ) をサポートし、組み込みのネットワーク セグメンテーション (VRF インスタンス/VN) と組み込みのグループベースを備えた任意の IP ベースのネットワーク上で動作できるようになります。ポリシー。
参考: CCNP および CCIE Enterprise Core ENCOR 350-401 公式認定ガイド

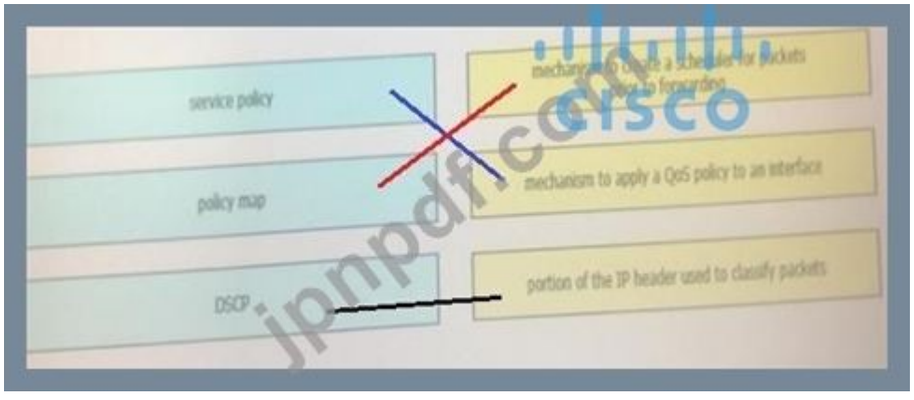
最新問題: **15**

左側の Qos メカニズムを右側の正しい説明にドラッグ アンド ドロップします。

Answer:

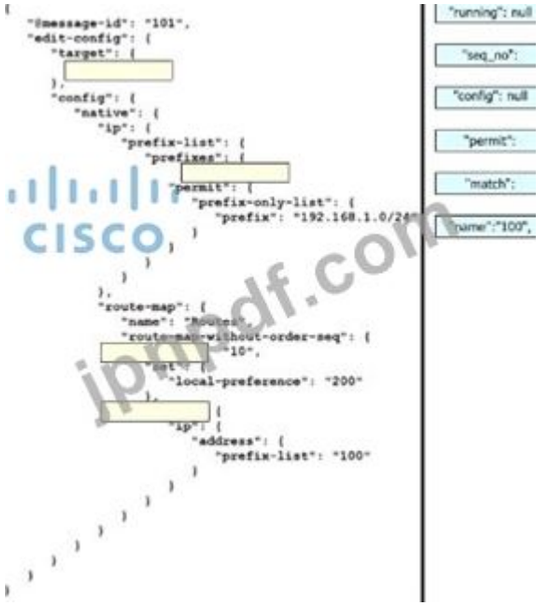


説明

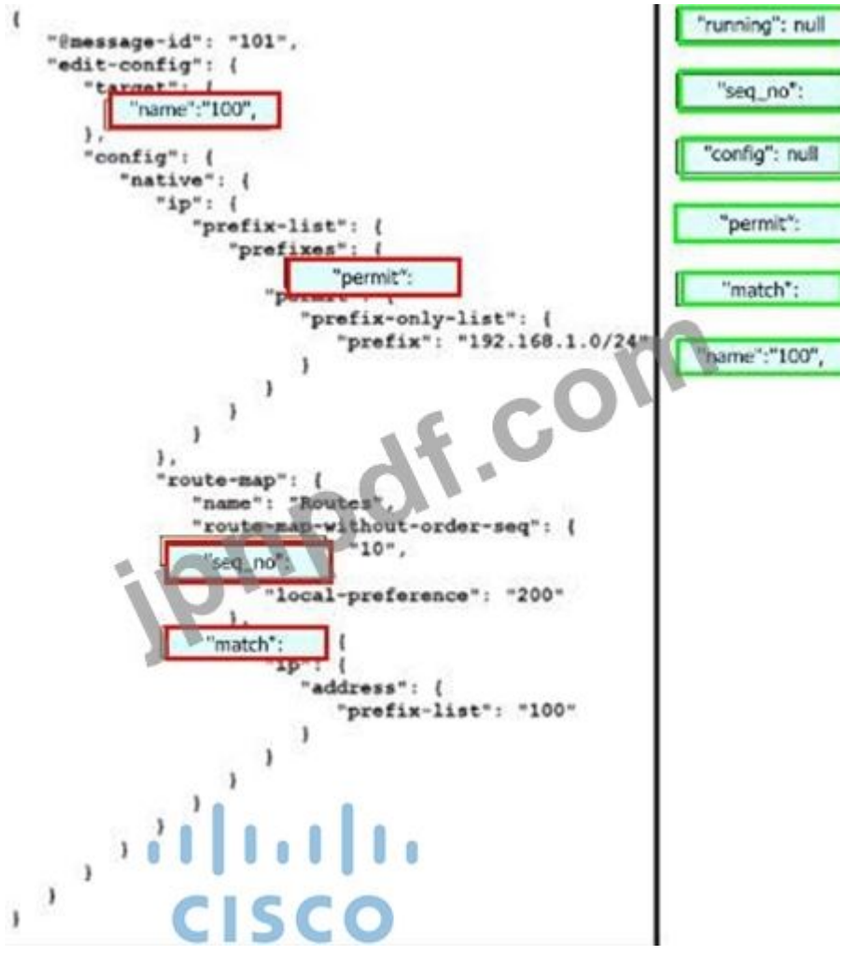


最新問題**: 16**

スニペットをコード内の空白にドラッグ アンド ドロップして、ルート マップにプレフィックス リストを追加し、ローカル プリファレンスを設定するスクリプトを作成します。すべてのオプションが使用されるわけではありません



Answer:



最新問題: 17
展示を参照してください。

エンジニアは、デフォルト設定を使用して Cisco ISE 上のゲスト ポータルを設計しています。テスト段階でゲスト ポータルを表示すると、エンジニアは警告を受け取ります。どの問題が発生していますか?
A. ポータルを提供しているサーバーには自己署名証明書があります。
B. サポートされていないブラウザを使用して接続しています
C. ポータルを提供しているサーバーの証明書の有効期限が切れています。
D. サポートされていないプロトコルを使用した接続です。
Answer: A (メーッセージを残す)

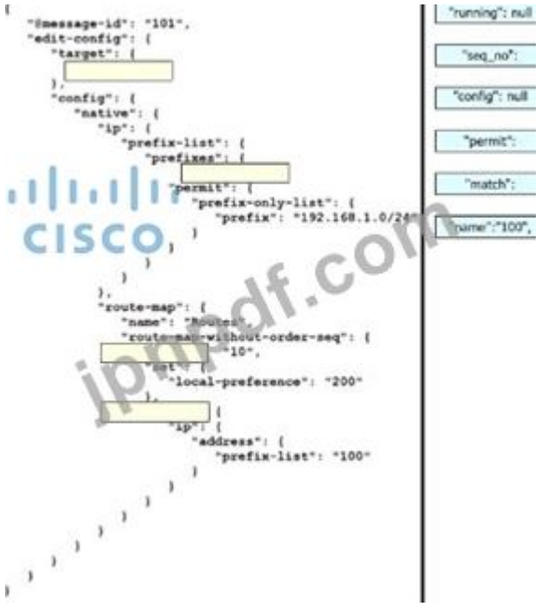
最新問題: 18
ワイヤレス ユーザーは、ワイヤレス ネットワークから頻繁に切断されると報告しています。ネットワーク エンジニアは、トラブルシューティングを行っているときに、ユーザーが切断した後、入力を必要とせずに接続が自動的に再確立されることに気付きました。エンジニアは、これらのメッセージ ログにも注目します。

```
AP 'AP2' is down. Reason: Radio channel set. 6:54:04 PM
AP 'AP4' is down. Reason: Radio channel set. 6:44:49 PM
AP 'AP7' is down. Reason: Radio channel set. 6:34:32 PM
```

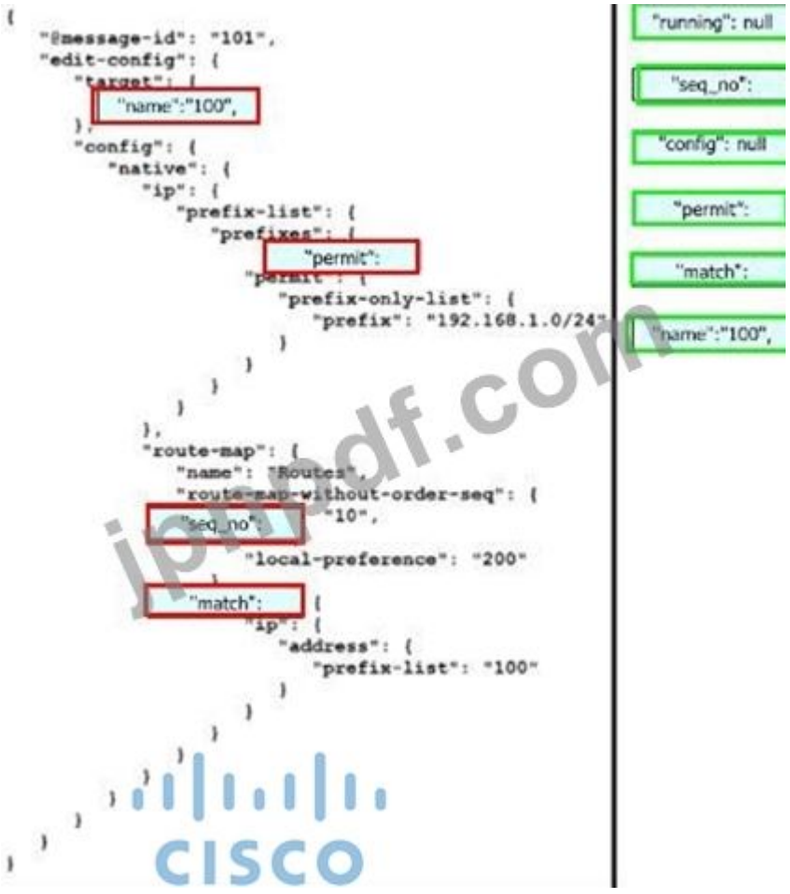
ユーザーへの影響を軽減するアクションはどれですか?
A. AP ハートビート タイムアウトを増やします。
B. BandSelect を増やす
C. カバレッジホール検出を有効にする
D. 動的チャネル割り当て間隔を長くします。

Answer: D (メーッセージを残す)
説明
これらのメッセージ ログは、無線チャネルが
リセットされています (AP は短時間ダウンしている必要があります)。と
動的チャネル割り当て (DCA) により、無線は次のことができます。
あるチャンネルから別のチャンネルに頻繁に切り替わりますが、
混乱を引き起こします。デフォルトの DCA 間隔は 10 分です。
これはメッセージ ログの時刻と一致します。に
DCA 間隔を長くすると、DCA の数を減らすことができます。
ユーザーがラジオを変えるために切断された回数
チャンネル。

最新問題**: 19**
スニペットをコード内の空白にドラッグ アンド ドロップして、ルート マップにプレフィックス リストを追加し、ローカル プリファレンスを設定するスクリプトを作成します。すべてのオプションが使用されるわけではありません

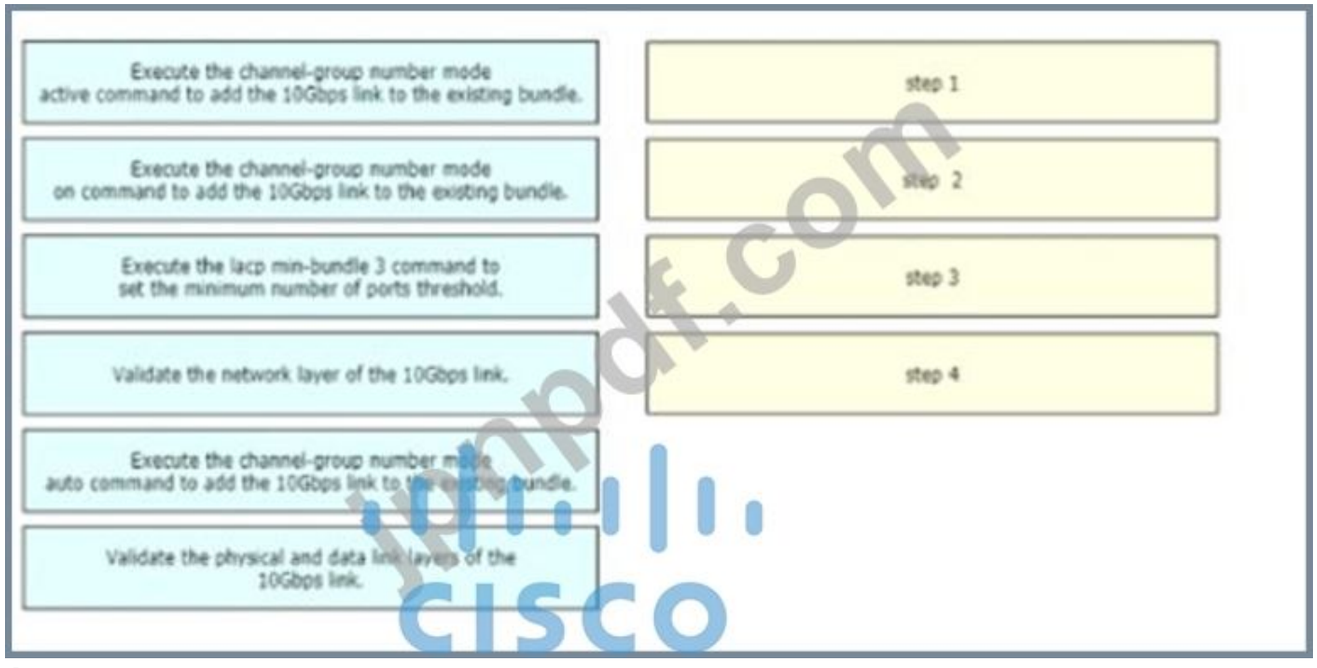


Answer:



最新問題**: 20**

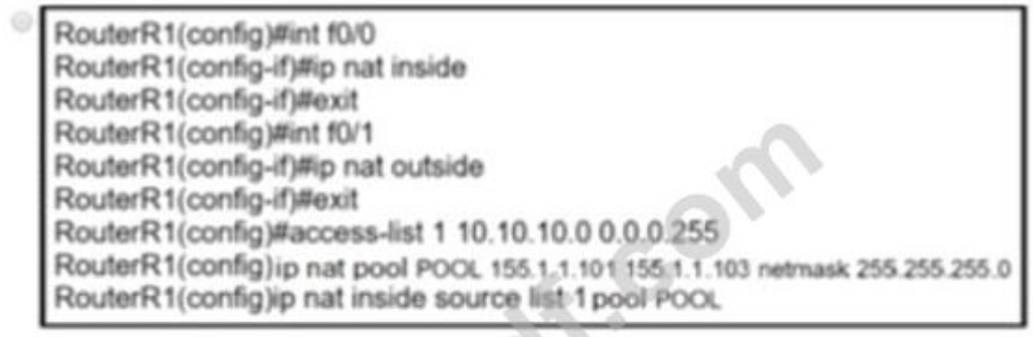
ネットワーク エンジニアは、既存の 2x10Gps LACP ベースの LAG に追加の 10Gps リンクを追加して、その容量を増強しています。ネットワーク標準では、メンバー リンクの 1 つがダウンした場合、バンドル インターフェイスのサービスを停止し、運用ネットワークへの影響を最小限に抑えて新しいリンクを追加する必要があります。エンジニアが実行する必要があるタスクを左側から右側のシーケンスにドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。

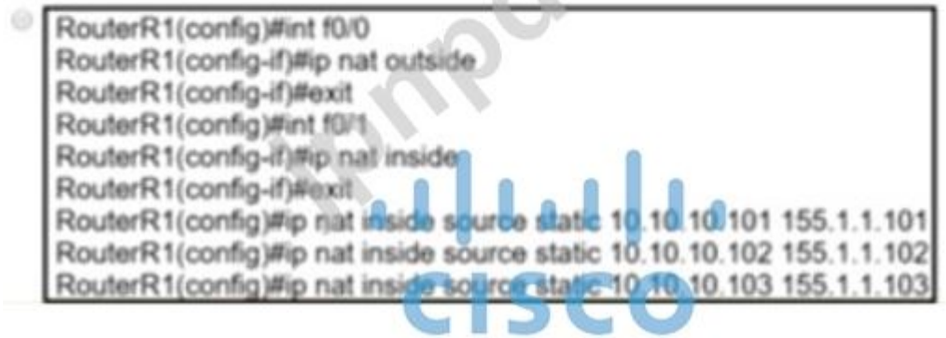


Answer:

最新問題**: 21**

展示を参照してください。ルーター r R1 上のどのコマンド セットが、プライベート ホスト PC1、PC2、および PC3 からパブリック スペースのアドレスへの決定論的な変換を許可しますか?





A. オプション D
B. オプション B
C. オプション A
D. オプション C
Answer: C (メーッセージを残す**)**

最新問題: **22**
展示を参照してください。

```
R1#debug ip ospf hello
R1#debug condition interface Fa0/1
      Condition 1 Set
```

OPSF デバッグ出力について正しいのはどれですか?
A. 出力には、ルータ R1 がすべてのインターフェイスで送受信したすべての OSPF メッセージが表示されます。
B. 出力には、ルータ R1 が送信してインターフェイス Fa0/1 で受信したすべての OSPF メッセージが表示されます。
C. 出力には、ルータ R1 が送受信した OSPF hello および LSACK メッセージが表示されます。
D. 出力には、ルータ R1 が送信し、インターフェイス Fa0/1 で受信した OSPF hello メッセージが表示されます。
Answer: D (メーッセージを残す**)**

最新問題: **23**
エンジニアは、設計ワークフローを使用して、Cisco DNA Center に新しいネットワーク インフラストラクチャを作成します。物理ネットワークデバイスの階層はどのように構成されていますか?
A. 場所別
B. 役割別
C. 組織別
D. ホスト名の命名規則による
Answer: (解答を表示する**)**
説明

最新問題: **24**
同期 EEM アプレット ポリシーを使用してテキストをアクティブ コンソールに直接表示する方法はどれですか?
A. イベントマネージャーアプレットブーム
イベント syslog パターン "UP"
アクション 1.0 は "コンソールへの直接ログ記録"を取得します
B. イベントマネージャーアプレットブーム
イベント syslog パターン "UP"
アクション 1.0 syslog 優先度 ダイレクト メッセージ "コンソールに直接ログを記録"
C. イベントマネージャーアプレットブーム
イベント syslog パターン "UP"
アクション 1.0 は "コンソールに直接ログを記録"します。
D. イベントマネージャーアプレットブーム

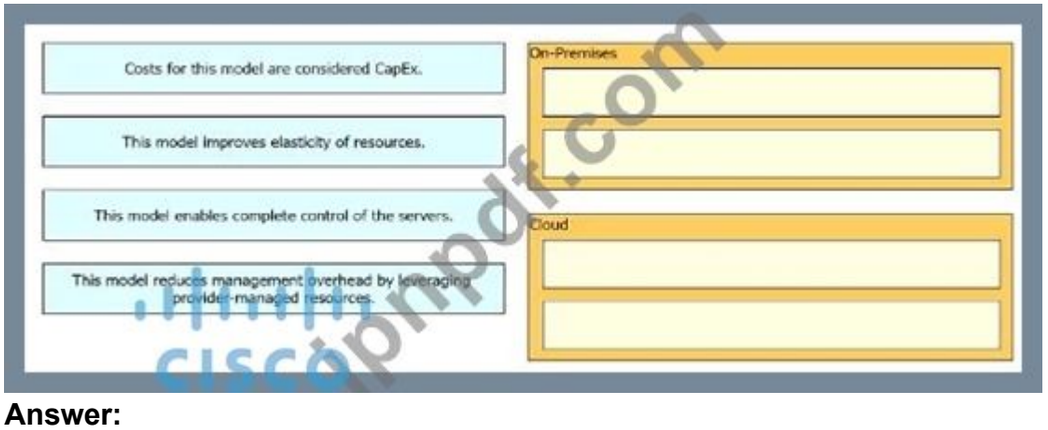
イベント syslog パターン「UP」
アクション 1.0 文字列「コンソールに直接ログを記録する」
Answer: B (メーッセージを残す)
Embedded Event Manager の実行時にデータをローカル tty に直接出力するアクションを有効にするには（EEM）アプレットがトリガーされる場合は、アプレット コンフィギュレーション モードで action put コマンドを使用します。
次の例は、データをローカル tty に直接出力する方法を示しています。

```
Router(config-applet)# event manager applet puts
Router(config-applet)# event none
Router(config-applet)# action 1 regexp "(.*) (.*) (.*)" "one two three" _match _sub1
Router(config-applet)# action 2 puts "match is $_match"
Router(config-applet)# action 3 puts "submatch 1 is $_sub1"
Router# event manager run puts
match is one two three
submatch 1 is one
Router#
```

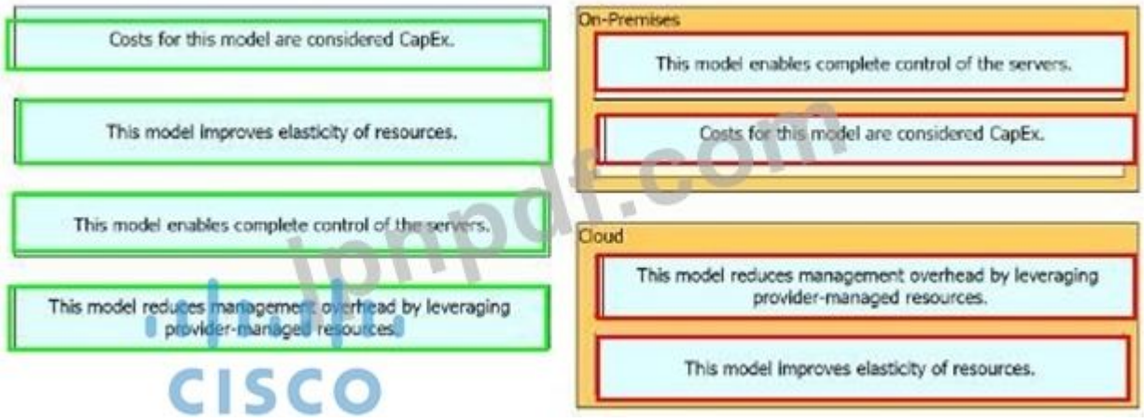
action puts コマンドは同期イベントに適用されます。このコマンドの出力は、
同期アプレットは、syslog をバイパスして、tty に直接表示されます。
参照：
a1.html

最新問題: **25**
Cisco SD-Access 導入におけるファブリック コントロール プレーン ノードの機能は何ですか?
A. ファブリック内のポリシーの適用とネットワークのセグメント化を担当します。
B. 従来の非ファブリック対応環境との統合を提供します。
C. ファブリック内のエンドポイントとネットワークを追跡する包括的なデータベースを保持します。
D. ファブリック内でトラフィックのカプセル化とセキュリティ プロファイルの適用を実行します。
Answer: D (メーッセージを残す)

最新問題: **26**
左側の特性を右側のインフラストラクチャ展開モデルにドラッグ アンド ドロップします。



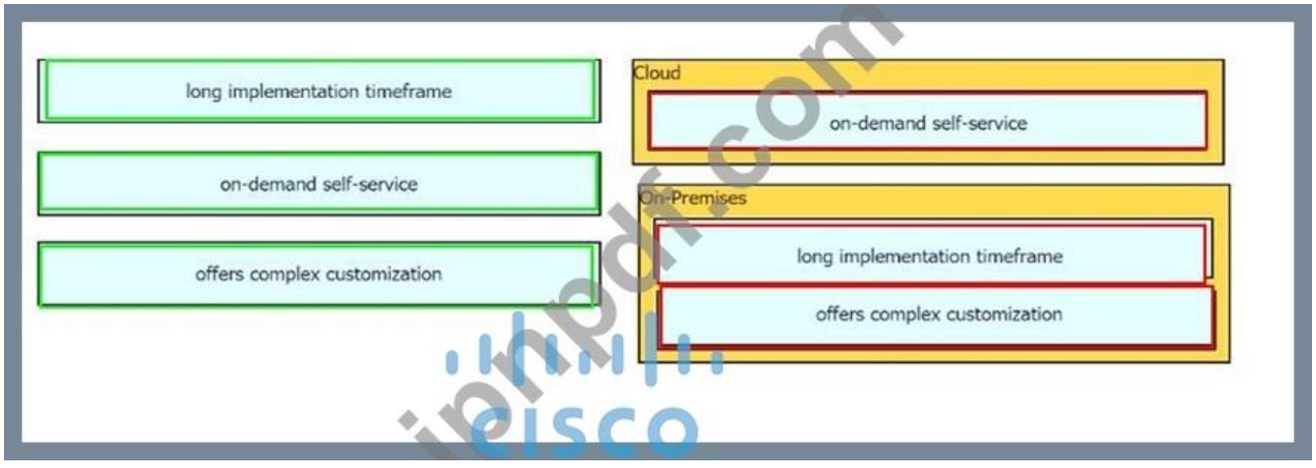
Answer:



最新問題: **27**

左側の特性を右側の展開モデルにドラッグ アンド ドロップします。

Answer:



最新問題: **28**

データモデリング言語はどのように使用されますか

A. データを簡単に構造化、グループ化、検証、複製できるようにするため

B. 変更できない、有限で明確に定義されたネットワーク要素を表します。

C. インフラストラクチャ内の非構造化データのフローをモデル化します。

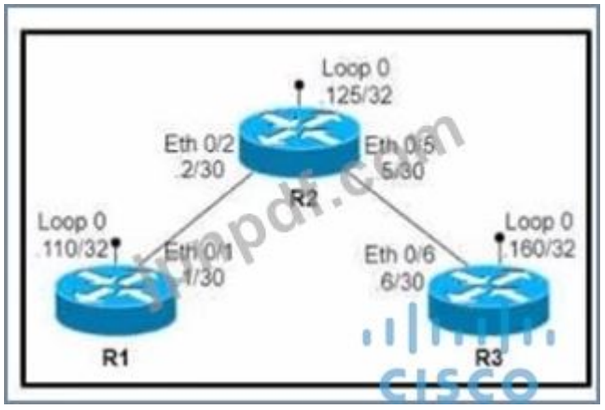
D. スクリプト言語に人間が読みやすいものを提供するため

Answer: D (メーッセージを残す)

replacing the process of manual configuration. Data models are written in a standard, industry-defined language. Although configurations using CLIs are easier (more human-friendly), automating the configuration using data models results in scalability.

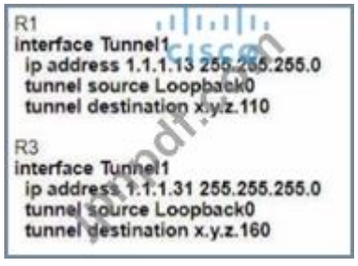
最新問題**: 29**

展示を参照してください。



エンジニアはすべてのルーター間のルーティングを構成し、GRE トンネル経由で R1 を R3 に接続するための構成を構築する必要があります どの構成を適用する必要がありますか?

A.



B.

C.

D.


Answer: D (メッセージを残す)

最新問題**: 30**

VXLAN における VTEP の機能は何ですか?

A. VXLAN ファブリック内のエンドホストの場所を動的に検出します。

B. VXLAN ヘッダーのルーティング アンダーレイとオーバーレイを提供します。

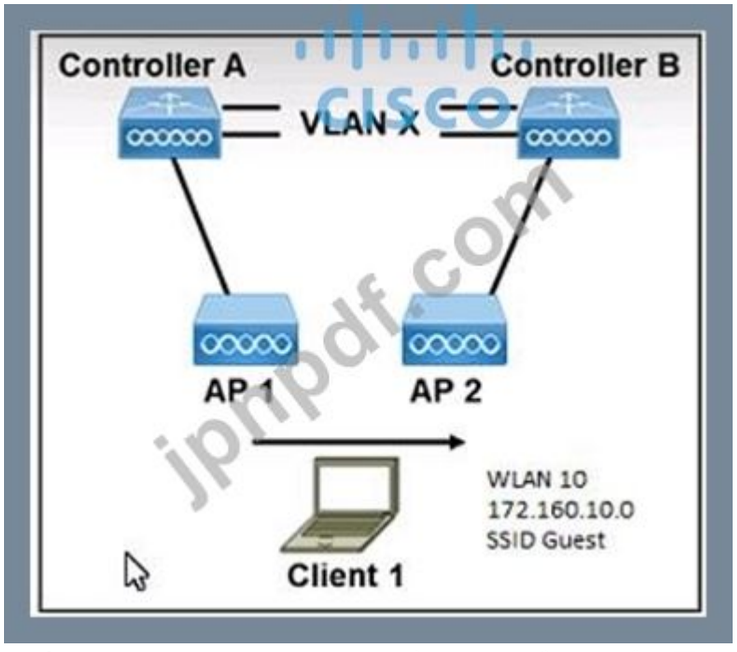
C. VXLAN ファブリックのエンドホストの場所を静的にポイントします。

D. VXLAN ファブリックへのトラフィックと VXLAN ファブリックからのトラフィックのカプセル化解除

Answer: D (メッセージを残す)

最新問題**: 31**

展示を参照してください。



両方のコントローラは同じモビリティ グループに属します。クライアント 1 が、同じ WLAN 内の異なるコントローラに登録されている AP 間をローミングすると、どのような結果が発生しますか?

A. コントローラ A とコントローラ B の間に CAPWAP トンネルが作成されます。

B. クライアント データベース エントリがコントローラ A からコントローラ B に移動します。

C. クライアント 1 は、EoIP トンネルを使用してコントローラ B に接続します。

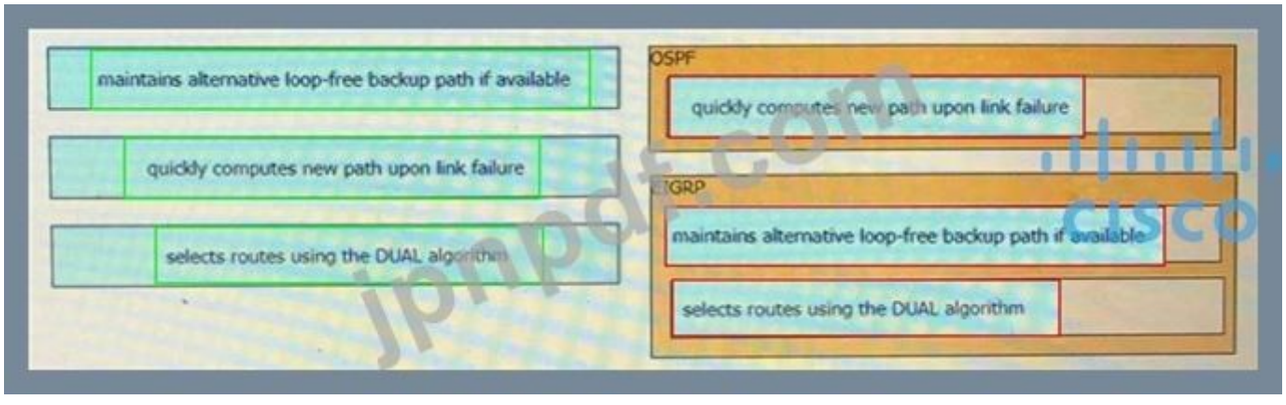
D. クライアント 1 は EoIP トンネルを使用してコントローラ A に接続します。

Answer: B (メッセージを残す)

最新問題: **32**

特性を左側から右側に説明されているルーティング プロトコルにドラッグ アンド ドロップします。

Answer:

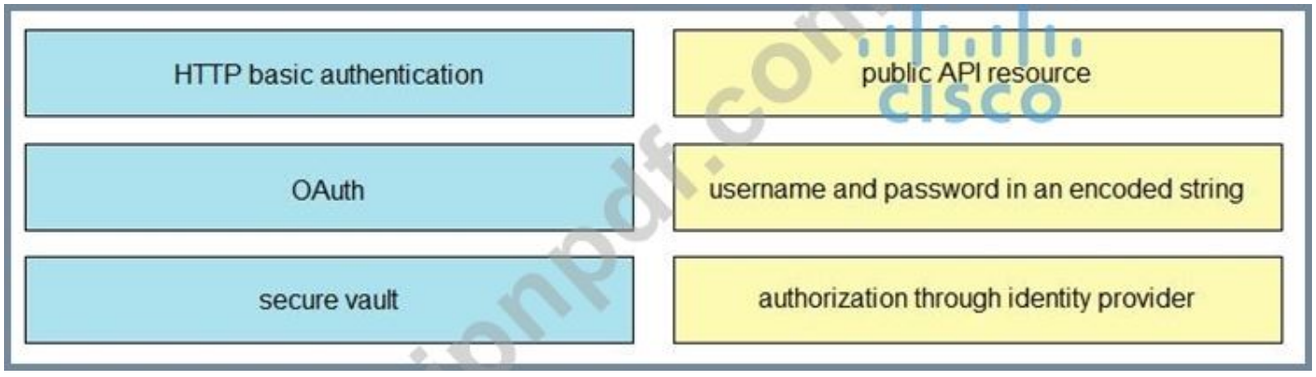


最新問題: **33**

左側の Qos メカニズムを右側の正しい説明にドラッグ アンド ドロップします。

Answer:

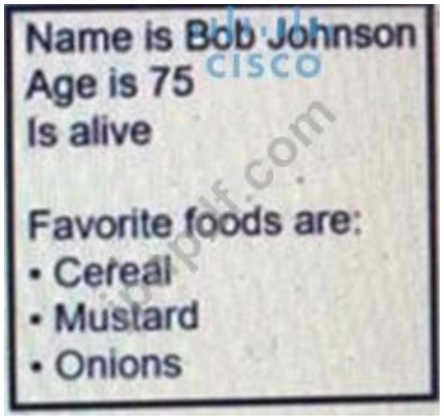
最新問題: **34**
左側の REST API 認証メソッドを右側の説明にドラッグ アンド ドロップします。



Answer:

最新問題: **35**
エージェントベースの構成管理ツールとエージェントレス構成管理ツールについて正しいのはどれですか?
A. エージェントレス ツールでは、マスターとスレーブ間のメッセージング システムは必要ありません。
B. エージェントベースのツールは、スレーブ ノードに Python や Ruby などの高級言語インタープリターを必要としません。
C. エージェントベースのツールでは、スレーブ ノードに追加のソフトウェア パッケージをインストールする必要はありません。
D. エージェントレス ツールは、プロキシ ノードを使用してスレーブ ノードとインターフェイスします。
Answer: (解答を表示する**)**

最新問題: **36**
展示を参照してください。



データから形成される Json 構文は何ですか?

A. {"名前": "ボブ ジョンソン"、"年齢": 75 歳、"生きている": true、"好きな食べ物": ["シリアル"、"マスタード"、"玉ねぎ"]}

B. {"~名前": "~ボブ ジョンソン"、"~年齢": 75、"~生きている": True、"~好きな食べ物": "~シリアル"、"~マスタード"、"~玉ねぎ' }

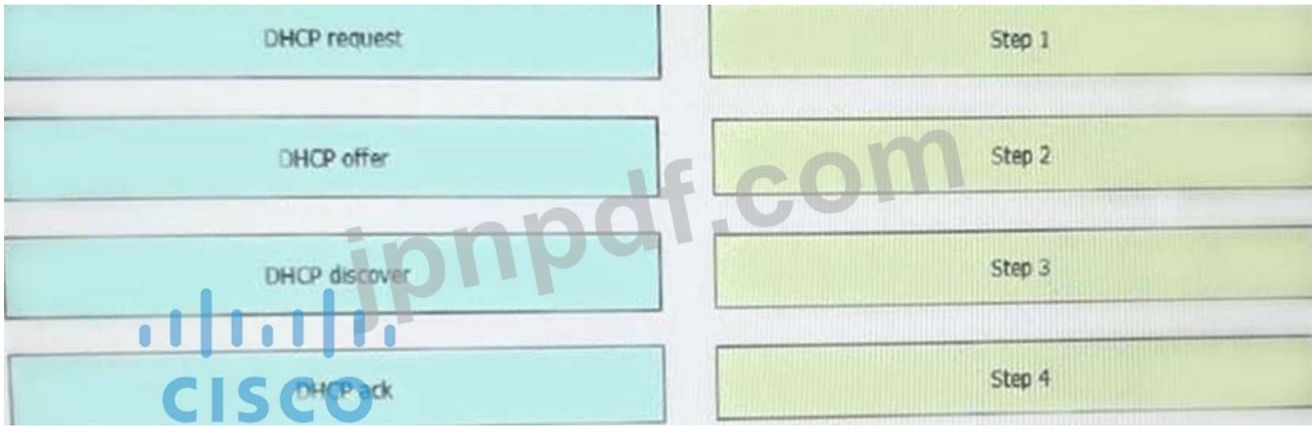
C. {名前: ボブ ジョンソン、年齢: 75、生きていること: true、好きな食べ物: [シリアル、マスタード、玉ねぎ]}

D. {"名前": "ボブ ジョンソン"、"年齢": 75、"生きている": true、"好きな食べ物": ["シリアル"、"マスタード"、"玉ねぎ"]}

Answer: D (メーッセージを残す)

最新問題**: 37**

クライアントと AP の間で交換される DHCP メッセージを、右側の交換順序にドラッグ アンド ドロップします。



Answer:

説明

テーブルの説明が自動的に生成される

DHCP クライアントと DHCP サーバーの間では、DHCPDISCOVER、DHCPO FFER、DHCPREQUEST、および DHCPACKNOWLEDGEMENT の 4 つのメッセージが送信されます。

このプロセスは、DORA (Discover、Offer、Request、Acknowledgement) と略されることがよくあります。

最新問題**: 38**

展示を参照してください。

Python コード出力ではどの HTTP JSON 応答が得られますか?

A. 7.61

B. 名前エラー: 名前 ｢json｣が定義されていません

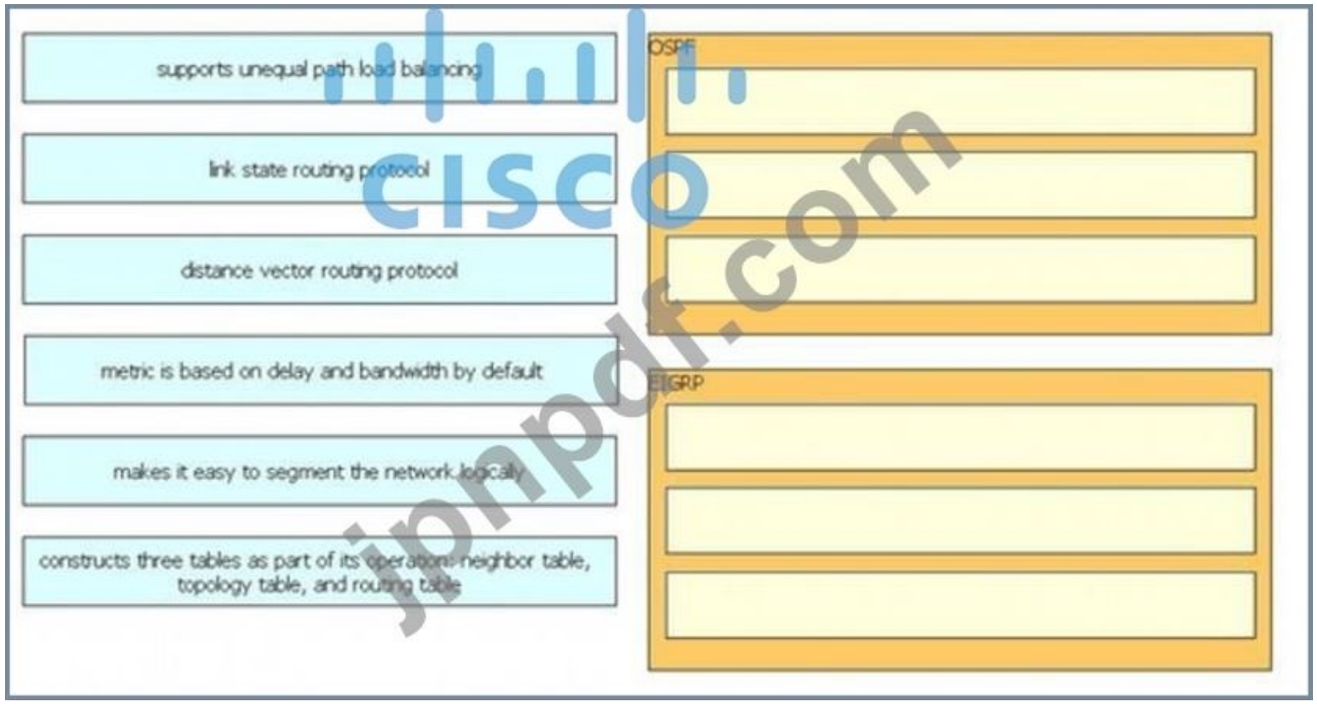
C. 7.0(3)I7(4)

D. KeyError 'kickstart_ver_str'

Answer: C (メーッセージを残す**)**

最新問題**: 39**

特性を左側から右側に説明されているルーティング プロトコルにドラッグ アンド ドロップします。



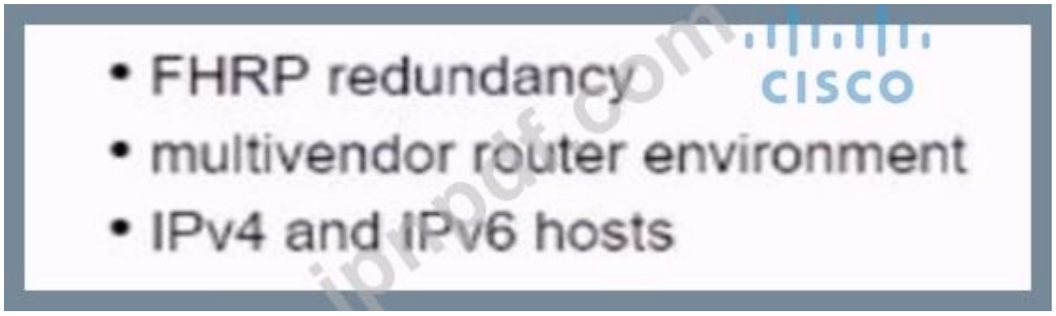
Answer:

説明

自動生成される図の説明

最新問題**: 40**

顧客は、次の要件をサポートするネットワーク設計を要求します。



設計にはどのプロトコルが含まれていますか?

A. GLBP

B. VRRPバージョン3

C. HSRP バージョン 2

D. VRRPバージョン2

Answer: (解答を表示する**)**

最新問題**: 41**

ワイヤレス受信信号強度インジケーターとは何ですか?

A. 受信した無線信号の強度をノイズレベルと比較した値

B. 送信電力、ケーブル損失、アンテナ ゲインを使用して、アンテナから送信されるワイヤレス信号の強さの値

C. 定義された距離にわたってどれだけ無線信号が失われるかという値

D. 疲れのない信号がどの程度後退するかを示す値 (dBm 単位で測定)

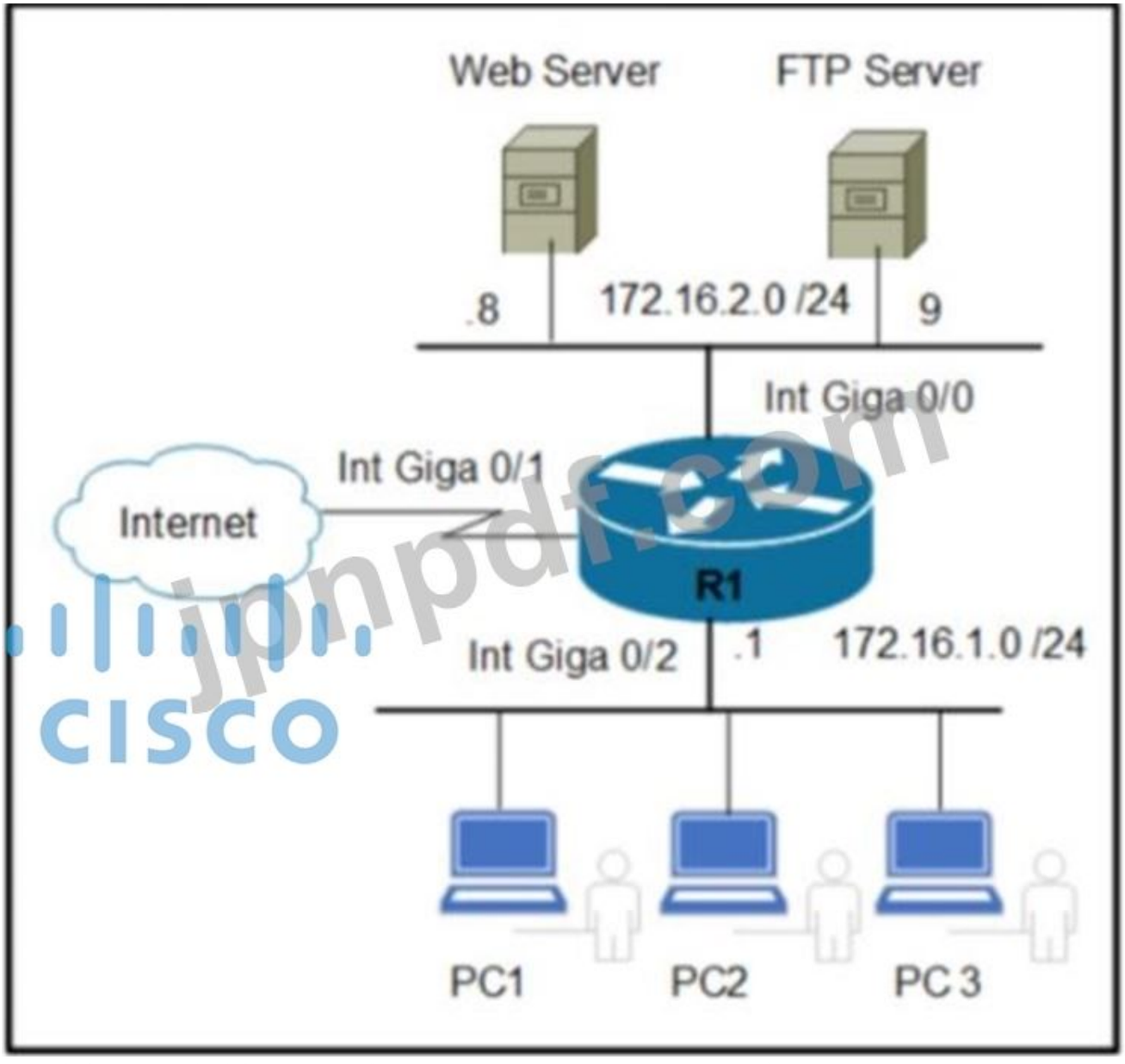
Answer: D (メーッセージを残す**)**

RSSI (受信信号強度インジケーター」) は、デバイスがアクセス ポイントまたはルーターからの信号をどの程度受信できるかを示す測定値です。これは、良好なワイヤレス接続を得るのに十分な信号があるかどうかを判断するのに役立つ値です。

この値は、0 (ゼロ) から -120 (マイナス 120) までのデシベル (dBm) で測定されます。0 (ゼロ) に近づくほど信号が強くなり、優れていることを意味します。通常、音声ネットワークには -65db 以上の信号レベルが必要ですが、データ ネットワークには -80db 以上が必要です。

最新問題**: 42**

私の出品物を参照してください。



展示を参照してください。エンジニアは、172.16.1.0 /24 上のユーザーから 172.16.2.0 /24 への FTP トラフィックを許可し、他のすべてのトラフィックをブロックする必要があります。どの構成を適用する必要がありますか?

A)

```
R1(config)# access-list 120 deny any any
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21
R1(config)#interface giga 0/0
R1(config-if)#ip access-group 120 out
```

B)

```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 in
```

C)

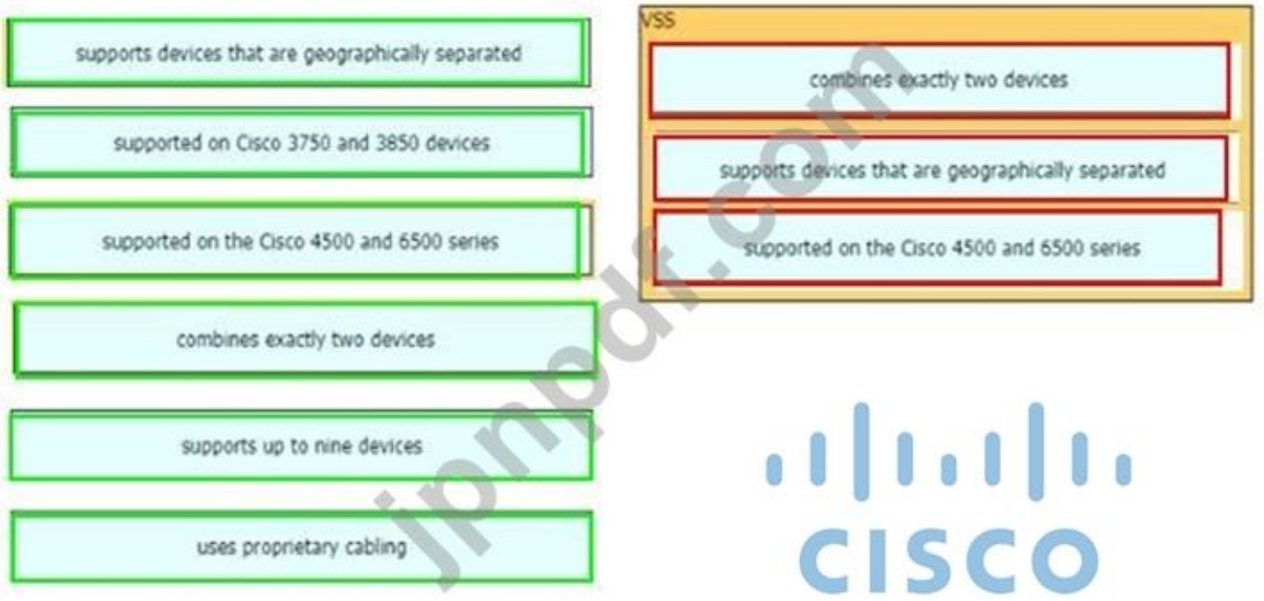
```
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 20
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 21
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 in
R1(config)# access-list 120 permit tcp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)# access-list 120 permit udp 172.16.1.0 0.0.0.255 21 172.16.2.0 0.0.0.255
R1(config)#interface giga 0/2
R1(config-if)#ip access-group 120 out
```

A. オプション C
B. オプション B
C. オプション A
D. オプション D
Answer: (解答を表示する**)**

最新問題**: 43**
Cisco SD-WAN の単一管理プレーンはどのコントローラですか?
A. vBond
B. vEdge
C. vSmart
D. vManage
Answer: D (メーッセージを残す**)**
参照：
Cisco SD-WAN ソリューションの主なコンポーネントは、vManage ネットワーク管理システム (管理プレーン)、vSmart コントローラ (コントロール プレーン)、vBond オーケストレータ (オーケストレーション プレーン)、および vEdge ルータ (データ プレーン) で構成されます。
+ vManage - この集中ネットワーク管理システムは、アンダーレイおよびオーバーレイ ネットワーク内のすべての Cisco SD-WAN デバイスとリンクを簡単に監視、設定、保守するための GUI インターフェイスを提供します。
+ vSmart コントローラー - このソフトウェアベースのコンポーネントは、SD-WAN ネットワークの集中コントロール プレーンを担当します。各 vEdge ルーターへの安全な接続を確立し、オーバーレイ管理プロトコル (OMP) を介してルートとポリシー情報を配布し、ルート リフレクターとして機能します。また、暗号キー情報を配布することで vEdge ルーター間の安全なデータ プレーン接続を調整し、非常にスケーラブルな IKE レスアーキテクチャを実現します。
+ vBond オーケストレーター - このソフトウェア ベースのコンポーネントは、vEdge デバイスの初期認証を実行し、vSmart と vEdge の接続を調整します。また、ネットワーク アドレス変換 (NAT) の背後にあるデバイスの通信を可能にするという重要な役割もあります。
+ vEdge ルーター - このデバイスは、ハードウェア アプライアンスまたはソフトウェア ベースのルーターとして利用でき、物理サイトまたはクラウドに設置され、1 つ以上の WAN トランスポートを介してサイト間に安全なデータ プレーン接続を提供します。トラフィック転送、セキュリティ、暗号化、サービス品質 (QoS)、ボーダー ゲートウェイ プロトコル (BGP) や Open Shortest Path First (OSPF) などのルーティング プロトコルなどを担当します。
2018年10月.pdf

最新問題: **44**
VSSテクノロジーの説明を左から右にドラッグアンドドロップします。すべてのオプションが使用されるわけではありません。

Answer:



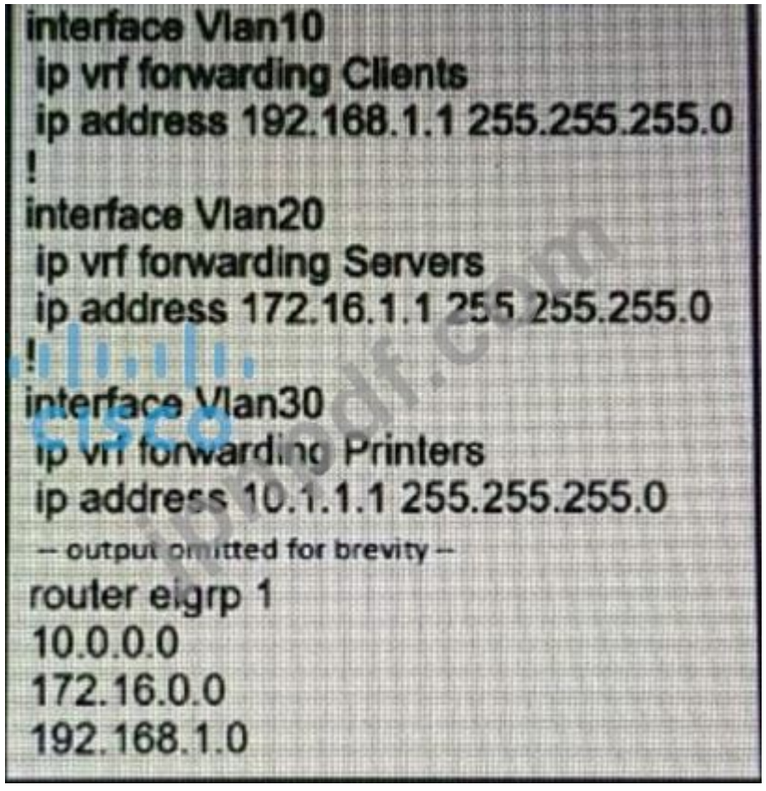
最新問題: **45**
Cisco Cyber Threat Defense ソリューションの Stealthwatch コンポーネントは何を提供しますか?
A. コアおよびアクセス ネットワークへの DDoS 攻撃を阻止するリアルタイムの脅威管理
B. ネットワーク上のユーザー、デバイス、トラフィックのリアルタイム認識
C. マルウェア制御
D. Web トラフィックの動的な脅威制御
Answer: B (メーッセージを残す**)**
説明

Cisco Stealthwatch は、大量のデータを収集して分析します。
最も大規模で最も動的なネットワークにも対応できるデータ
包括的な内部可視化と保護。助けになる
セキュリティ運用チームはリアルタイムの状況認識を獲得します
拡張ネットワーク上のすべてのユーザー、デバイス、トラフィックの
彼らは脅威に迅速かつ効果的に対応できます。」
ページ1
https://media.zones.com/images/pdf/cisco-stealthwatch-solution-overview.pdf

最新問題: **46**
左側の説明を右側のルーティング プロトコルにドラッグ アンド ドロップします。

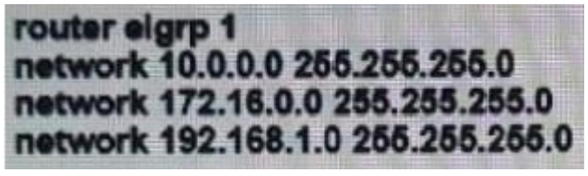
Answer:

最新問題: **47**



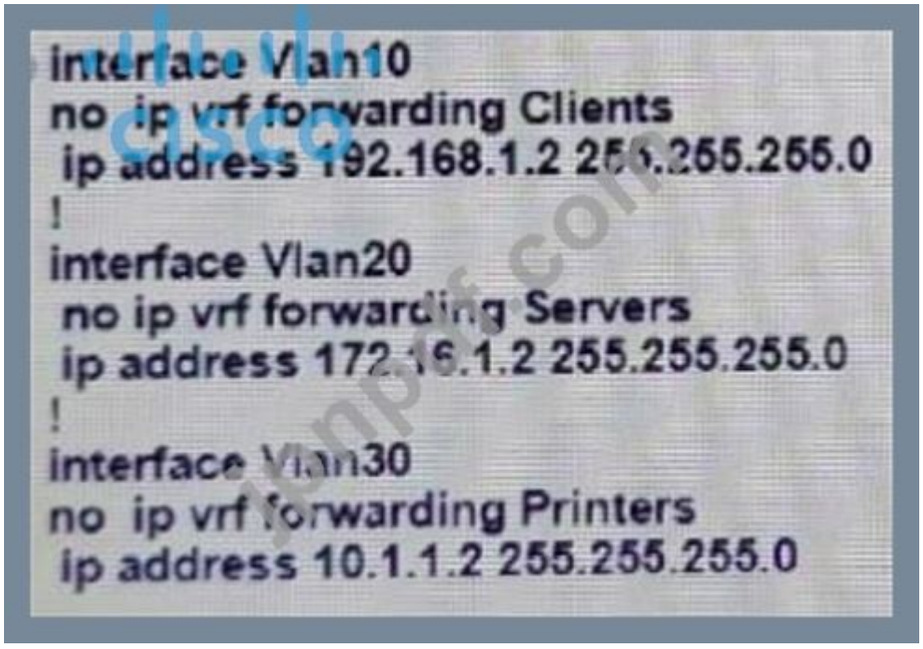
展示を参照してください。エンジニアは、クライアント、サーバー、プリンター間でパケットをルーティングするためにスティック上のルーターを構成しようとします。ただし、最初のテストでは、この構成が機能しないことが示されています。この問題を解決するコマンド セットはどれですか?

A)

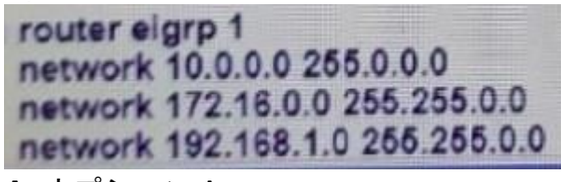


B)

C)



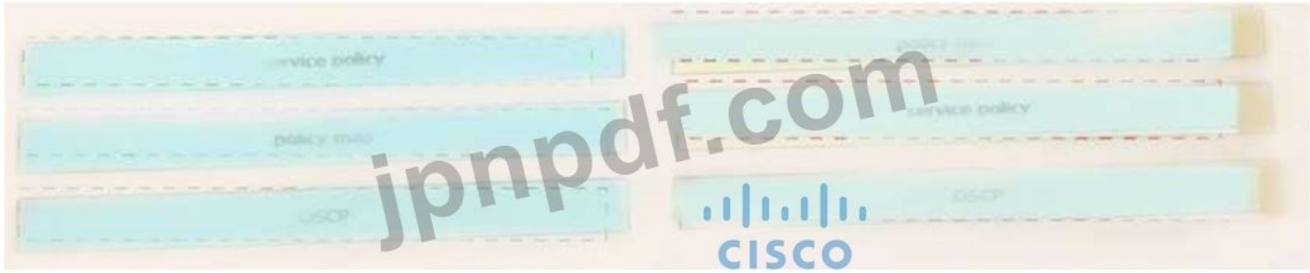
D)



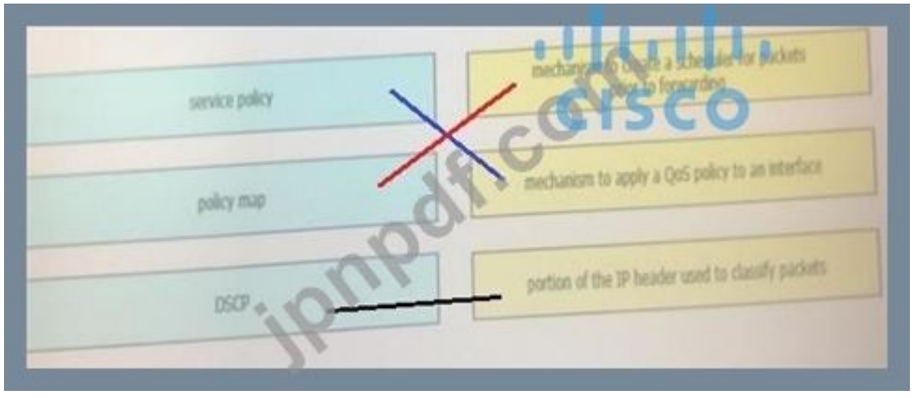
A. オプション A
B. オプション B
C. オプション C
D. オプション D
Answer: C (メーッセージを残す**)**
説明
VRF へのインターフェイスの割り当てまたは削除後は、IP アドレスを再設定する必要があります。それ以外の場合、そのインターフェイスには IP アドレスがありません。

最新問題**: 48**
左側の Qos メカニズムを右側の正しい説明にドラッグ アンド ドロップします。

Answer:



説明



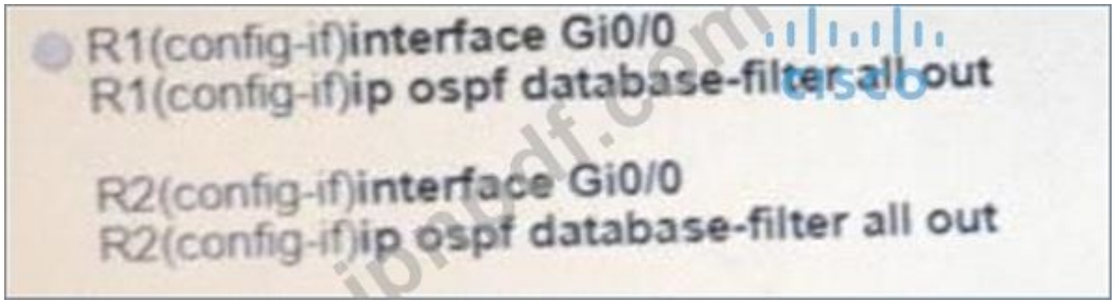
最新問題**: 49**

展示を参照してください。

ネットワーク エンジニアは、ルーター R1 とルーター R2 の間で OSPF を構成しています。エンジニアは、DR/BDR 選択がエリア 0 のギガビット イーサネット インターフェイスで発生しないことを確認する必要があります。この目標を達成できる設定セットはどれですか?

A.

B.


C.


D.


Answer: (解答を表示する**)**

ブロードキャスト ネットワークと非ブロードキャスト ネットワークは DR/BDR を選択しますが、ポイントツーポイント/

マルチポイントでは DR/BDR を選択しません。したがって、2 つの Gi0/0 を設定する必要があります。

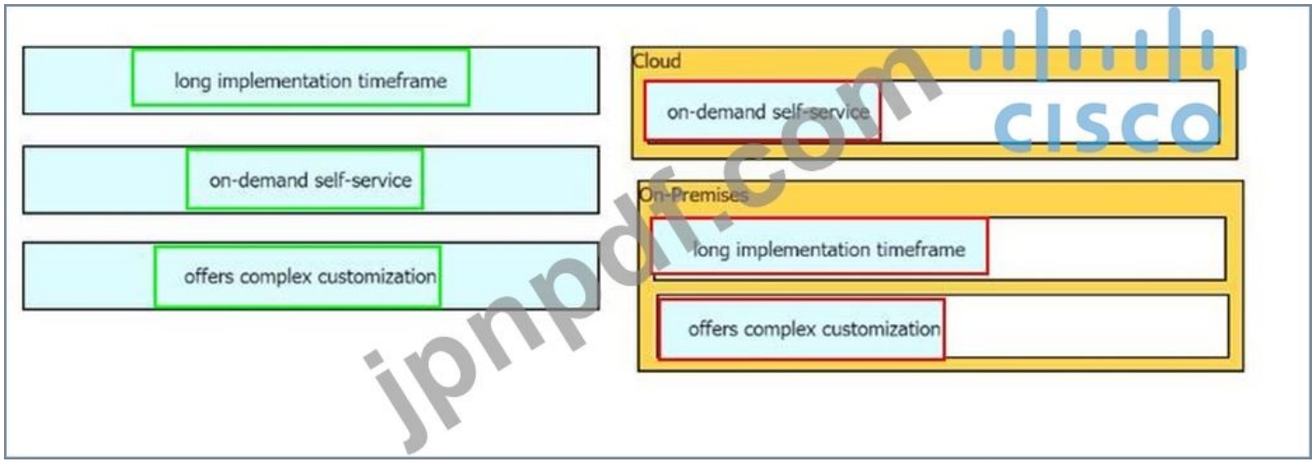
ポイントツーポイントまたはポイントツーマルチポイント ネットワークへのインターフェイスを提供し、DR/BDR が確実に機能するようにします。

選挙は起こらない。

最新問題**: 50**

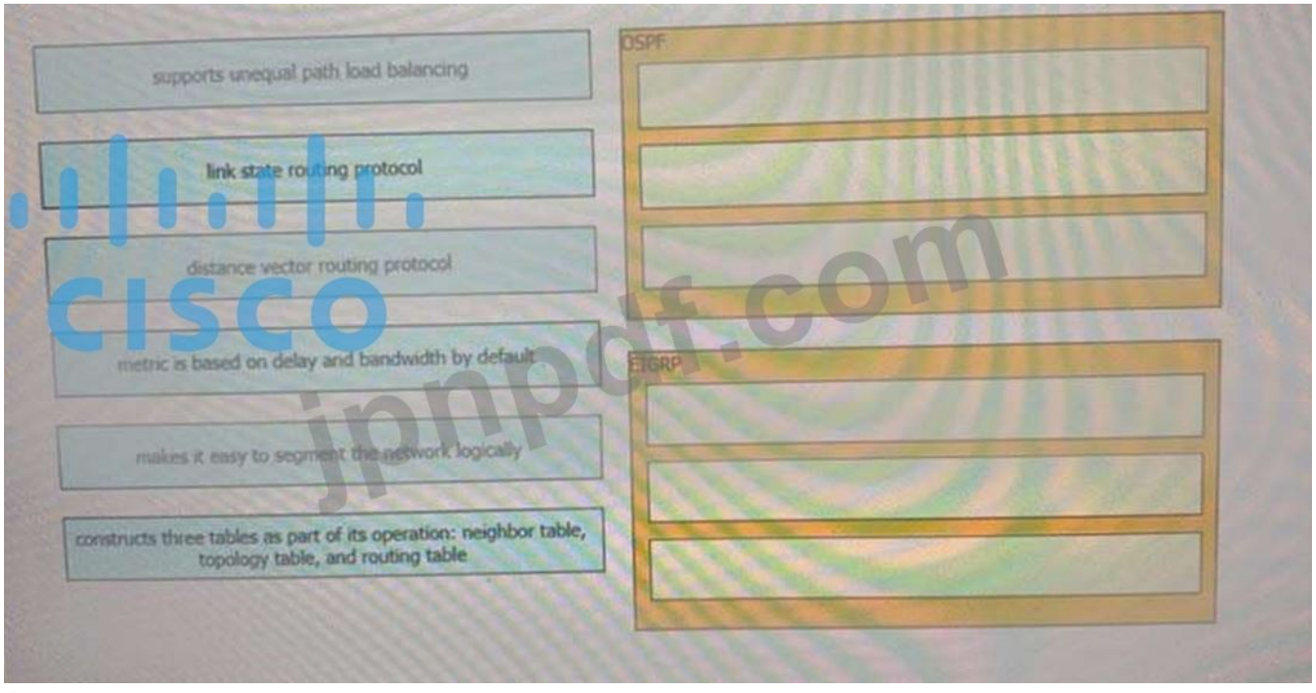
左側の特性を右側の展開モデルにドラッグ アンド ドロップします。

Answer:

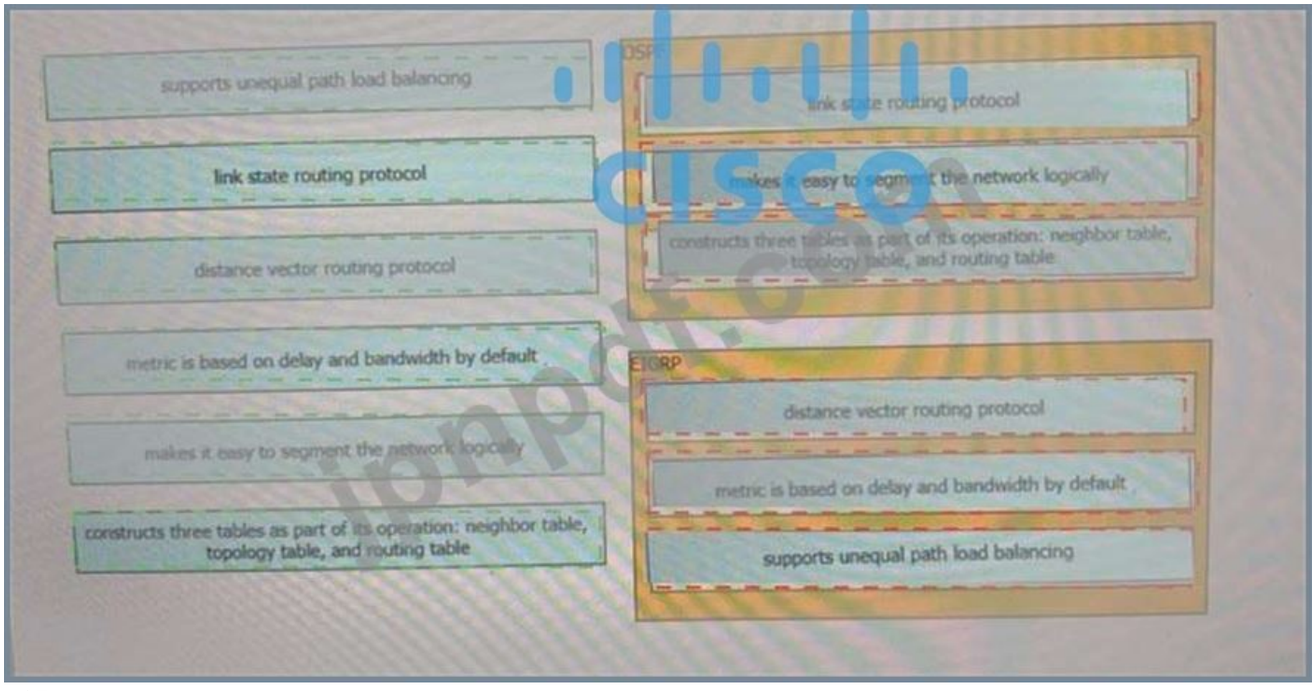


最新問題: **51**

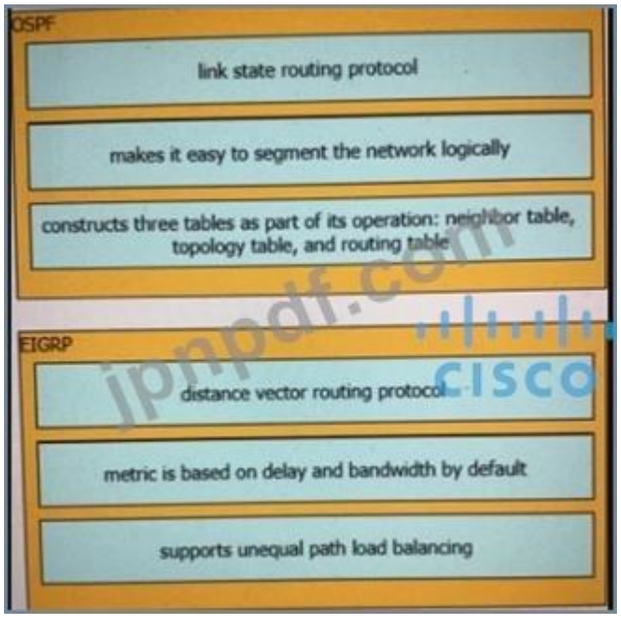
説明を左側から、右側に説明されているルーティング プロトコルにドラッグ ドロップします。



Answer:

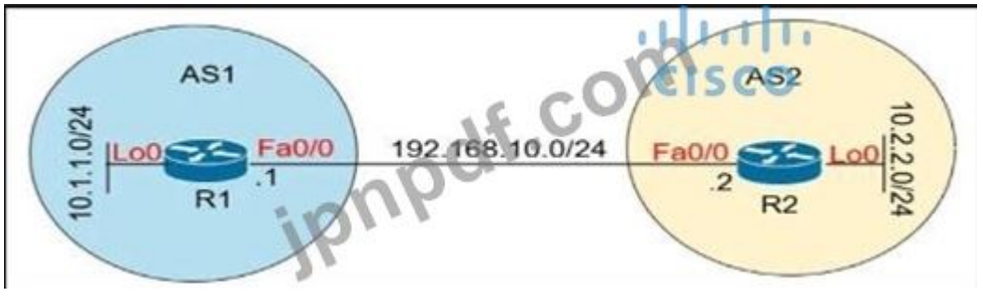


説明



最新問題**: 52**

展示を参照してください。



これら 2 つの直接接続された隣接ルータ間に EBGP ネイバーシップを確立し、BGP を介して 2 つのルータのループバック ネットワークを交換する構成はどれですか?

A)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

B)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

C)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.0.0.0 mask 255.0.0.0

R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.0.0.0 mask 255.0.0.0
```

D)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#neighbor 10.2.2.2 update-source lo0
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#neighbor 10.1.1.1 update-source lo0
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

A. オプション A

B. オプション B

C. オプション C

D. オプション D

Answer: (解答を表示する**)**

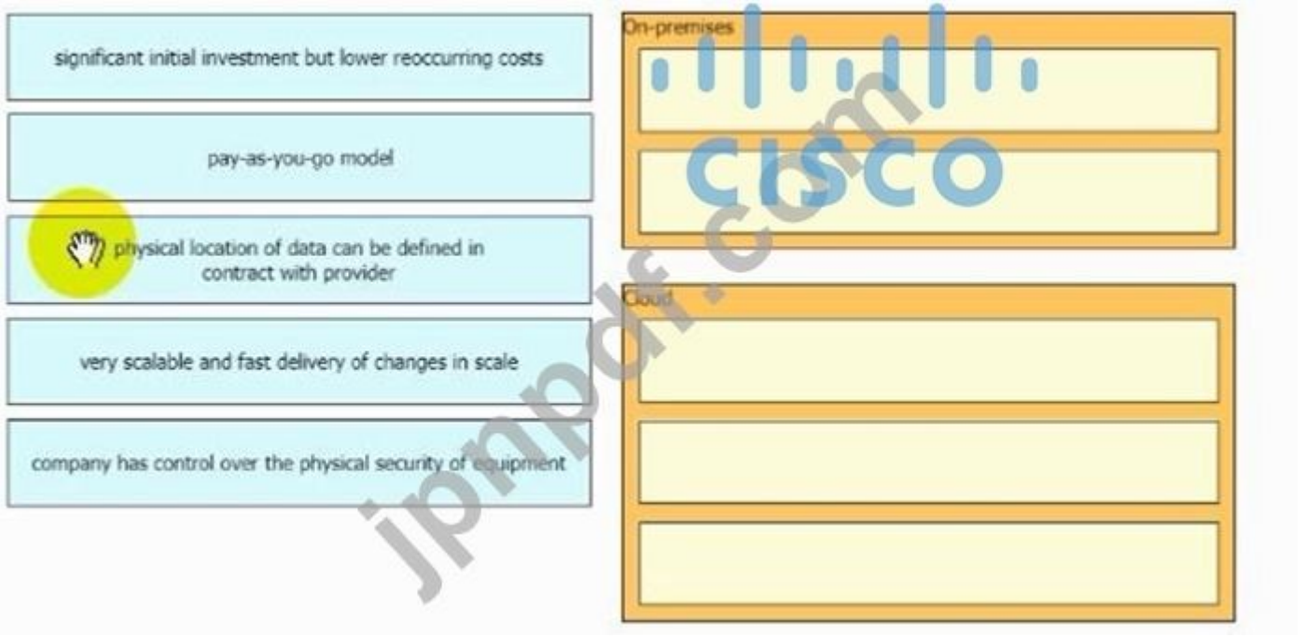
BGP では、 ſnetwork」コマンド (

この場合、R1 のネットワーク 10.1.1.0/24、R2 のネットワーク 10.2.2.0/24)。BGP は次の点で非常に厳格です。広告のルーティング。言い換えれば、BGP は正確に存在するネットワークのみをアドバタイズします。

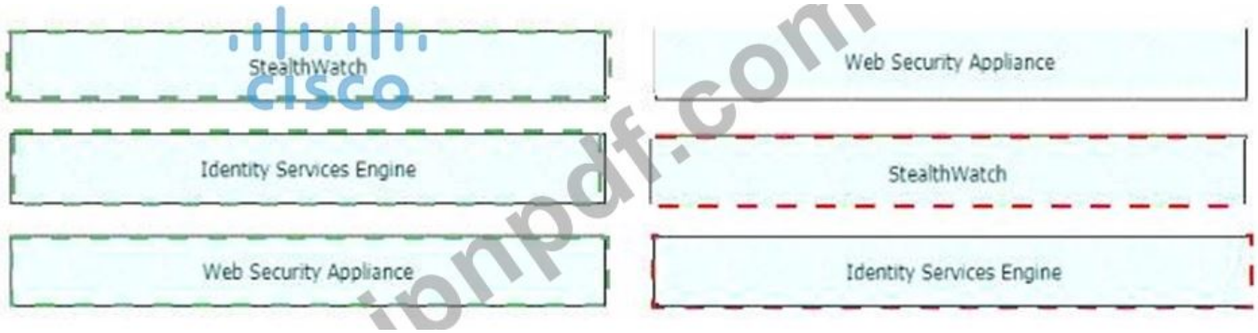
ルーティングテーブル。この場合、「network xx0.0 Mask 255.255.0.0」というコマンドを入力すると、
「ネットワーク x.0.0.0 マスク 255.0.0.0」または「ネットワーク xxxx マスク 255.255.255.255」の場合、BGP は機能しません。
何でも宣伝します。
直接リンクを介して eBGP 隣接関係を確立するのは簡単です。しかし、どのような場合に何が必要になるかを見てみましょう
ループバック インターフェイスを介して eBGP ネイバーシップを確立したいと考えています。2 つ必要になります
コマンド:
+ R1 上のコマンド「neighbor 10.1.1.1 ebgp-multihop 2」および「neighbor 10.2.2.2 ebgpmultihop」
R1 では 2"。このコマンドは、BGP アップデートが R1 に到達できるように、TTL 値を 2 に増やします。
2 ホップ離れた BGP ネイバー。
+ 'R1 (config) #router bgp 1 と応答します
R1 (構成ルーター) #neighbor 192.168.10.2 リモートとして 2
R1 (config-router) #network 10.1.1.0 マスク 255.255.255.0
R2 (構成) #router bgp 2
R2 (構成ルーター) #neighbor 192.168.10.1 リモートとして 1
R2 (config-router) #network 10.2.2.0 マスク 255.255.255.0
ワイヤレスの簡単な概要
Cisco アクセス ポイント (AP) は、自律モードまたは軽量モードの 2 つのモードのいずれかで動作できます。
+ 自律: 自給自足かつスタンドアロン。小規模な無線ネットワークに使用されます。
+ 軽量: Cisco 軽量 AP (LAP) が機能するには、ワイヤレス LAN コントローラ (WLC) に接続する必要があります。
LAP と WLC は、CAPWAP トンネルの論理ペアを介して相互に通信します。
- Control and Provisioning for Wireless Access Point (CAPWAP) は、制御に関する IETF 標準です。
AP と WLC 間のセットアップ、認証、および操作のためのメッセージング。CAPWAP は次のようなものです
LWAPP と異なりますが、次の違いがあります。
+CAPWAP は、認証と暗号化に Datagram Transport Layer Security (DTLS) を使用します。
AP とコントローラ間のトラフィックを保護します。LWAPP は AES を使用します。
+ CAPWAP には、動的な最大伝送単位 (MTU) 検出メカニズムがあります。
+ CAPWAP は UDP ポート 5246 (制御メッセージ) および 5247 (データ メッセージ) で実行されます。
LAP は、次の 6 つの異なるモードのいずれかで動作します。
+ ローカル モード (デフォルト モード): ノイズ フロアと干渉を測定し、侵入をスキャンします。
未使用チャネルでの 180 秒ごとの検出 (IDS) イベント
+ FlexConnect (以前はハイブリッド リモート エッジ AP (H-REAP) として知られていました) モード: データ トラフィックを許可します
ローカルで切り替えられ、コントローラーには戻りません。FlexConnect AP はスタンドアロンで実行可能
WLC に接続されていない場合でも、クライアント認証とスイッチ VLAN トラフィックをローカルで実行できます (ローカル

切り替わりました）。FlexConnect AP は、ユーザーの無線データと制御トラフィックの両方を（CAPWAP 経由で）トンネリングして、
集中型 WLC（中央スイッチ）。
+ モニター モード: クライアントとインフラストラクチャ間のデータ トラフィックは処理されません。それは次のように機能します
位置情報サービス (LBS)、不正 AP 検出、IDS 用のセンサー
+ 不正検出モード: 不正 AP を監視します。データはまったく扱いません。
+ スニファー モード: スニファーとして実行し、特定のチャネル上のすべてのパケットをキャプチャして転送します。
プロトコル分析ツール (Wireshark、Airopeek など) を使用して、
パケットを収集し、問題を診断します。トラブルシューティングの目的でのみ使用されます。
+ ブリッジ モード: WLAN と有線インフラストラクチャをブリッジします。
Mobility Express は、実際の WLAN の代わりにアクセス ポイント (AP) をコントローラとして使用する機能です。
コントローラ。ただし、このソリューションは、小規模から中規模、またはマルチサイトのブランチ ロケーションにのみ適しています。
専用の WLC に投資したくない場合もあります。Mobility Express WLC は最大 100 の Aps をサポートできます

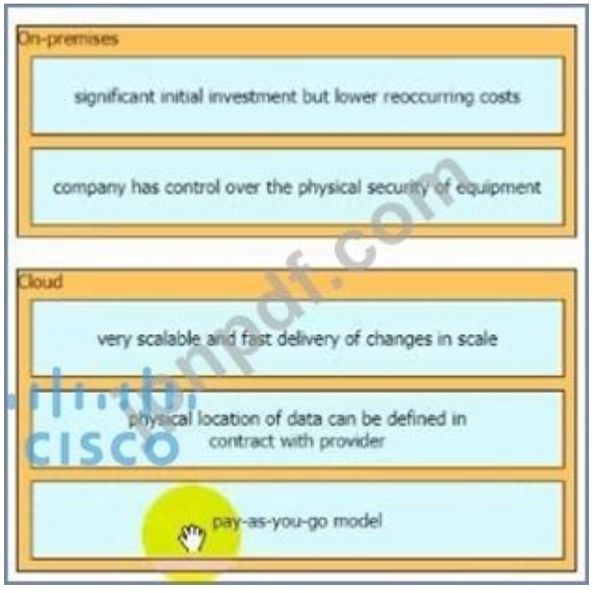
最新問題**: 53**
左側の特性を右側の適切なインフラストラクチャ展開タイプにドラッグ アンド ドロップします。



Answer:

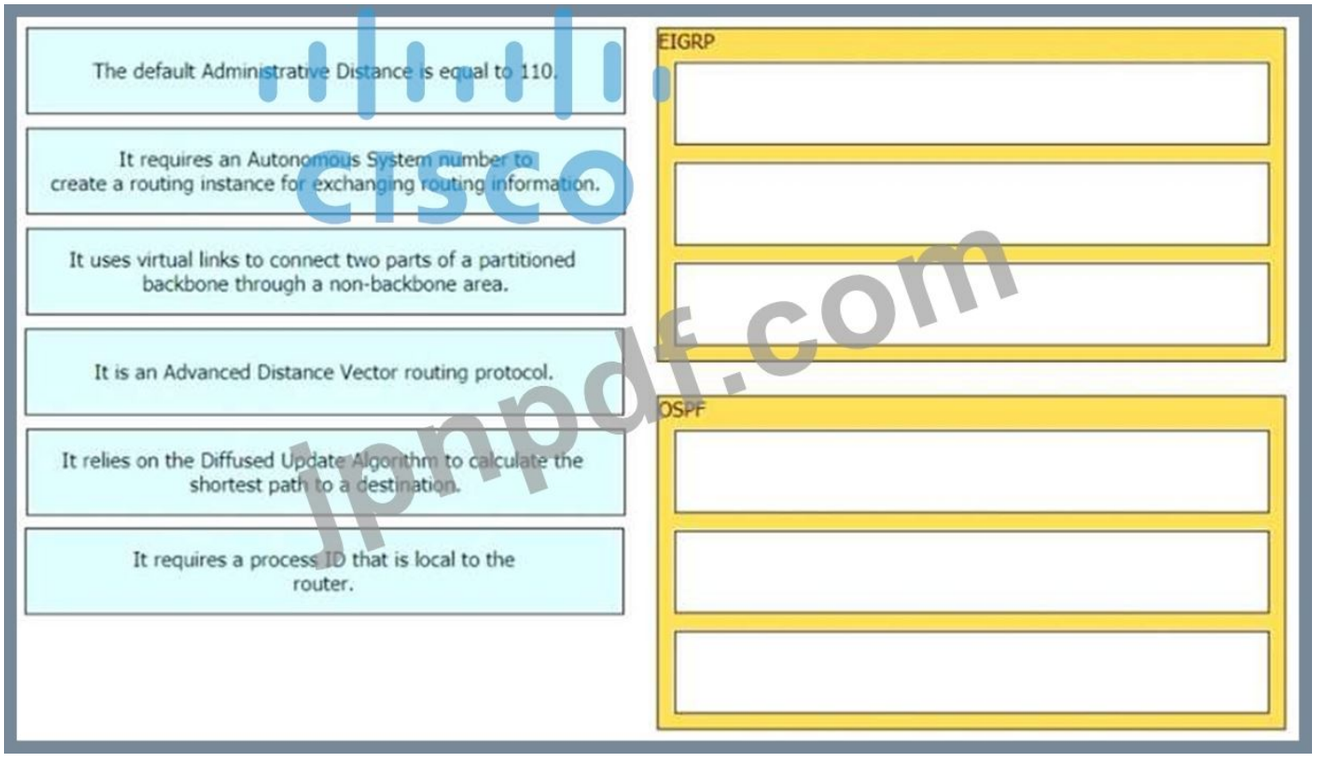


説明

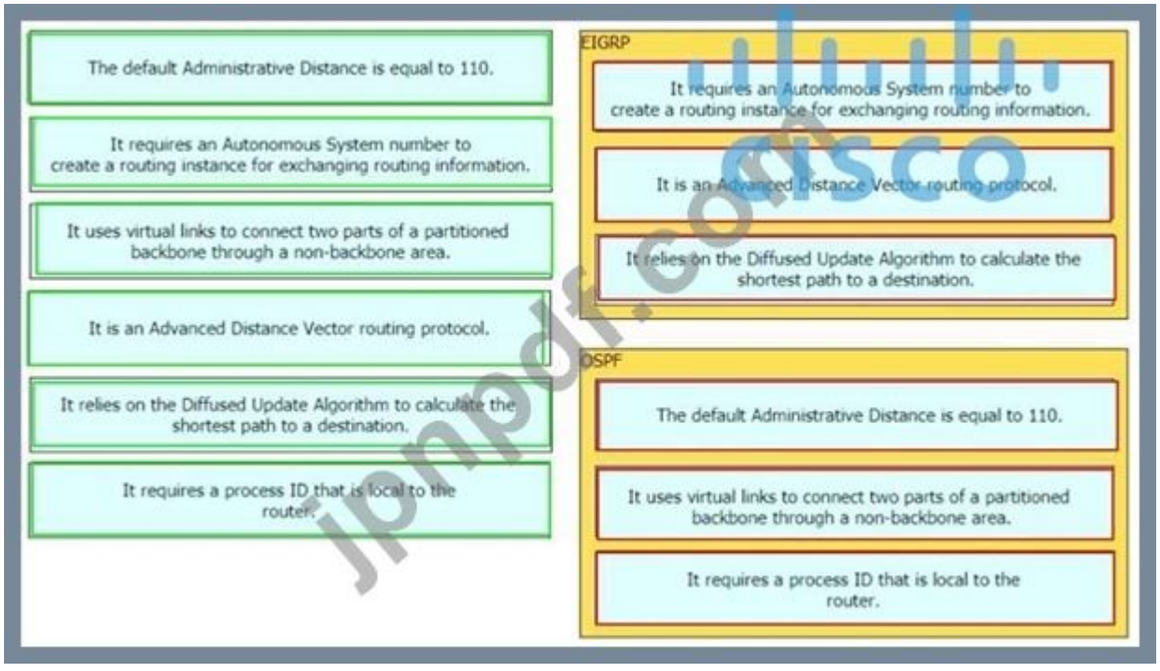


最新問題: **54**

特性を左側から右側に説明されているルーティング プロトコルにドラッグ アンド ドロップします。



Answer:



最新問題**: 55**

展示を参照してください。

```
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 172.16.30.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0          1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.11.29/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0          1         no          no            Base
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
  Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
```

ネットワーク エンジニアは OSPF を構成し、ルーター構成を確認します。どのインターフェイスが OSPF 隣接関係を確立できますか?

A. GigabitEthernet0/1 および GigabitEthernet0/1.40

B. GigabitEthernet0/1のみ

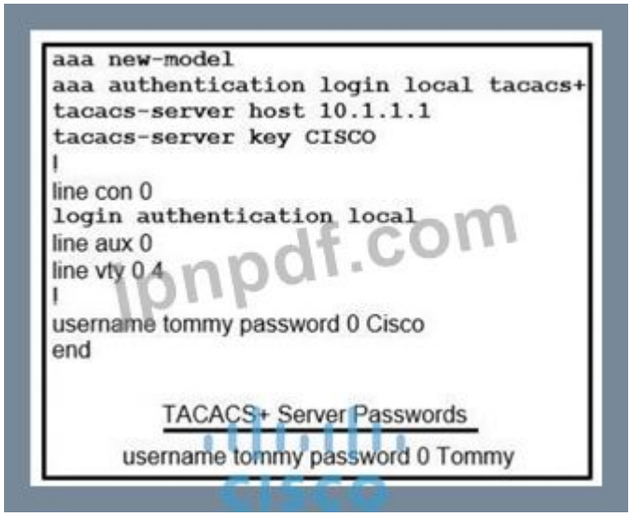
C. ギガビット イーサネット 0/0 およびギガビット イーサネット 0/1

D. GigabttEthernet0/0 のみ

Answer: D (メーッセージを残す**)**

最新問題**: 56**

展示を参照してください。



通常の操作では、ユーザー名 「tommy」の line con 0 へのアクセスを許可するパスワードはどれですか?

A. シスコ

B. ローカル

C. 0 シスコ

D. トミー

Answer: A (メーッセージを残す**)**

説明

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacac

最新問題**: 57**

VRF-lite に関する 2 つの記述のうち、正しいものはどれですか? (2つお選びください)

A. 1 台のスイッチで複数の顧客をサポートできます。

B. ほとんどのルーティング pr をサポートします。

C. お客様のルーターが OSPF 経由で ISP に接続されている場合に使用する必要があります。

D. パケット交換速度を向上させることができます。

E. MPLS-VRF ラベル交換およびラベル付きパケットをサポートします。

Answer: A,B (メーッセージを残す**)**

説明

VRF-Lite では、ルート識別子 (RD) が顧客のルーティング テーブルを識別し、顧客に重複するアドレスを割り当てることができます。したがって、重複するアドレスを持つ複数の顧客をサポートできます。-> 回答 「単一のスイッチで複数の顧客をサポートできます」は正しいです。

VRF は通常、MPLS 導入に使用されます。MPLS なしで VRF を使用する場合、VRF lite と呼ばれます -> 「MPLS-VRF ラベル交換とラベル付きパケットをサポートします」という回答は正しくありません。

VRF-Lite は、BGP、OSPF、EIGRP、RIP、およびスタティック ルーティングのほとんどの一般的なルーティング プロトコルをサポートします -> 回答 「EIGRP、ISIS、OSPF を含むほとんどのルーティング プロトコルをサポートします」が正しいです。

最新問題: **58**

私の出品物を参照してください。

```
import requests
import json

url='https://switchIP.foo.com/ins'
switchuser='username'
switchpassword='password123'

myheaders={'content-type':'application/json-rpc'}
payload=[
  {
    "jsonrpc": "2.0",
    "method": "cli",
    "params": {
      "cmd": "show clock",
      "version": 1
    },
    "id": 1
  }
]
response = requests.post(url,data=json.dumps(payload), headers=myheaders,auth=(switchuser,switchpassword), verify=False).json()
```

展示を参照してください。応答を解析して 『8:32:21.474 UTC sun Mar 10 2019?」と出力する Python コードはどれですか?

A. print(response[jresult']['body']['simple_time']}

B. print(response[result']['body']['simple_time']}

C. print(response['resut'][0||'simple_time']}

D. print(response['body']['simple_time']}

Answer: B (メーッセージを残す**)**

最新問題: **59**

展示を参照してください。エンジニアはルータ R1 にログインしようとします。どの設定でログインを成功させることができますか?

A)

```
R1# username admin privilege 15
aaa authorization exec default local
```

B)

```
R1#netconf-yang
username admin privilege 15 secret cisco123
aaa new-model
aaa authorization exec default local
```

C)

```
R1# aaa new-model
aaa authorization exec default local
enable aaa admin privilege 15
```

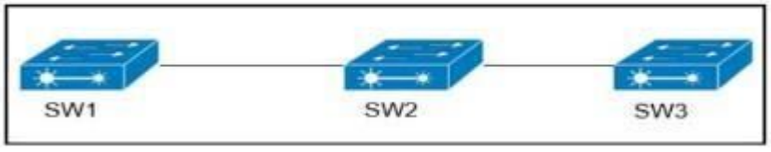
D)

```
R1#username admin privilege 15
aaa authorization exec default local
netconf-yang
```

A. オプション A
B. オプション C
C. オプション D
D. オプション B

Answer: D (メーッセージを残す)

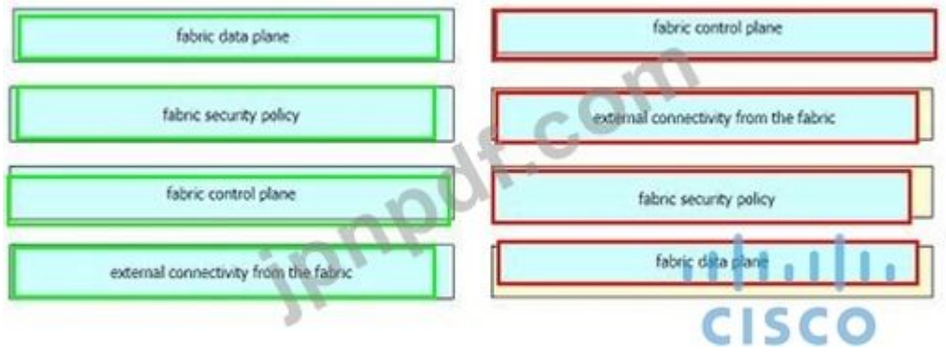
最新問題: **60**
出品物を参照してください。



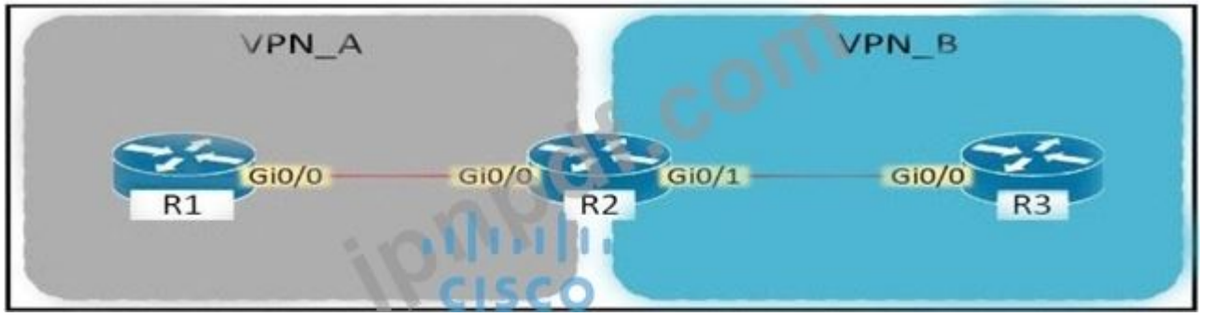
VLAN 50 と 60 はすべてのスイッチ間のトランク リンク上に存在します SW3 のすべてのアクセス ポートは VLAN 50 用に設定されており、SW1 は VTP サーバです どのコマンドにより SW3 が VLAN からのみフレームを受信できるようになります
50?
A. SW1 (config)#vtp プルーニング
B. SW3(config)#vtp モード トランスペアレント
C. SW2(config)=vtp プルーニング
D. SW1 (config >vtp モード トランスペアレント)
Answer: A (メーッセージを残す)
説明
SW3 には VLAN 60 がないため、この VLAN のトラフィック (SW2 から送信) を受信できません。
したがって、SW2 が VLAN 60 トラフィックを SW3 に転送しないように、SW3 で VTP プルーニングを設定する必要があります。また、SW2 ではなく SW1 (VTP サーバー) でプルーニングを設定する必要があることに注意してください。

最新問題: **61**
Cisco SD-Access ソリューション領域を左側から右側の使用するプロトコルにドラッグ アンド ドロップします。

Answer:



最新問題: **62**
展示を参照してください。



R が CE ルータであると仮定すると、どの VRF が R1 の Gi0/0 に割り当てられますか?
A. VRF VPN_B
B. デフォルト VRF
C. 管理 VRF
D. VRF VPN_A
Answer: (解答を表示する**)**
説明
R1 の Gi0/0 の構成には特別なことは何もありません。R2 上の Gi0/0 インターフェイスのみが VRF VPN_A に割り当てられます。ここでのデフォルト VRF は、Cisco IOS のグローバル ルーティング テーブルの概念に似ています。

最新問題: **63**
CLI を使用して Cisco IOS XE を実行するコントローラを設定しています。802.11w 保護された管理フレームに使用される 3 つの構成オプションはどれですか? （3つお選びください。）
A. saquery-再試行時間

B. 有効
C. カムバックタイム
D. 必須
E. SA 分解保護
F. アソシエーションカムバック
Answer: A,D,F (メーッセージを残す**)**

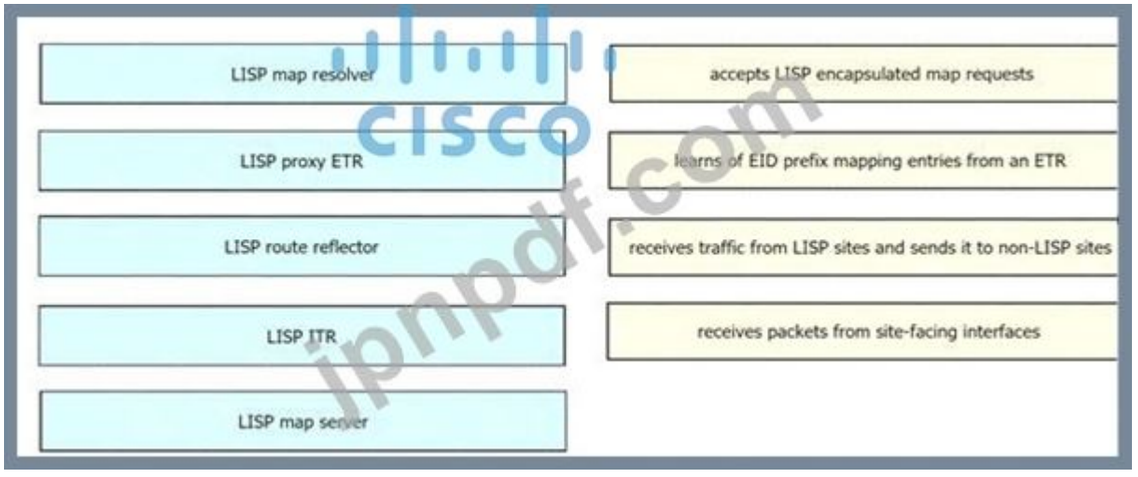
最新問題**: 64**
データセンター環境で VM を使用してサーバーを仮想化する 2 つの利点は何ですか?
(2つお選びください。)
A. セキュリティの向上
B. ラックスペース、電力、および冷却要件の削減
C. IP および MAC アドレス要件の軽減
D. スピーディな導入
E. 小さいレイヤー 2 ドメイン
Answer: B,D (メーッセージを残す**)**
サーバーの仮想化と仮想マシンの使用は、データセンターのダイナミクスを大きく変えています。ほとんどの組織は、データセンターで複数の物理サーバーをホストするコストと複雑さに苦労しています。スケールアウトサーバー アーキテクチャと従来の 『 つのアプリケーション、1 つのサーバー」のスプロール化の両方の結果であるデータセンターの拡大により、十分に活用されていない多数のサーバーの収容、電力供給、冷却に問題が生じています。さらに、IT 組織は、サーバー リソースを気まぐれで常に変化する組織のニーズに適合させるという従来のコストと運用上の課題に引き続き対処しています。
仮想マシンは、ゲスト オペレーティング システムとそれぞれのアプリケーション間の完全な分離を維持しながら、複数のアプリケーションおよびオペレーティング システム環境を単一の物理サーバー上でホストできるようにすることで、これらの課題の多くを大幅に軽減できます。したがって、サーバー仮想化により、組織は、利用率の低い多数のサーバーを、複数の仮想マシンを実行する利用率の高い 1 台のサーバーと交換できるようになり、サーバーの統合が促進されます。
複数の物理サーバーを統合することにより、組織は次のような利点を得ることができます。
+ 十分に活用されていないサーバーは廃止または再導入できます。
+ ラックスペースを再利用できます。
+ 電力と冷却の負荷を軽減できます。
+ 新しい仮想サーバーを迅速に展開できます。
+ CapEx (使用率が高いということは、購入する必要があるサーバーが少ないことを意味します) と OpEx (サーバーが少ないということは、環境がよりシンプルで、メンテナンスコストが低いことを意味します) を削減できます。
参照: https://www.cisco.com/c/en/us/solutions/collarate/data-center-virtualization/net_implementation_white_paper0900aecd806a9c05.html

最新問題**: 65**
Cisco SD-WAN ファブリックの vManage によって処理される機能はどれですか?

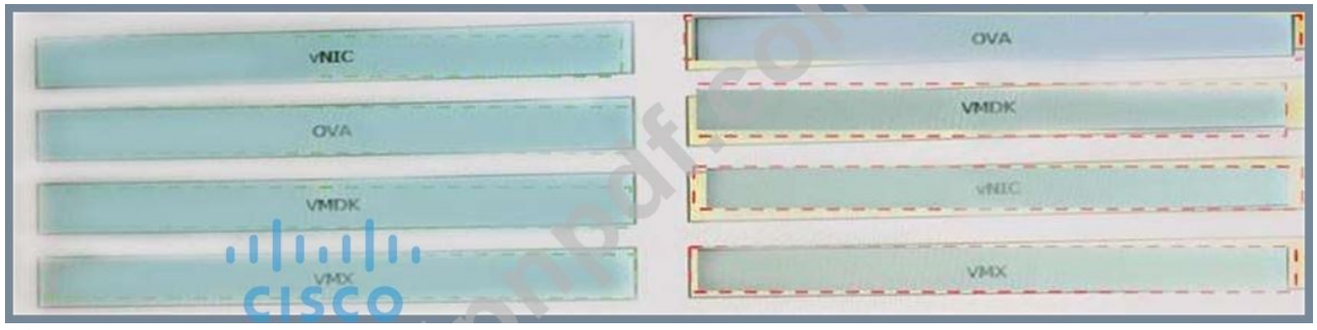
A. BFD セッションを確立して、リンクとノードの活性度をテストします。
B. ノードとの IPsec トンネルを確立します。
C. データ転送を管理するポリシーを配布します。
D. WAN エッジのリモート ソフトウェア アップグレードを実行します。vSmart と vBond
Answer: A (メーッセージを残す**)**

最新問題**: 66**
Cisco DNA Center がデバイスを検出するために使用する 3 つの方法はどれですか？ 3つお選びください。）
A. CDP
B. SNMP
C. LLDP
D. ピング
E. NETCONF
F. 指定された IP アドレスの範囲
Answer: (解答を表示する**)**
説明
Cisco DNA Center は、LLDP、CDP (Cisco Discovery Protocol)、および IP Range という 3 つの検出方法をサポートしています。
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/LTRNMS-2500-LG.pdf

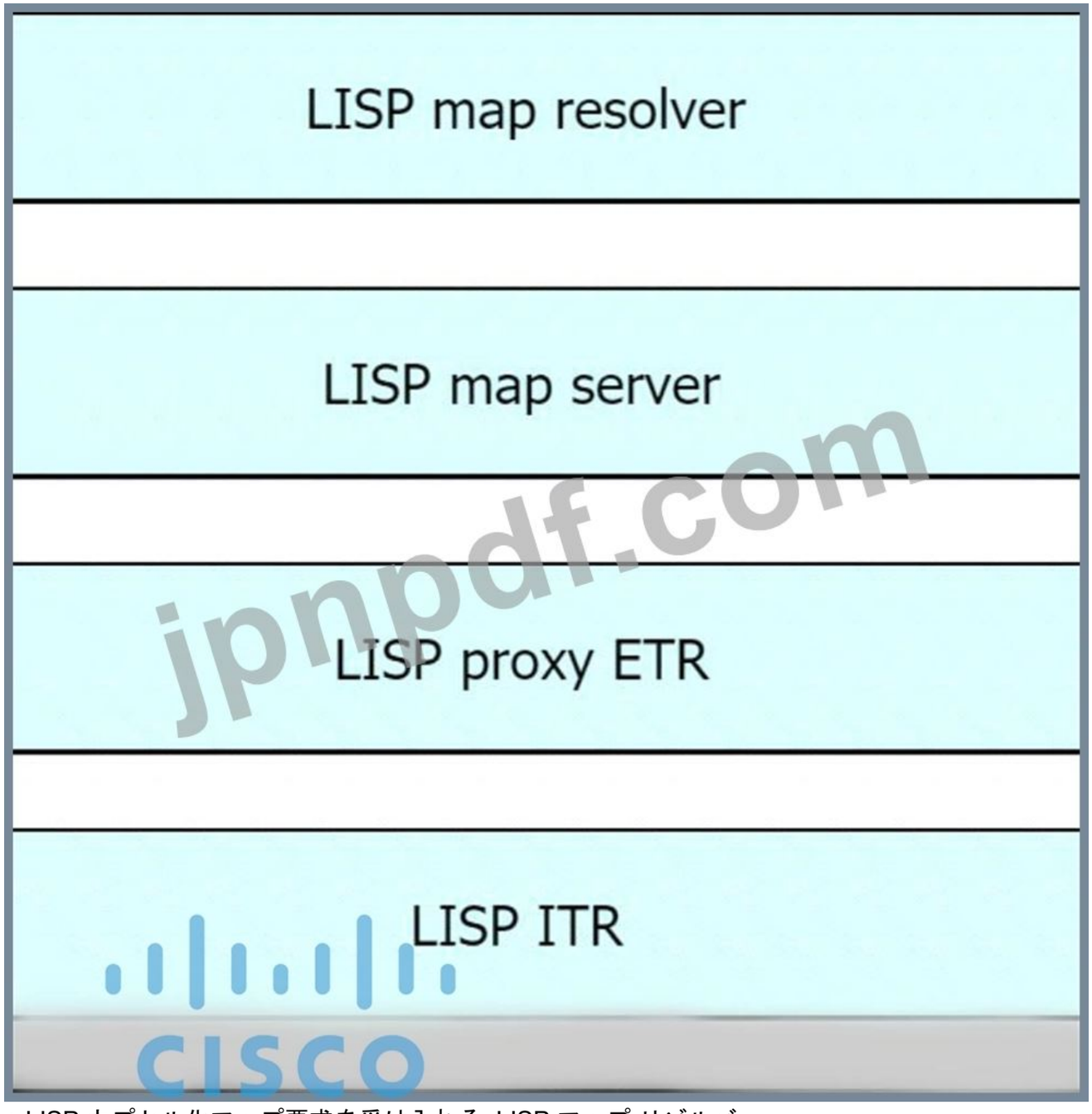
最新問題**: 67**
LISP コンポーネントを左側から、右側で実行される機能にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。



Answer:



説明



+ LISP カプセル化マップ要求を受け入れる: LISP マップ リゾルバー
+ ETR から EID プレフィックス マッピング エントリを学習します: LISP マップ サーバー
+ LISP サイトからトラフィックを受信し、非 LISP サイトに送信します: LISP プロキシ ETR

+ サイト側インターフェイスからパケットを受信: LISP ITR
説明
ITR は、宛先 EID を宛先 RLOC にマッピングし、ITR RLOC の送信元 IP アドレスと出力トンネル ルーター (ETR) の RLOC の宛先 IP アドレスを含む追加のヘッダーで元のパケットをカプセル化する機能です。
カプセル化後、元のパケットは LISP パケットになります。
ETR は、LISP でカプセル化されたパケットを受信し、カプセル化を解除して、ローカル EID に転送する機能です。この機能には EID から RLOC へのマッピングも必要なため、「マップ サーバー」の IP アドレスと認証用のキー (パスワード) を指定する必要があります。
LISP プロキシ ETR (PETR) は、非 LISP サイトに代わって ETR 機能を実装します。PETR は通常、LISP サイトが非 LISP サイトにトラフィックを送信する必要があるが、ルーティング可能な EID をパケット ソースとして受け入れないサービス プロバイダーを介して LISP サイトが接続されている場合に使用されます。PETR は ETR と同様に機能しますが、EID が非 LISP サイトの宛先にトラフィックを送信する点が異なります。
Map Server (MS) は、認証キーの登録と EID から RLOC へのマッピングを処理します。ETR は、設定されているすべての Map Server に定期的な Map-Register メッセージを送信します。
マップ リゾルバ (MR): LISP カプセル化マップ リクエスト (通常は ITR から) を受け入れる LISP コンポーネントで、宛先 IP アドレスが EID 名前空間の一部であるかどうかを迅速に判断します。

最新問題: **68**
展示を参照してください。

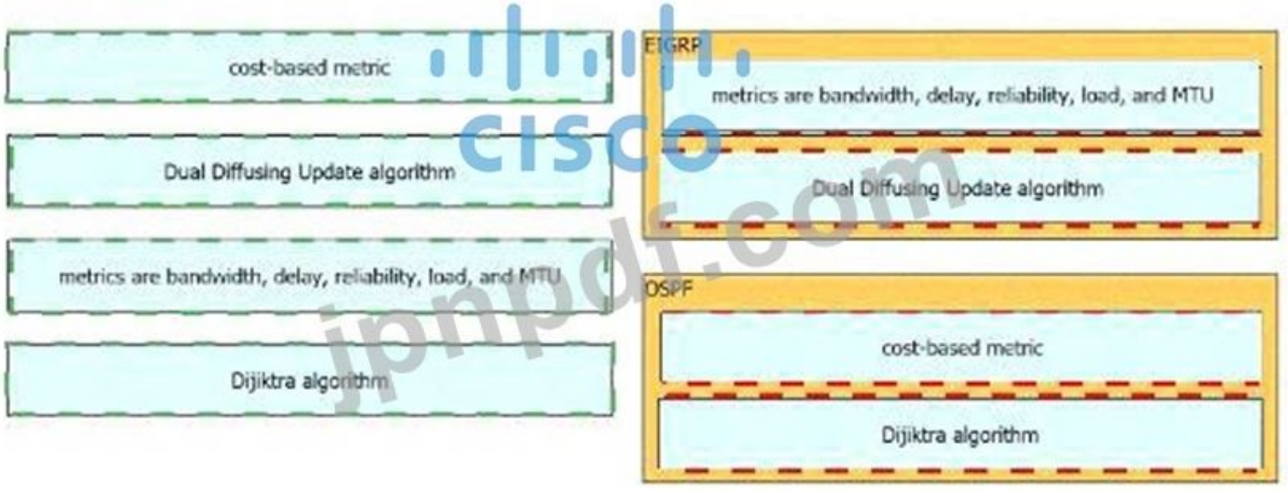
```
event manager applet LARGECONFIG
   event cli pattern "show running-config" sync yes
   action 1.0 puts "Warning! This device has a VERY LARGE configuration
         and may take some time to process"
   action 1.1 puts nonewline "Do you wish to continue [Y/N]"
   action 1.2 gets response
   action 1.3 string toupper "$response"
   action 1.4 string match "$_string_result" "Y"
   action 2.0 if $_string_result eq 1
   action 2.1 cli command "enable"
   action 2.2 cli command "show running-config"
   action 2.3 puts $_cli_result
   action 2.4 cli command "exit"
   action 2.9 end
```

EEM アプレット設定に関する 2 つの記述のうち、正しいものはどれですか? (2つお選びください。)
A. CLI コマンドの実行後に EEM アプレットが実行されます。
B. 実行コンフィギュレーションは、CLI で文字 Y が入力された場合にのみ表示されます。
C. CLI コマンドが実行される前に EEM アプレットが実行されます。
D. EEM アプレットには大文字と小文字を区別しない応答が必要です
Answer: B,C (メーッセージを残す)
説明
events cli コマンドで sync yes オプションを使用すると、CLI コマンドが実行される前に EEM アプレットが実行されます。EEM アプレットは、CLI コマンドを実行するか (exit_status を 1 に設定)、実行しない (exit_status を 0 に設定) かを示す _exit_status 変数を設定する必要があります。
sync no オプションを使用すると、EEM アプレットは CLI コマンドと並行してバックグラウンドで実行されます。
参照: https://blog.ipspace.net/2011/01/eem-event-cli-command-options-and.html

最新問題: **69**

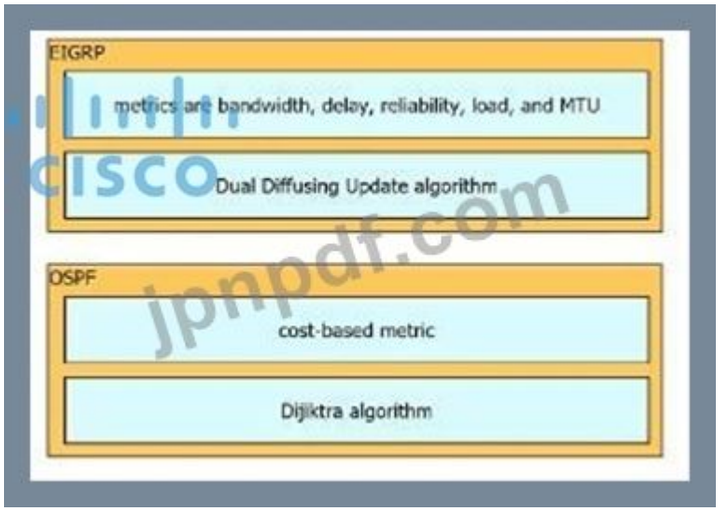
特性を左側から右側に説明されているルーティング プロトコルにドラッグ アンド ドロップします。

Answer:



説明

グラフィカル ユーザー インターフェイス、アプリケーションの説明が自動的に生成される



最新問題: **70**

展示を参照してください。外部ユーザーは、TCP ポート 8080 でリッスンしている社内 Web サーバーへの HTTP 接続を必要とします。この要件を満たすコマンド セットはどれですか?

- interface G0/0
  ip address 209.165.200.225 255.255.255.224
  ip nat inside

  interface G0/1
  ip address 10.1.1.1 255.255.255.0
  ip nat outside

  ip nat inside source static tcp 10.1.1.1 8080 209.165.200.225 80

- interface G0/0
  ip address 209.165.200.225 255.255.255.224
  ip nat outside

  interface G0/1
  ip address 10.1.1.1 255.255.255.0
  ip nat inside

  ip nat inside source static tcp 10.1.1.100 8080 interface G0/0 80

- interface G0/0
  ip address 209.165.200.225 255.255.255.224
  ip nat inside

- interface G0/0
  ip address 209.165.200.225 255.255.255.224
  ip nat inside

  interface G0/1
  ip address 10.1.1.1 255.255.255.0
  ip nat outside

  ip nat inside source static tcp 209.165.200.225 80 10.1.1.100 8080

- interface G0/0
  ip address 209.165.200.225 255.255.255.224
  ip nat outside

  interface G0/1
  ip address 10.1.1.1 255.255.255.0
  ip nat inside

  ip nat inside source static tcp 209.165.200.225 8080 10.1.1.100 8080

A. オプション B
B. オプション A
C. オプション D
D. オプション E
E. オプション C
Answer: A (メーッセージを残す**)**

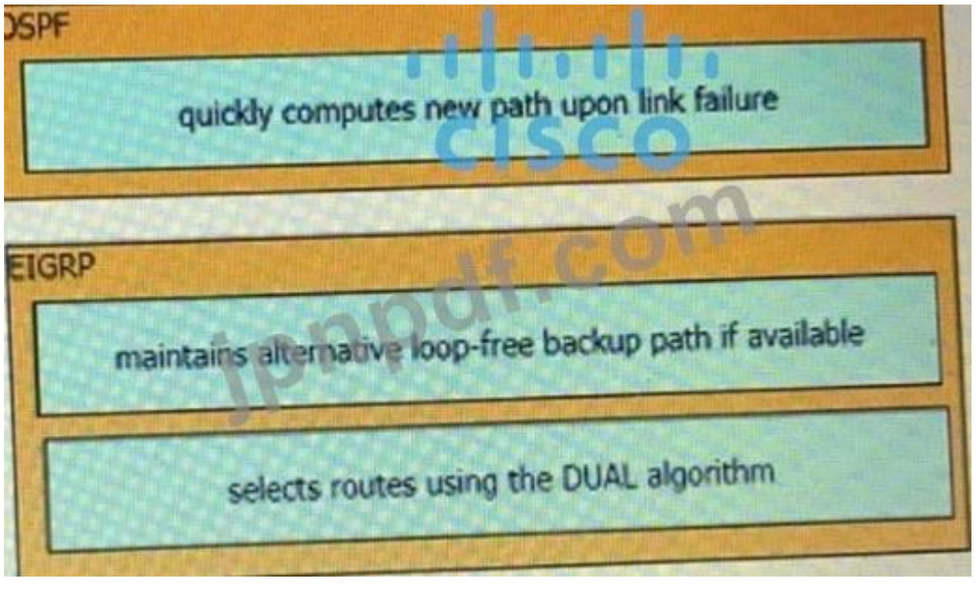
最新問題**: 71**
エンジニアが高速移行を有効にして WLAN を設定します。一部のレガシー クライアントがこの WLAN に接続できません。他のクライアントが OLTI に基づく高速移行を使用できるようにしながら、レガシー クライアントの接続を許可する機能はどれですか?
A. DS経由
B. アダプティブ R
C. 802.11V
D. 802.11k
Answer: B (メーッセージを残す**)**
802.11r 高速移行 (FT) ローミングは、802.11 IEEE 標準の修正です。これはローミングの新しい概念です。新しい AP との最初のハンドシェイクは、クライアントがターゲット AP にローミングする前に発生します。したがって、これは高速遷移と呼ばれます。802.11r では、次の 2 つのローミング方法が提供されます。
+ 無線: このタイプのローミングでは、クライアントは高速移行 (FT) 認証アルゴリズムによる IEEE 802.11 認証を使用してターゲット AP と直接通信します。+ Over-the-DS (分散システム): このタイプのローミングでは、クライアントは現在の AP を通じてターゲット AP と通信します。クライアントとターゲット AP 間の通信は、クライアントと現在の AP 間の FT アクション フレームで伝送され、コントローラを通じて送信されます。
ただし、これらの方法はいずれもレガシー クライアントを処理しません。
802.11k を使用すると、11k 対応クライアントが、ローミングの候補である既知の近隣 AP に関する情報を含む近隣レポートを要求できます。
参照：
IEEE 802.11v は、ワイヤレス ネットワーク管理に対する多数の機能強化を説明する IEEE 802.11 標準の修正版です。そのような機能強化の 1 つが、クライアントがより長くスリープできるようにすることでバッテリー寿命を向上させるネットワーク支援省電力です。もう 1 つの機能強化は、ネットワーク アシスト ローミングです。これにより、WLAN は関連付けられたクライアントにリクエストを送信し、関連付けるべきより適切な AP についてクライアントにアドバイスできるようになります。これは、負荷分散と、接続が不十分なクライアントの誘導の両方に役立ちます。
Cisco 802.11r は 3 つのモードをサポートします。+ 純粋モード :802.11r クライアントのみの接続を許可 + 混合モード :FT をサポートするクライアントとサポートしないクライアントの両方の接続を許可 + アダプティブ モード :FT AKM をまったくアドバタイズしませんが、サポートされているクライアントが接続すると FT したがって、ここでは 「アダプティブ モード」が最良の答えです。

最新問題**: 72**
特性を左側から右側に説明されているルーティング プロトコルにドラッグ アンド ドロップします。

Answer:

説明

タイムラインを含む画像 自動生成された説明

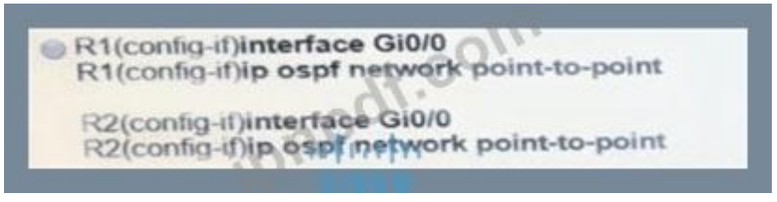


最新問題**: 73**

展示を参照してください。

ネットワーク エンジニアは、ルーター R1 とルーター R2 の間で OSPF を構成しています。エンジニアは、DR/BDR 選択がエリア 0 のギガビット イーサネット インターフェイスで発生しないことを確認する必要があります。この目標を達成できる設定セットはどれですか?

A)



B)

C)

D)

A. オプション A
B. オプション B
C. オプション C
D. オプション D
Answer: A (メーッセージを残す**)**
説明
ブロードキャスト ネットワークと非ブロードキャスト ネットワークは DR/BDR を選択しますが、ポイントツーポイント/
マルチポイントでは DR/BDR を選択しません。したがって、2 つの Gi0/0 を設定する必要があります。
ポイントツーポイントまたはポイントツーマルチポイント ネットワークへのインターフェイスを提供し、DR/BDR 選択が発生しないようにします。

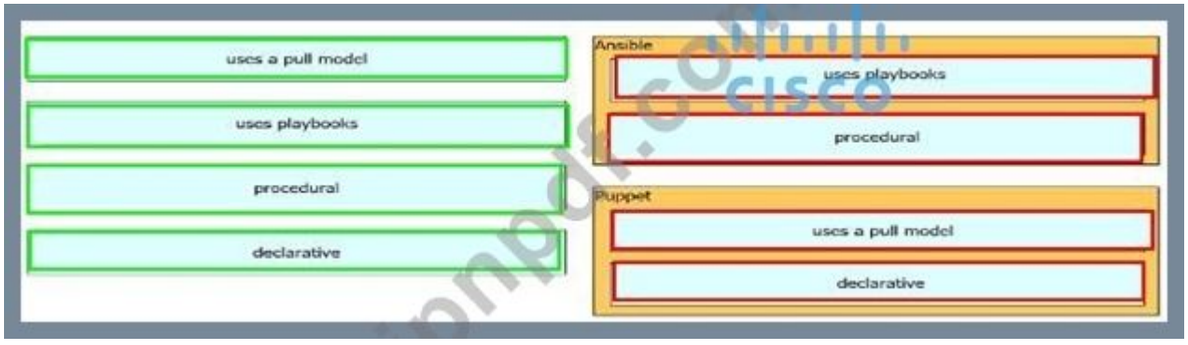
最新問題**: 74**
RIB は FIB とどう違うのですか?
A. RIB は、ネットワーク トポロジとルーティング テーブルを作成するために使用されます。FIB は、特定のネットワーク宛先へのルートのリストです。
B. FIB には、単一の宛先に対して多数のルートが含まれます。RIB は、単一の宛先への最適なルートです。
C. RIB には、同じ宛先プレフィックスへのルートが多数含まれています。FIB には最適なルートのみが含まれます
D. FIB はネットワーク トポロジとルーティング テーブルを維持します。RIB は、特定のネットワーク宛先へのルートの list です。
Answer: A (メーッセージを残す**)**
説明
FIB is used for forwarding,
RIB is derived from the control plane,

最新問題**: 75**
spaning-tree portfast コマンドの主な効果は何ですか?
A. BPDU メッセージを有効にします
B. スパニングツリーのコンバージェンス時間を最小限に抑えます。
C. スイッチがリロードされると、ポートはただちにフォワーディング ステートになります。
D. リスニング状態のポートを即座に有効にします。
Answer: B (メーッセージを残す**)**
説明
Port Fast の目的は、スパニング ツリーが収束するまでインターフェイスが待機する時間を最小限に抑えることです。これは、エンド ステーションに接続されているインターフェイスで使用される場合にのみ効果があります。
参照：
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_55_se/configuration/guid

最新問題: **76**

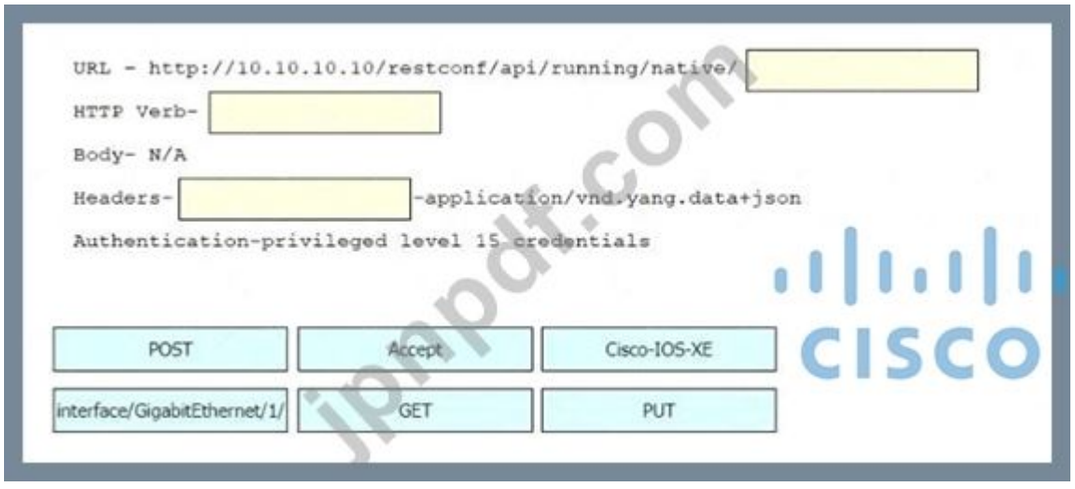
左側の特性を、右側で説明されているオーケストレーション ツールにドラッグ アンド ドロップします。

Answer:

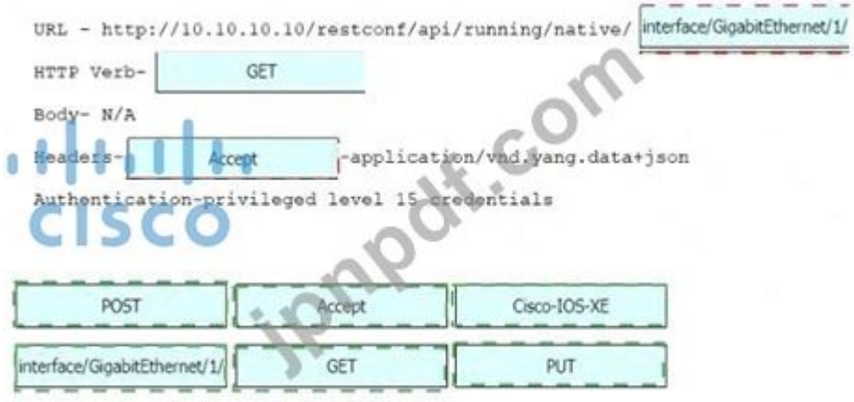


最新問題: **77**

展示を参照してください スニペットを RESTCONF リクエストにドラッグ アンド ドロップして、この応答を返すリクエストを形成します すべてのオプションが使用されるわけではありません



Answer:



説明

最新問題**: 78**

Cisco Cyber Threat Defense を構成するソリューションを左側から右側の達成目標にドラッグ アンド ドロップします。

Answer:

最新問題**: 79**

展示を参照してください。

エンジニアは SW1 と SW2 の間のポット チャネルをアクセス ポートからトランクに再設定し、SW1 のログでこのエラーにすぐに気づきました。

このエラーを解決するコマンド セットはどれですか?

A)

```
SW1(config-if)#interface G0/0
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

B)

```
SW1(config-if)#interface G0/0
SW1(config-if)#no spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

C)

```
SW1(config-if)#interface G0/1
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

D)

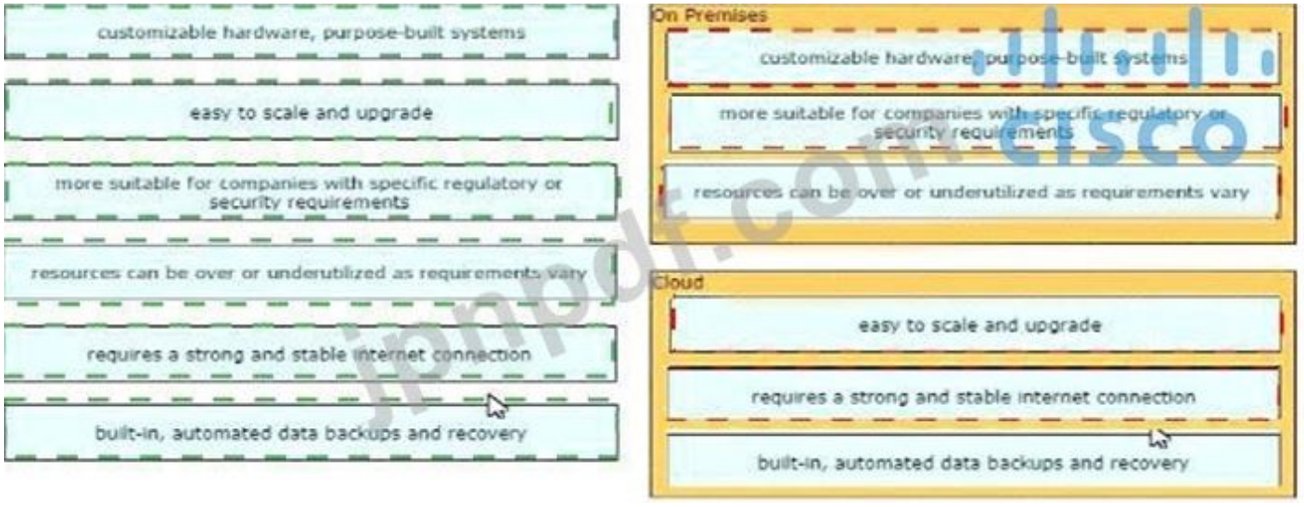
```
SW1(config-if)#interface G0/0
SW1(config-if)#no spanning-tree bpdufilter
SW1(config-if)#shut
SW1(config-if)#no shut
```

A. オプション D
B. オプション B
C. オプション C
D. オプション A
Answer: (解答を表示する**)**

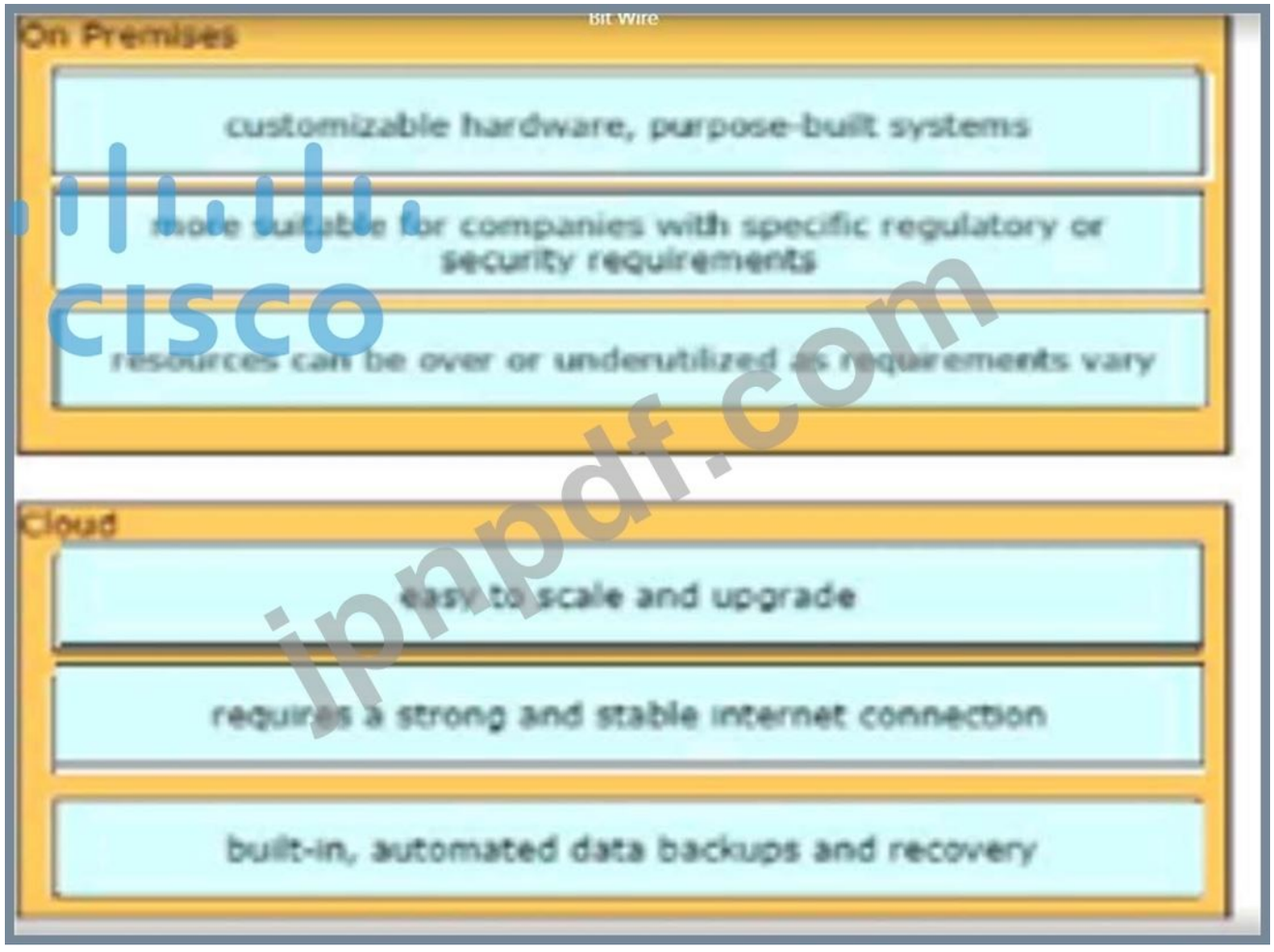
最新問題**: 80**
仮想マシン環境でブロードキャスト放射が発生する 2 つの理由は何ですか? (2つお選びください。)
A. vSwitch とネットワーク スイッチ間の通信はマルチキャスト ベースです。
B. 仮想マシン環境では、レイヤー 2 ドメインが大きくなる可能性があります。
C. vSwitch とネットワーク スイッチ間の通信はブロードキャスト ベースです。
D. vSwitch はブロードキャスト パケットを処理するためにサーバー CPU に割り込む必要があります。
E. 仮想マシンは主にブロードキャスト モードを通じて通信します。
Answer: C,D (メーッセージを残す**)**

最新問題**: 81**
左側の特性を右側の適切なインフラストラクチャ展開タイプにドラッグ アンド ドロップします。

Answer:

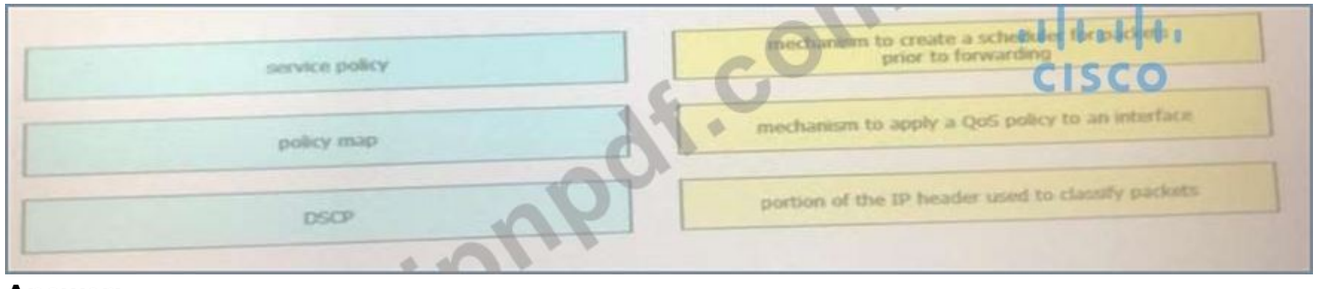


説明
オンプレミス: カスタマイズ可能、特定の要件、リソース
クラウド: スケール、組み込みの自動バックアップ、強力で安定したインターネット

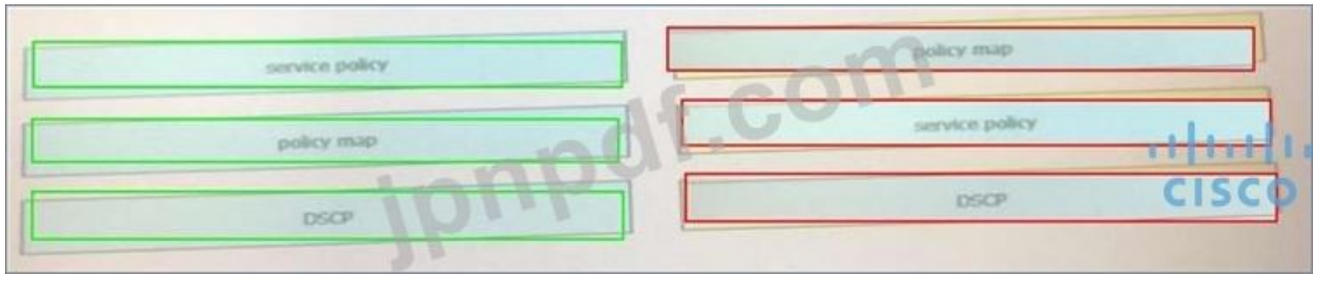


最新問題: **82**

左側の Qos メカニズムを右側の正しい説明にドラッグ アンド ドロップします。



Answer:



最新問題: **83**

ワイヤレス ユーザーは、ワイヤレス ネットワークから頻繁に切断されると報告しています。ネットワーク エンジニアは、トラブルシューティングを行っているときに、ユーザーが切断した後、入力を必要とせずに接続が自動的に再確立されることに気付きました。エンジニアは、これらのメッセージ ログにも注目します。

AP 'AP2' is down. Reason: Radio channel set. 6:54:04 PM
AP 'AP4' is down. Reason: Radio channel set. 6:44:49 PM
AP 'AP7' is down. Reason: Radio channel set. 6:34:32 PM

ユーザーへの影響を軽減するアクションはどれですか?

A. AP ハートビート タイムアウトを増やします。

B. BandSelect を増やす

C. カバレッジホール検出を有効にする

D. 動的チャネル割り当て間隔を長くします。

Answer: D (メーッセージを残す**)**

説明

これらのメッセージ ログは、無線チャネルが
リセットされています (AP は短時間ダウンしている必要があります)。と
動的チャネル割り当て (DCA) により、無線は次のことができます。
あるチャンネルから別のチャンネルに頻繁に切り替わりますが、
混乱を引き起こします。デフォルトの DCA 間隔は 10 分です。
これはメッセージ ログの時刻と一致します。に
DCA 間隔を長くすると、DCA の数を減らすことができます。
ユーザーがラジオを変えるために切断された回数
チャンネル。

最新問題**: 84**

展示を参照してください。

エンジニアは、冗長構成で新しいルーターのペアを設置しています。各ルーターのスタンバイ ステータスをチェックすると、エンジニアはルーターが期待どおりに機能していないことに気づきました。どの操作を行うと構成エラーが解決されますか?

A. 一致するホールド タイマーと遅延タイマーを設定します。

B. 一致するキー文字列を構成します

C. 一致する優先度の値を設定します。

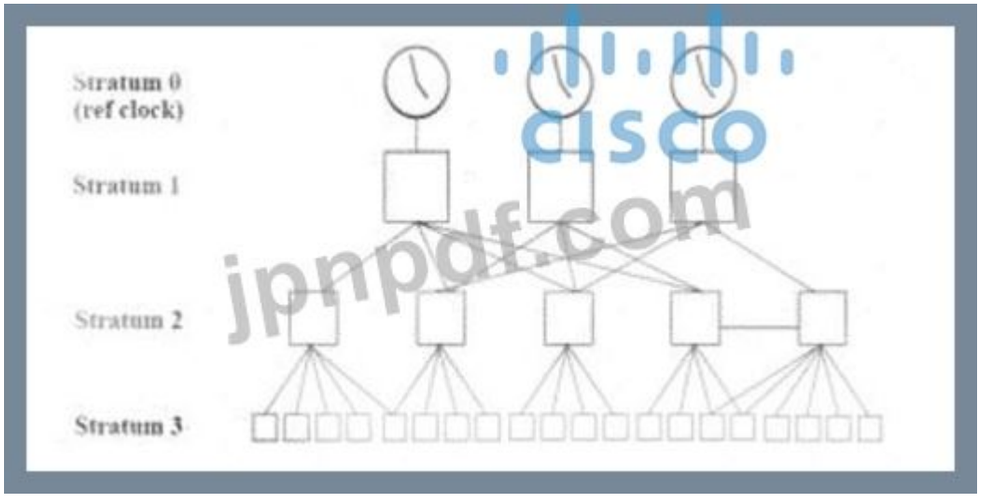
D. 一意の仮想 IP アドレスを構成します

Answer: B (メーッセージを残す**)**

説明

出力結果から、R1 のキー文字列が Cisco123 であることがわかります。（文字C は大文字）、R2 の文字は cisco123! です。これにより認証に不一致が生じるため、キー文字列を修正する必要があります。
key-string [暗号化タイプ] text-string: キーのテキスト文字列を設定します。text-string 引数は英数字であり、大文字と小文字が区別され、特殊文字がサポートされます。
参照：
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/security/configuration/guide/b_Ci

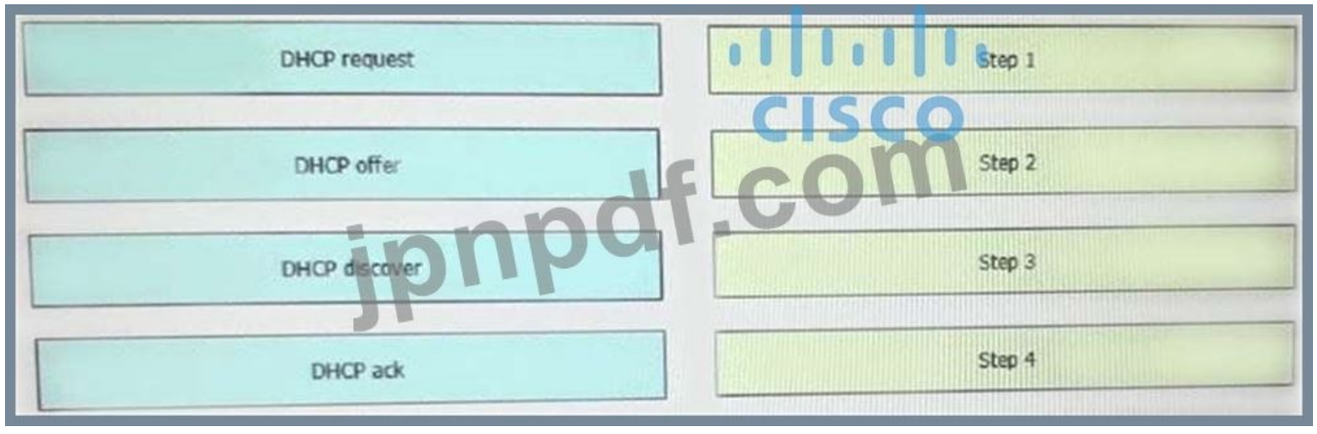
最新問題**: 85**
信頼できるタイム ソースに直接接続されているサーバーは、どの NTP 階層レベルですか?
A. ストラタム 0
B. ストラタム 1
C. ストラタム14
D. ストラタム15
Answer: B (メーッセージを残す**)**
説明
ストラタム レベルは、基準クロックからの距離を定義します。あ
基準クロックは、正確であると想定され、遅延がほとんどまたはまったくないストラタム 0 デバイスです。Stratum 0 サーバーはネットワーク上で使用できませんが、Stratum-1 サーバーとして動作するコンピューターに直接接続されます。Stratum 1 タイム サーバーは、プライマリ ネットワーク時間標準として機能します。



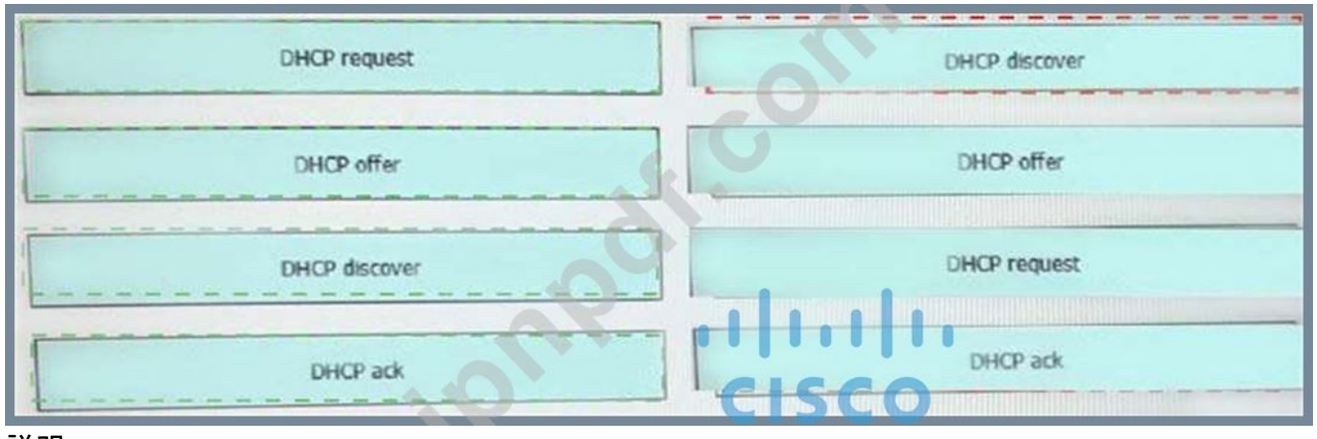
ストラタム 2 サーバーはストラタム 1 サーバーに接続されます。次に、ストラタム 3 サーバーがストラタム 2 サーバーに接続され、以下同様に接続されます。ストラタム 2 サーバーは、ストラタム 1 サーバーからの NTP パケット要求を介して時刻を取得します。ストラタム 3 サーバーは、ストラタム 2 サーバーからの NTP パケット要求を介して時刻を取得します。ストラタム サーバーは、同じレベルの他のストラタム サーバーとピアリングして、ピア グループ内のすべてのデバイスにより安定した堅牢な時刻を提供することもできます (たとえば、ストラタム 2 サーバーは他のストラタム 2 サーバーとピアリングできます)。
NTP では、ストラタムの概念を使用して、あるネットワークから NTP が何ホップ離れているかを記述します。マシンは信頼できるタイム ソースからのものです。ストラタム1タイムサーバー
通常、権威ある時刻源 (ラジオや原子時計、全地球測位システム (GPS) 時刻源など) が直接接続されており、ストラタム 2 タイム サーバーは NTP 経由でストラタム 1 タイム サーバーから時刻を受信します。

参照: https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/bsm/16-6-1/b-bsm-xe-16-6-1-asr920/bsm-timecalendar-セット.html

最新問題: **86**
クライアントと AP の間で交換される DHCP メッセージを、右側の交換順序にドラッグ アンド ドロップします。



Answer:



説明

DHCP クライアントと DHCP サーバーの間では、DHCPDISCOVER、DHCPO FFER、DHCPREQUEST、および DHCPACKNOWLEDGEMENT の 4 つのメッセージが送信されます。
このプロセスは、DORA (Discover、Offer、Request、Acknowledgement) と略されることがよくあります。

最新問題: **87**

展示を参照してください。

100 パケットごとに 50 パケットを分析するには、どのコマンド セットを設定に追加する必要がありますか?

A)

```
interface GigabitEthernet 0/0/0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

B)

```
sampler SAMPLER-1
 no mode random 1-out-of 2
 mode percent 50

nterface GigabitEthernet 0/0/0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

C)

```
flow monitor FLOW-MONITOR-1
 record v4_r1
 sampler SAMPLER-1

interface GigabitEthernet 0/0/0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

```
sampler SAMPLER-1
 mode random 1-out-of 2
 flow FLOW-MONITOR-1

interface GigabitEthernet 0/0/0
 ip flow monitor SAMPLER-1 input
```

A. オプション B

B. オプション D

C. オプション C

D. オプション A

Answer: (解答を表示する**)**

最新問題: **88**

展示を参照してください。VRRP 用にオブジェクト追跡が設定されています。ルーター Edge-01 および Edge-02 を有効にしました。Edge-01 でインターフェイス G0/0 がダウンした場合に、Edge-02 が Edge-01 をプリエンプトするコマンドはどれですか?

A. オプション C
B. オプション B
C. オプション A
D. オプション D
Answer: C (メーッセージを残す**)**

最新問題**: 89**
展示を参照してください。

GRE トンネルをアップ/アップ状態にするには、どのコマンドをルーター 1 に適用する必要がありますか?
A. Router1(config-if)#トンネルソース GigabitEthernet0/1
B. Router1 (config)#interfacetunnel0
C. ルーテッド (ファネル モード gre マルチポイントの場合に設定)
D. Router1(config-if)&トンネル送信元Loopback0
Answer: (解答を表示する**)**

最新問題**: 90**

```
import ncclient

with ncclient.manager.connect(host='192.168.1.1', port=830, username='root',
                              password='teset123!', allow_agent=False) as m:
    print(m.get_config('running').data_xml)
```

展示を参照してください。展示内のコードを実行した後。NETCONF サーバーが NETCONF クライアントに返すデータの量をインターフェイスの構成のみに減らす手順はどれですか?

A. txml ライブラリを使用して、インターフェイスの構成について NETCONF サーバーから返されたデータを解析します。

B. JSON ライブラリを使用して、インターフェイスの構成に関して NFTCONF サーバーから返されたデータを解析します。

C. JSON フィルターを文字列として作成し、引数として get_config() メソッドに渡します。

D. XML フィルターを文字列として作成し、引数として get_config() メソッドに渡します。

Answer: D (メーッセージを残す)

最新問題**: 91**

展示を参照してください。

ポート チャネルは SW2 と SW3 の間に設定されます。SW2 は Cisco オペレーティング システムを実行していません。すべての物理接続がモードの場合、ポート チャネルは確立されません。SW3 の構成の抜粋に基づいて、問題の原因は何ですか?

A. ポート チャネル インターフェイスのリード バランスを src-mac に設定する必要があります。

B. SW2 のポート チャネルは互換性のないプロトコルを使用しています。

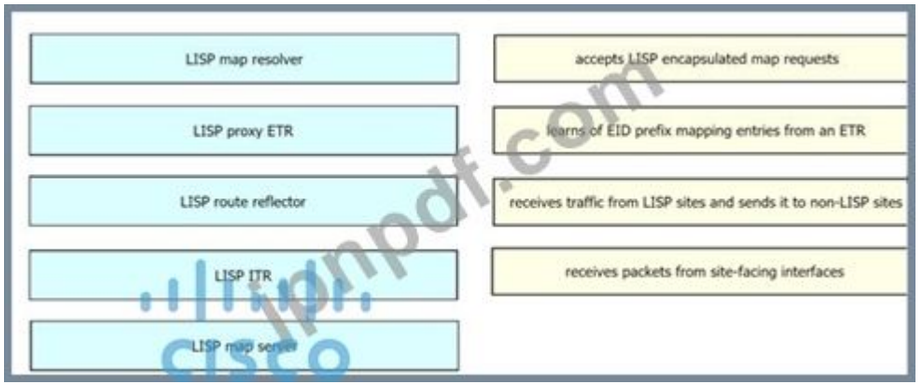
C. ポートチャネルは自動に設定する必要があります。

D. ポートチャネル トランクはネイティブ VLAN を許可していません。

Answer: (解答を表示する)

最新問題: 92

LISP コンポーネントを左側から、右側で実行される機能にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。



Answer:

Explanation:

+ LISP カプセル化マップ要求を受け入れる: LISP マップ リゾルバー
+ ETR から EID プレフィックス マッピング エントリを学習します: LISP マップ サーバー
+ LISP サイトからトラフィックを受信し、非 LISP サイトに送信します: LISP プロキシ ETR
+ サイト側インターフェイスからパケットを受信: LISP ITR

説明

ITR は、宛先 EID を宛先 RLOC にマッピングし、ITR RLOC の送信元 IP アドレスと出力トンネル ルーター (ETR) の RLOC の宛先 IP アドレスを含む追加のヘッダーで元のパケットをカプセル化する機能です。

カプセル化後、元のパケットは LISP パケットになります。

ETR は、LISP でカプセル化されたパケットを受信し、カプセル化を解除して、ローカル EID に転送する機能です。この機能には EID から RLOC へのマッピングも必要なため、『マップ サーバー』の IP アドレスと認証用のキー (パスワード) を指定する必要があります。

LISP プロキシ ETR (PETR) は、非 LISP サイトに代わって ETR 機能を実装します。PETR は通常、LISP サイトが非 LISP サイトにトラフィックを送信する必要があるが、ルーティング可能な EID をパケット ソースとして

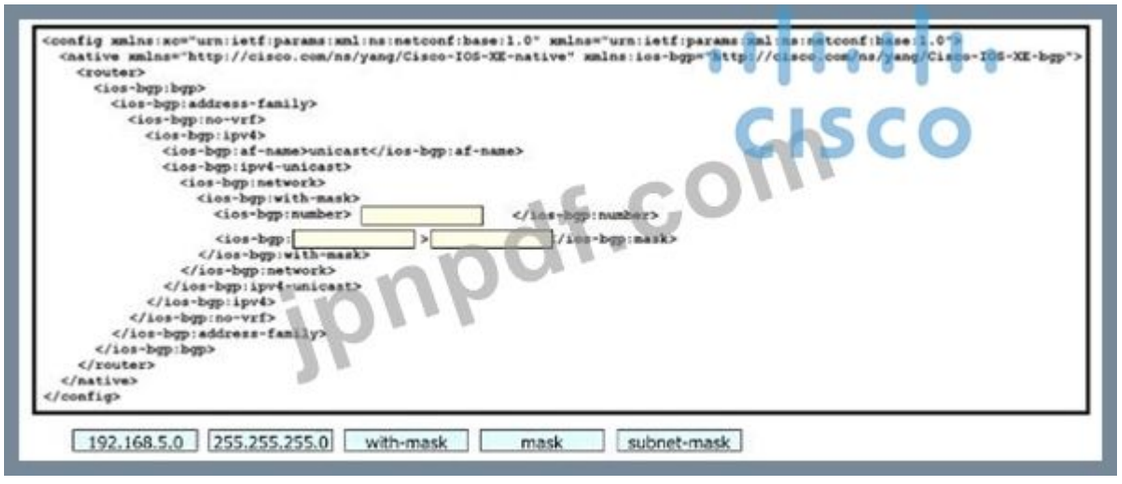
受け入れないサービス プロバイダーを介して LISP サイトが接続されている場合に使用されます。PETR は ETR と同様に機能しますが、EID が非 LISP サイトの宛先にトラフィックを送信する点が異なります。
Map Server (MS)は、認証キーの登録と EID から RLOC へのマッピングを処理します。ETR は、設定されているすべての Map Server に定期的な Map-Register メッセージを送信します。
マップ リゾルバ (MR): LISP カプセル化マップ リクエスト (通常は ITR から) を受け入れる LISP コンポーネントで、宛先 IP アドレスが EID 名前空間の一部であるかどうかを迅速に判断します。

最新問題: **93**
展示品に戻ります。

```
<interface>
    <Loopback>
      <name>100</name>
      <enabled>true</enabled>
    </Loopback>
  </interface>
```

展示を参照してください。このコードによって何が実現されるのでしょうか?
A. ループバック インターフェイスのシャットダウンを解除します。
B. ループバックインターフェースを削除します。
C. ループバックインターフェースの名前を変更します。
D. ループバックインターフェースを表示します。
Answer: (解答を表示する**)**

最新問題: **94**
スニペットをコード内の空白にドラッグ アンド ドロップして、ネットワーク プレフィックス 192.168.5.0/24 を BGP セッションにアドバタイズするスクリプトを構築します。すべてのオプションが使用されるわけではありません



Answer:

最新問題: **95**

IP ベースのアクセス コントロール ポリシーを展開するときに、Cisco Center はどのデバイスを設定しますか?

A. ISE と統合されているすべてのデバイス

B. 選択された個々のデバイス

C. 選択したサイトのすべてのデバイス

D. すべての有線デバイス

Answer: A (メーッセージを残す**)**

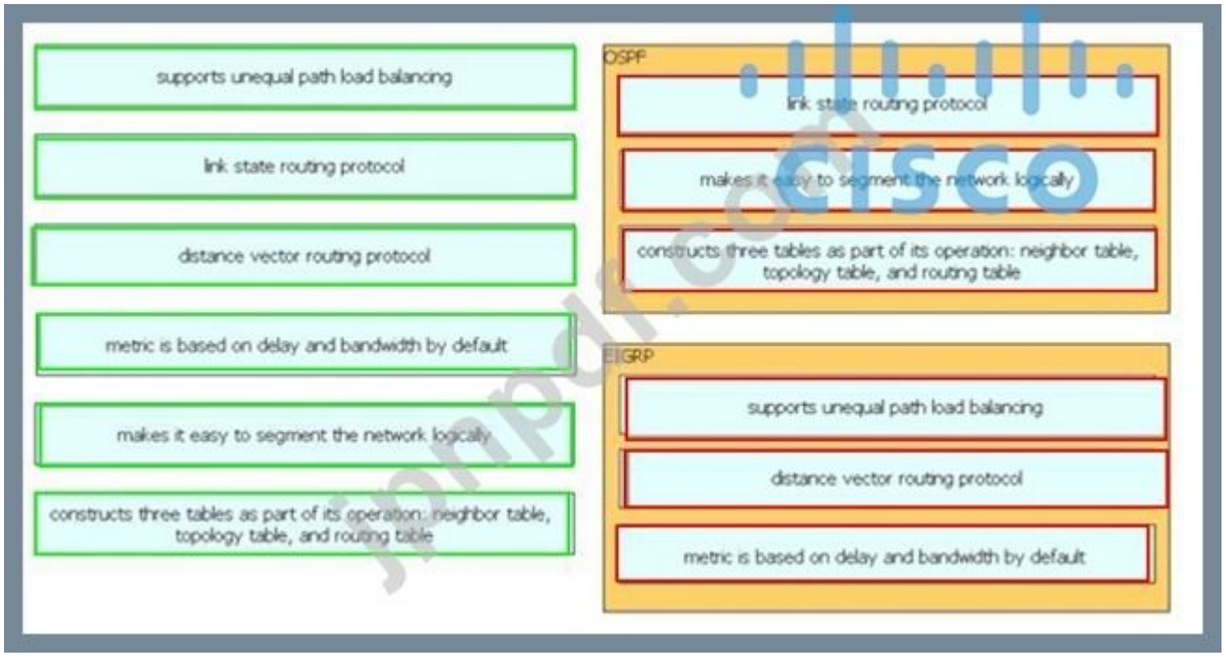
説明

[Deploy] をクリックすると、Cisco DNA Center は Cisco Identity Services Engine (Cisco ISE) に対して、ポリシーの変更に関する通知をネットワーク デバイスに送信するように要求します。

最新問題: **96**

特性を左側から右側に説明されているルーティング プロトコルにドラッグ アンド ドロップします。

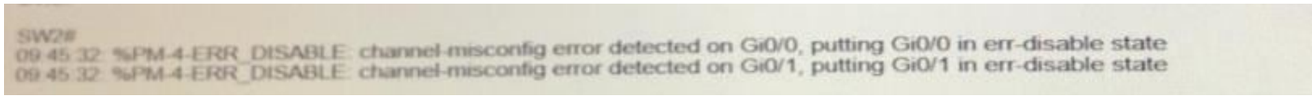
Answer:



最新問題**: 97**
ハイパーバイザーが仮想マシンで使用できるようにする必要がある 3 つのリソースはどれですか? (3つお選びください)
A. IPアドレス
B. 帯域幅
C. ストレージ
D. 安全なアクセス
E. プロセッサー
F. メモリ
Answer: B,C,F (メーッセージを残す**)**

最新問題**: 98**
展示を参照してください。

エンジニアがスイッチ SW1 とスイッチ SW2 の間に EtherChannel を設定すると、このエラー メッセージがスイッチ SW2 に記録されます。



SW1 からの出力とスイッチ SW2 で受信したログ メッセージに基づいて、エンジニアはこの問題を解決するためにどのようなアクションを実行する必要がありますか?

A. スイッチ SW1 のインターフェイス Gi0/1 の構成エラーを接続します。

B. スイッチ SW1 の EtherChannel に正しいポート メンバーを定義します。

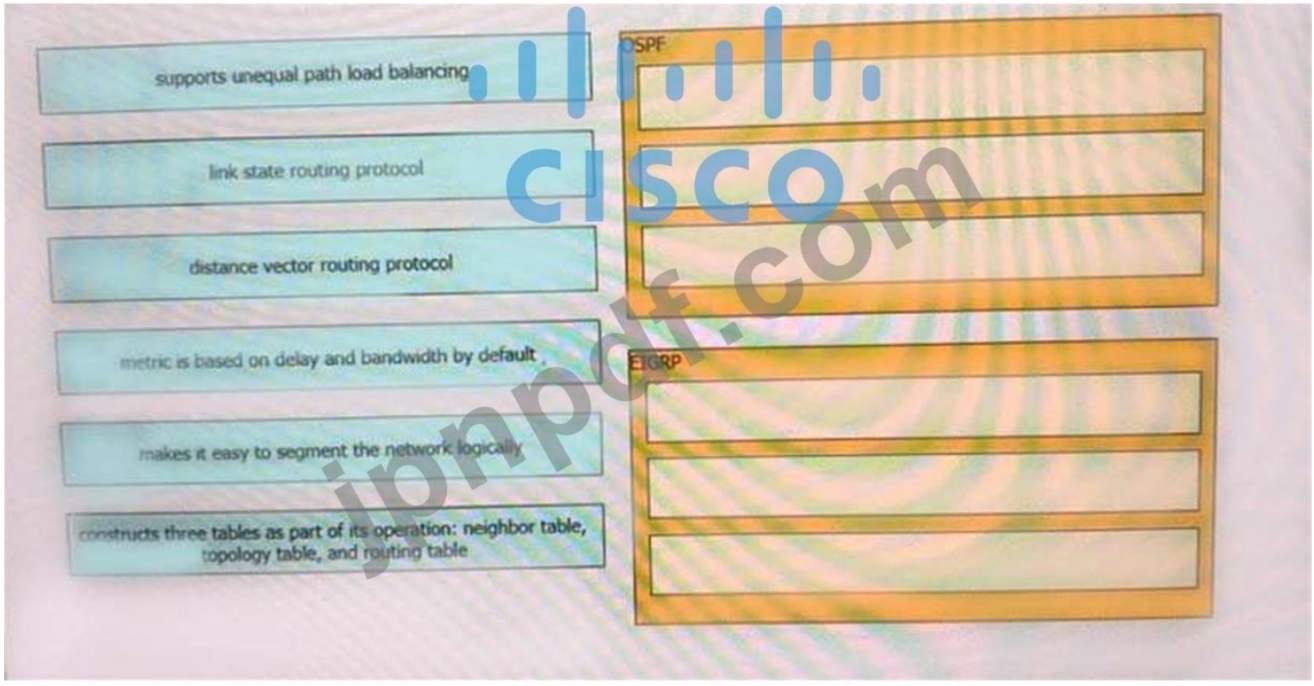
C. スイッチ SW1 と SW2 の EtherChannel に同じプロトコルを設定します。

D. インターフェイス Gi0/0 スイッチ SW1 の設定エラーを修正します。

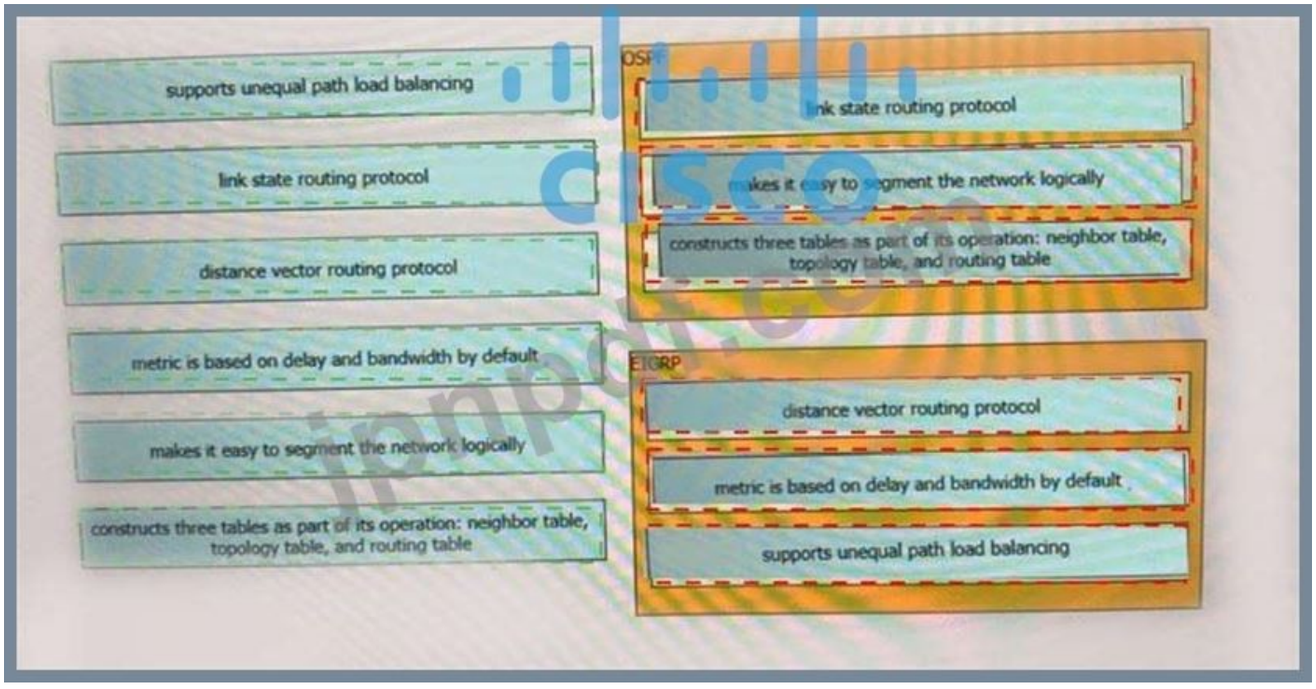
Answer: (解答を表示する**)**

最新問題**: 99**

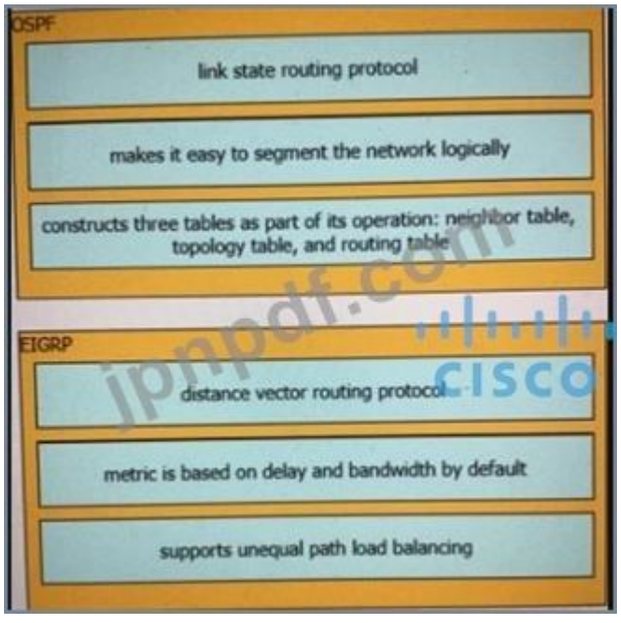
説明を左側から、右側に説明されているルーティング プロトコルにドラッグ ドロップします。



Answer:



説明

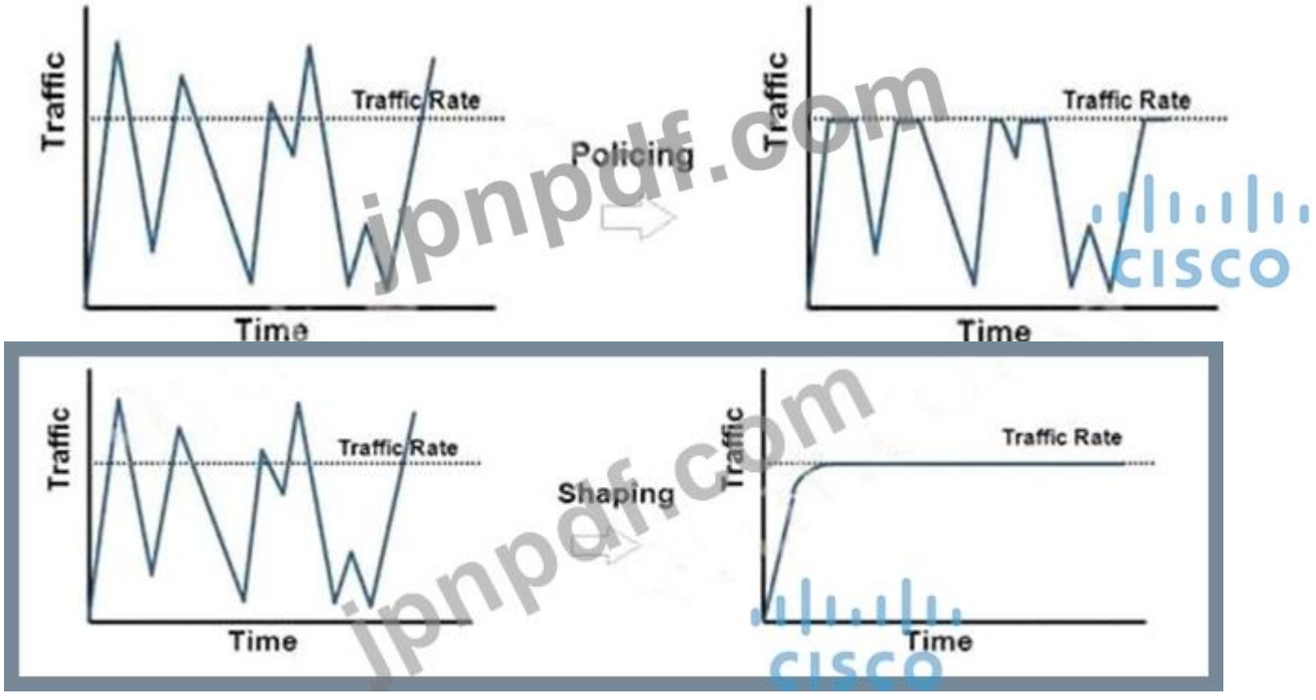


最新問題**: 100**

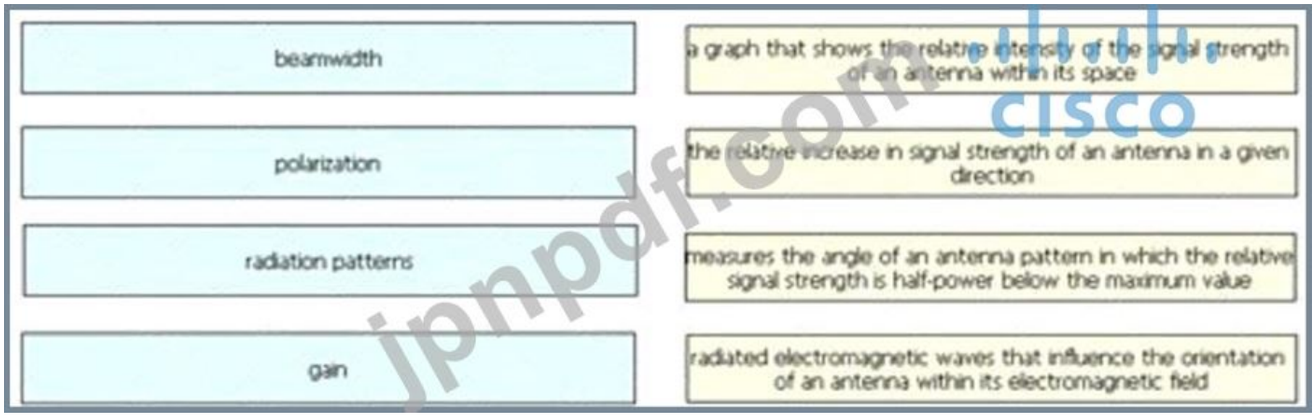
左側のツールを右側のエージェント タイプにドラッグ アンド ドロップします。

Answer:

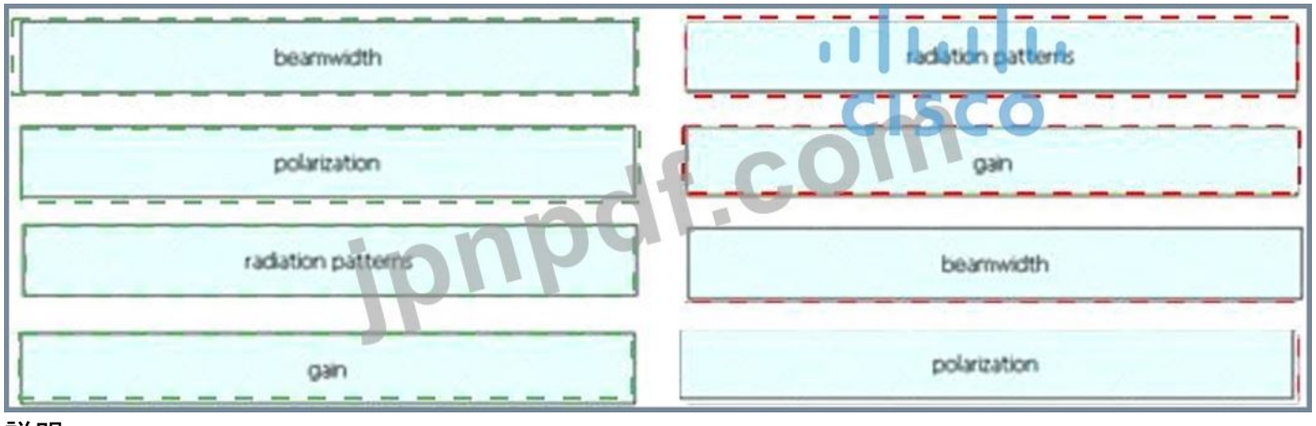
最新問題: **101**
QoS トラフィック シェーピングはネットワークの輻輳をどのように軽減しますか?
A. トラフィックが一定のビットレートを超えるとパケットをドロップします。
B. 認定レートを超えるパケットをバッファリングしてキューに入れます。
C. 大きなパケットを断片化し、配信のためにキューに入れます。
D. 優先度の低いキューからパケットをランダムにドロップします。
Answer: (解答を表示する**)**
説明
トラフィック シェーピングは、超過パケットをキューに保持し、その後の時間をかけて超過パケットを送信するようにスケジュールします。トラフィック シェーピングの結果、パケット出力レートが平滑化されます。



最新問題: **102**
左側のワイヤレス要素を右側の定義にドラッグ アンド ドロップします。

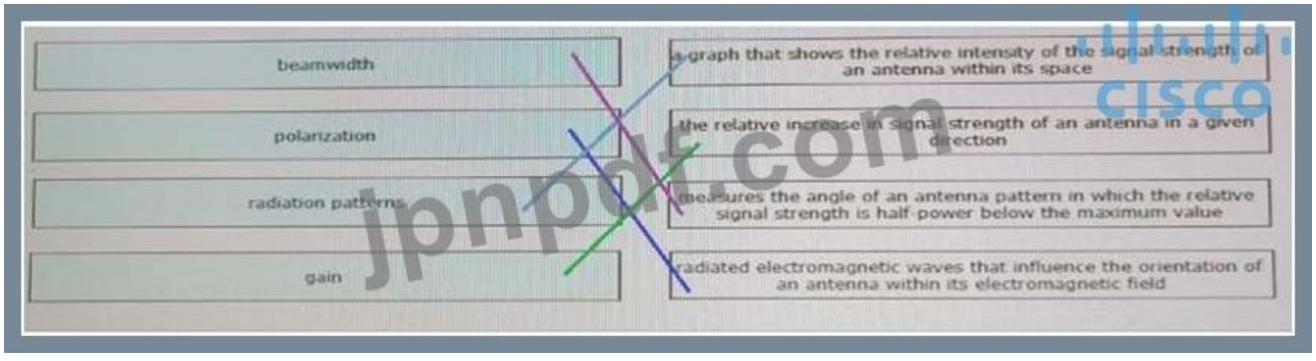


Answer:



説明

グラフ、折れ線グラフ 自動生成される説明



最新問題**: 103**

Cisco AP の FlexConnect モードに関する 2 つの説明のうち、正しいものはどれですか? (2つお選びください。)

A. FlexConnect モードは、ブランチ オフィスおよびリモート オフィスの導入向けのワイヤレス ソリューションです。

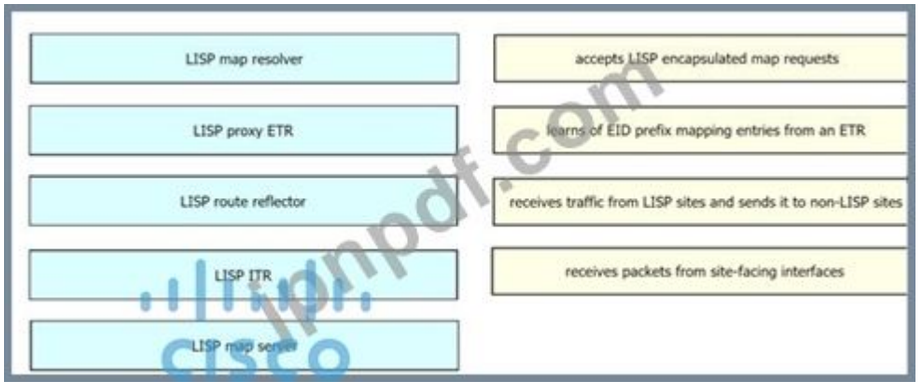
B. FlexConnect モードは、AP がメッシュ環境でセットアップされ、相互間のブリッジに使用される場合に使用されます。

C. FlexConnect モードは、指定された CAPWAP 対応 AP がクライアントとインフラストラクチャ間のデータトラフィックの管理から自身を除外できるように設計された機能です。

D. FlexConnect モードで動作する AP は不正 AP を検出できません。

E. コントローラに接続すると、FlexConnect AP はトラフィックをトンネルしてコントローラに戻すことができます。
Answer: A,E (メーッセージを残す**)**

最新問題**: 104**
LISP コンポーネントを左側から、右側で実行される機能にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。



Answer:

最新問題**: 105**
この EEM アプレット イベントは何を実現しますか?
「イベント snmp oid 1.3.6.1.3.7.1.5.1.2.4.2.9 get-type 次のエントリオプ g エントリ-val75 ポーリング間隔 5」
A. 5 回のポーリング サイクルの間、値が 75% を超えた場合に電子メールを発行します。
B. SNMP 変数を読み取り、値がライブ ポーリング サイクルの 75% を超えた場合。
C. 問い合わせ可能な SNMP 変数を示します。
D. 値が 75% に達すると、SNMP イベントが生成され、トラップ サーバーに送信されます。
Answer: B (メーッセージを残す**)**
説明
EEM は、イベントを監視し、監視対象のイベントが発生した場合、またはしきい値に達した場合に、情報提供または修正アクションを実行する機能を提供します。EEM ポリシーは、イベントとそのイベントの発生時に実行

されるアクションを定義するエンティティです。EEM ポリシーには、アプレットとスクリプトの 2 つのタイプがあります。アプレットは、CLI 設定内で定義される単純な形式のポリシーです。
Simple Network Management Protocol (SNMP)オブジェクト識別子の値をサンプリングすることによって実行される組み込みイベント マネージャ (EEM)アプレットのイベント基準を指定するには、アプレット コンフィギュレーション モードでevent snmp コマンドを使用します。
イベント SNMP oid oid-value get-type {正確 | } next} エントリ演算子 エントリ値 エントリ値 [exit-comb {または | and}] [exit-op 演算子] [exit-val exit-value] [exit-time exit-timevalue] ポーリング間隔 ポーリング整数値
+ oid: SNMPオブジェクト識別子(オブジェクトID)を指定します。
+ get-type: oid-value 引数で指定されたオブジェクト ID に適用される SNMP 取得操作のタイプを指定します。
- next - oid-value 引数で指定されたオブジェクト ID の英数字の後継であるオブジェクト ID を取得します。
+entry-op: 指定された演算子を使用して、現在のオブジェクト ID の内容とエントリ値を比較します。一致する場合、イベントがトリガーされ、終了基準が満たされるまでイベント監視が無効になります。
+entry-val: SNMP イベントを発生させるかどうかを決定するために現在のオブジェクト ID の内容を比較する値を指定します。
+ exit-op: 指定された演算子を使用して、現在のオブジェクト ID の内容と終了値を比較します。一致するものがあれば、イベントがトリガーされ、イベント監視が再び有効になります。
+ ポーリング間隔: 連続するポーリング間の時間間隔を指定します (秒単位) 参考: https://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtioseem.html 質問 2

最新問題**: 106**
MACsecの特徴は何ですか?
A. 802.1AE は Cisco AnyConnect NAM と SAP プロトコルを使用してネゴシエートされます
B. 802.1AE は、MKA プロトコルを使用してホストとスイッチ間で確立され、成功した 802 1X セッションのマスター セッション キーに基づいて暗号化キーをネゴシエートします。
C. 802.1AE は、Diffie-Hellman アルゴリズム (匿名暗号化モード) によって生成されたキーを使用する MKA プロトコルを使用してホストとスイッチ間で暗号化されます。
D. 802.1AE は暗号化および認証サービスを提供します
Answer: (解答を表示する**)**

最新問題**: 107**
Cisco SD-Access コントロール プレーンの特徴の 1 つは何ですか?

A. VXLAN テクノロジーに基づいています。
B. 各ルーターは、考えられるすべての宛先とルートを処理します。
C. ワイヤレス ネットワーク内でのみホストのモビリティを許可します。
D. リモート ルートを集中データベース サーバーに保存します。
Answer: D (メッセージを残す**)**
コントロール プレーン ノードは、ホスト トラッキング データベース (HTDB) を維持し、ロケーター/ID 分離プロトコル (LISP) を使用してマップ サーバーを提供し、ファブリック エッジ登録メッセージから HTDB にデータを取り込みます。マップ リゾルバーは、宛先ノードの位置情報を要求するエッジ デバイスからのクエリに応答します。

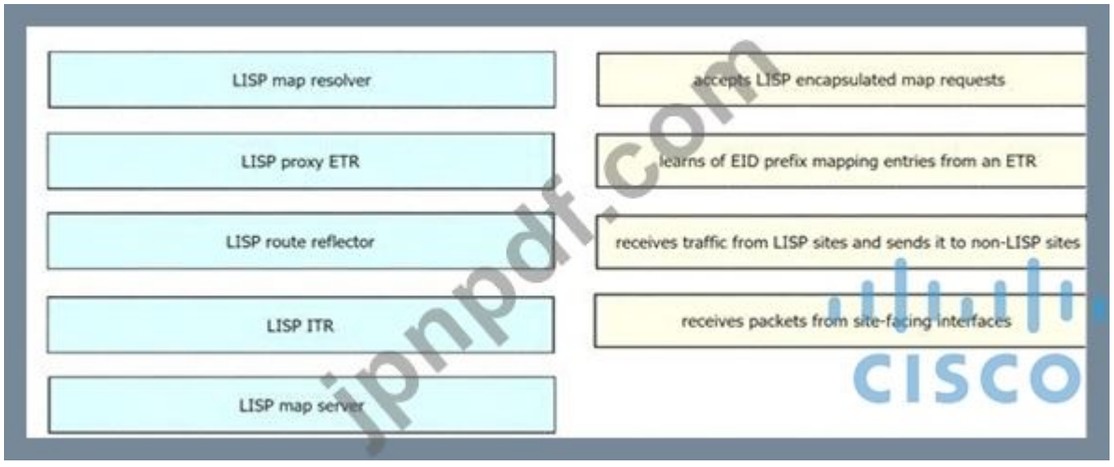
最新問題**: 108**
展示を参照してください。

```
R1#debug ip ospf hello
R1#debug condition interface Fa0/1
      Condition 1 Set
```

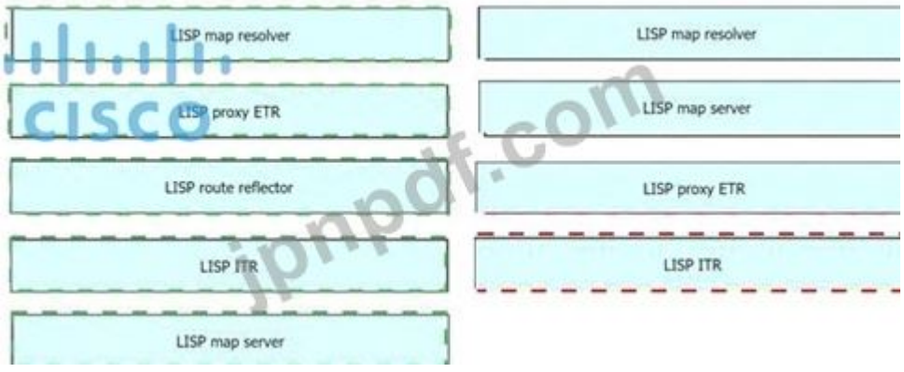
OPSF デバッグ出力について正しいのはどれですか?
A. 出力には、ルータ R1 が送信してインターフェイス Fa0/1 で受信したすべての OSPF メッセージが表示されます。
B. 出力には、ルータ R1 がすべてのインターフェイスで送受信したすべての OSPF メッセージが表示されます。
C. 出力には、ルータ R1 が送信し、インターフェイス Fa0/1 で受信した OSPF hello メッセージが表示されます。
D. 出力には、ルータ R1 が送受信した OSPF hello および LSACK メッセージが表示されます。
Answer: C (メッセージを残す**)**
説明
このコマンドの組み合わせは 「条件付きデバッグ」として知られており、条件に基づいてデバッグ出力をフィルター処理します。追加された各条件は、ブール論理の 「And」演算子のように動作します。 「debug ip ospf hello」の例をいくつか以下に示します。

```
*Oct 12 14:03:32.595: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet1/0 from
192.168.12.2
*Oct 12 14:03:33.227: OSPF: Rcv hello from 1.1.1.1 area 0 on FastEthernet1/0 from
192.168.12.1
*Oct 12 14:03:33.227: OSPF: Mismatched hello parameters from 192.168.12.1
```


最新問題**: 109**
LISP コンポーネントを左側から、右側で実行される機能にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。

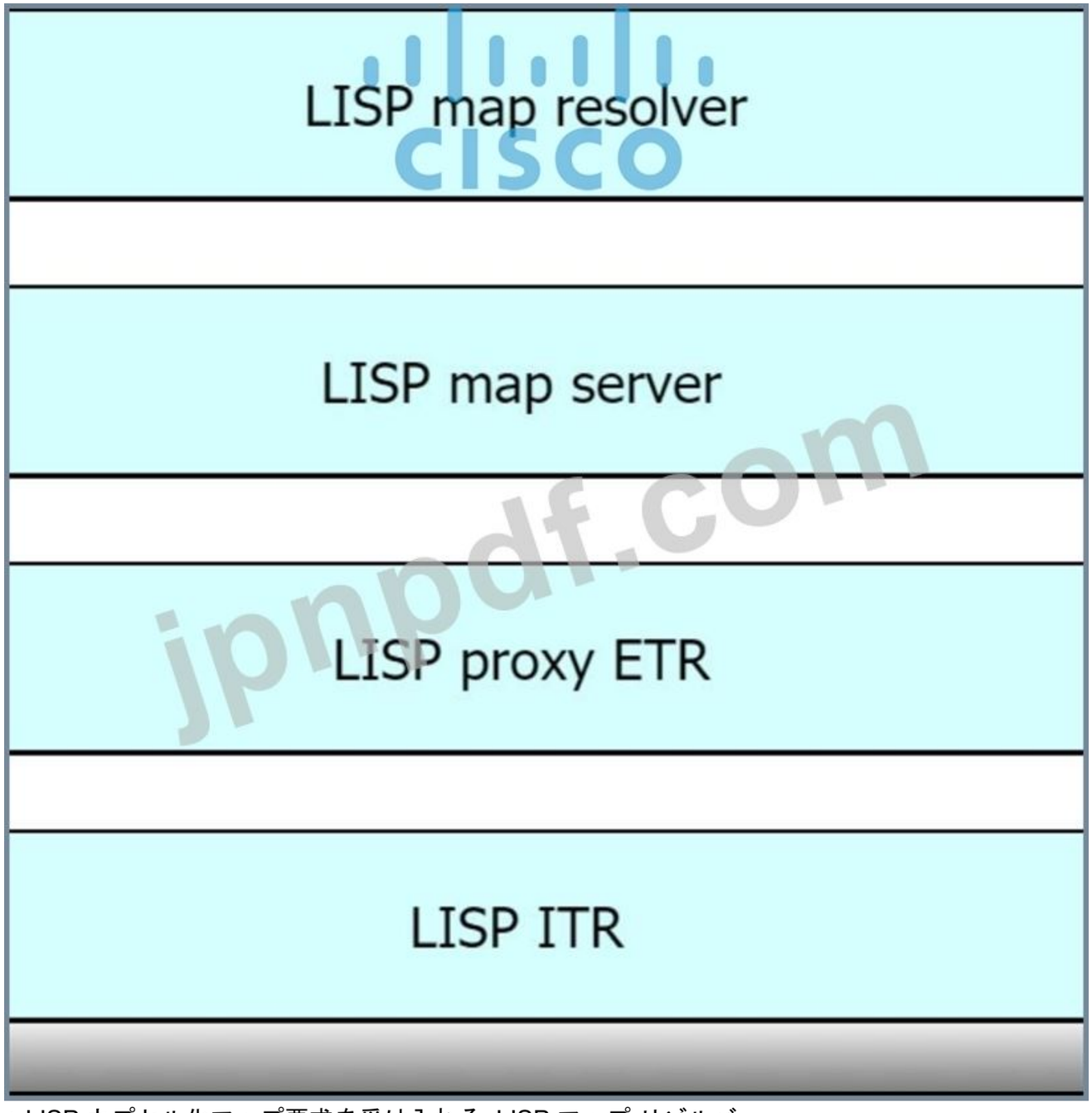


Answer:



説明

テーブルの説明が自動的に生成される



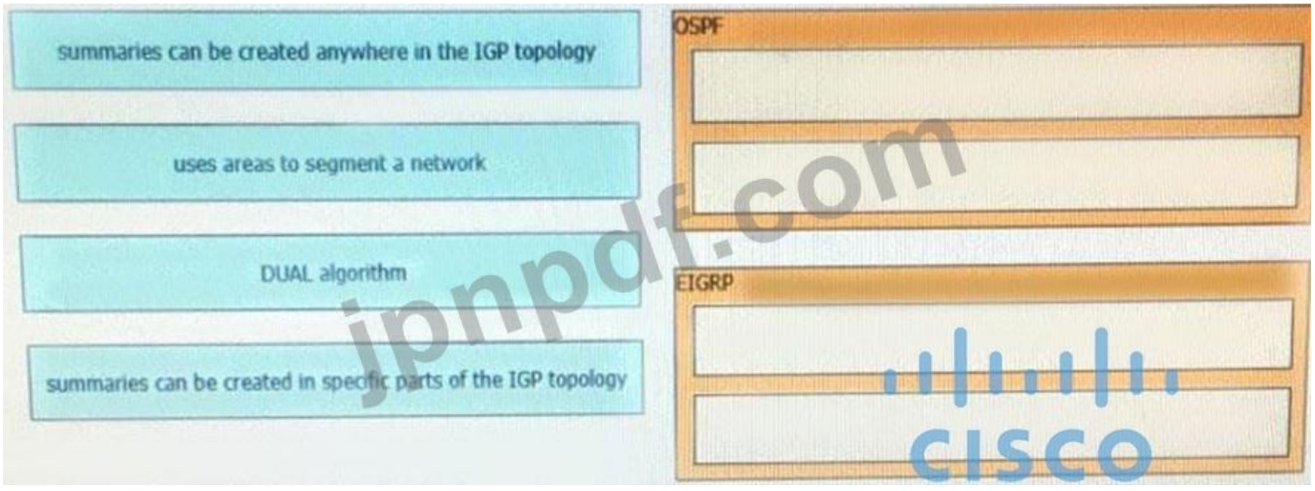
+ LISP カプセル化マップ要求を受け入れる: LISP マップ リゾルバー
+ ETR から EID プレフィックス マッピング エントリを学習します: LISP マップ サーバー
+ LISP サイトからトラフィックを受信し、非 LISP サイトに送信します: LISP プロキシ ETR
+ サイト側インターフェイスからパケットを受信: LISP ITR

説明

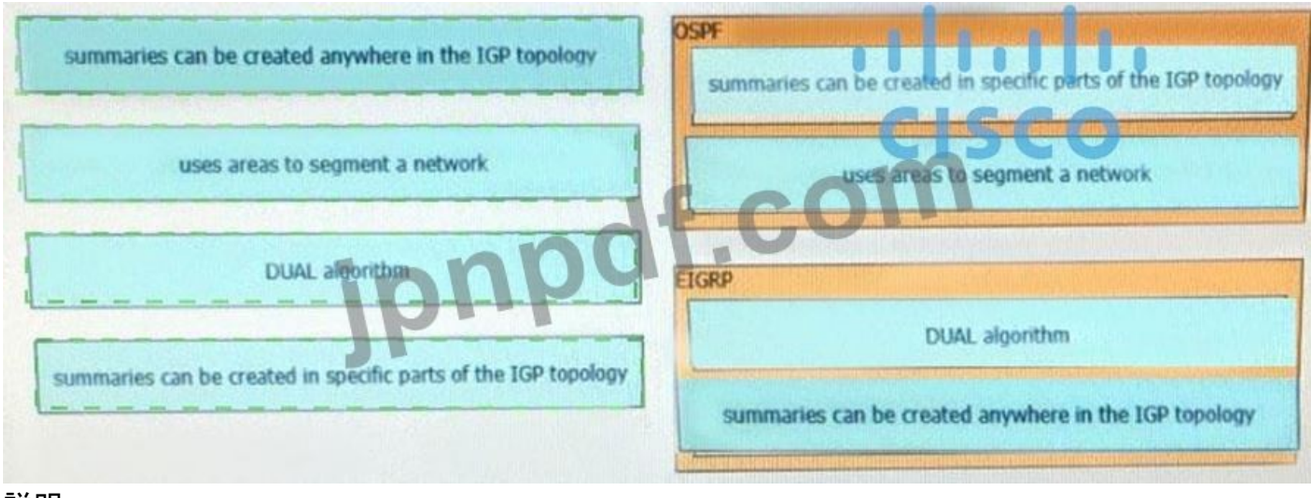
ITR は、宛先 EID を宛先 RLOC にマッピングし、ITR RLOC の送信元 IP アドレスと出力トンネル ルーター (ETR) の RLOC の宛先 IP アドレスを含む追加のヘッダーで元のパケットをカプセル化する機能です。
カプセル化後、元のパケットは LISP パケットになります。
ETR は、LISP でカプセル化されたパケットを受信し、カプセル化を解除して、ローカル EID に転送する機能です。この機能には EID から RLOC へのマッピングも必要なため、『マップ サーバー』の IP アドレスと認証用のキー (パスワード) を指定する必要があります。

LISP プロキシ ETR (PETR) は、非 LISP サイトに代わって ETR 機能を実装します。PETR は通常、LISP サイトが非 LISP サイトにトラフィックを送信する必要があるが、ルーティング可能な EID をパケット ソースとして受け入れないサービス プロバイダーを介して LISP サイトが接続されている場合に使用されます。PETR は ETR と同様に機能しますが、EID が非 LISP サイトの宛先にトラフィックを送信する点が異なります。
Map Server (MS) は、認証キーの登録と EID から RLOC へのマッピングを処理します。ETR は、設定されているすべての Map Server に定期的な Map-Register メッセージを送信します。
マップ リゾルバ (MR): LISP カプセル化マップ リクエスト (通常は ITR から) を受け入れる LISP コンポーネントで、宛先 IP アドレスが EID 名前空間の一部であるかどうかを迅速に判断します。

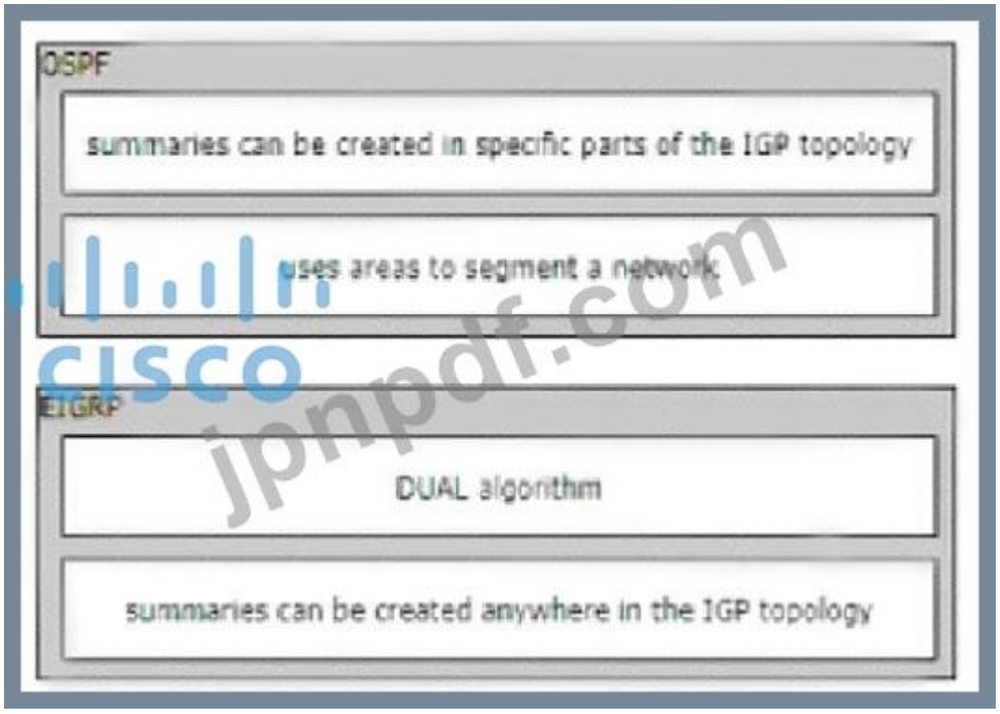
最新問題: **110**
説明を左側から、右側に説明されているルーティング プロトコルにドラッグ ドロップします。



Answer:



説明



ABR または ASBR でのみ集約できる OSPF とは異なり、EIGRP ではどこでも集約できます。手動サマライズは、ip summary-address eigrp asnumber アドレス マスク [administrative- distance summary-address eigrp 1 192.168.16.0 255.255.248.0) を介して、EIGRP ドメイン内のどこでも、すべてのルータ上、すべてのインターフェイス上に適用できます。少なくとも 1 つ以上の特定のルートが存在する限り、要約ルートはルーティングテーブルに存在します。最後の特定ルートが消えると、まとめルートもフェードアウトします。EIGRP 手動サマリー ルートで使用されるメトリックは、特定のルートの最小メトリックです。

最新問題: **111**
どの OSPF ネットワーク タイプに互換性があり、2 つのピアリング デバイスを介した通信が可能ですか?
A. 放送から非放送へ
B. ポイントツーマルチポイントから非ブロードキャストへ
C. ポイントツーポイントへのブロードキャスト
D. ポイントツーマルチポイントからブロードキャストへ
Answer: (解答を表示する**)**
次のさまざまな OSPF タイプは相互に互換性があります。
+ ブロードキャストおよび非ブロードキャスト (ハロー/デッド タイマーを調整)
+ ポイントツーポイントおよびポイントツーマルチポイント (ハロー/デッド タイマーを調整)
ブロードキャスト ネットワークと非ブロードキャスト ネットワークは、互換性を保つために DR/BDR を選択します。ポイントツーポイント/マルチポイントは DR/BDR を選択しないため、互換性があります。

最新問題: **112**
Cisco SD-Access ファブリック データ プレーンを設計する場合、どのトンネリング技術が使用されますか?
A. LISP
B. VRFライト

C. VRF
D. VXLAN
Answer: D (メーッセージを残す**)**
説明

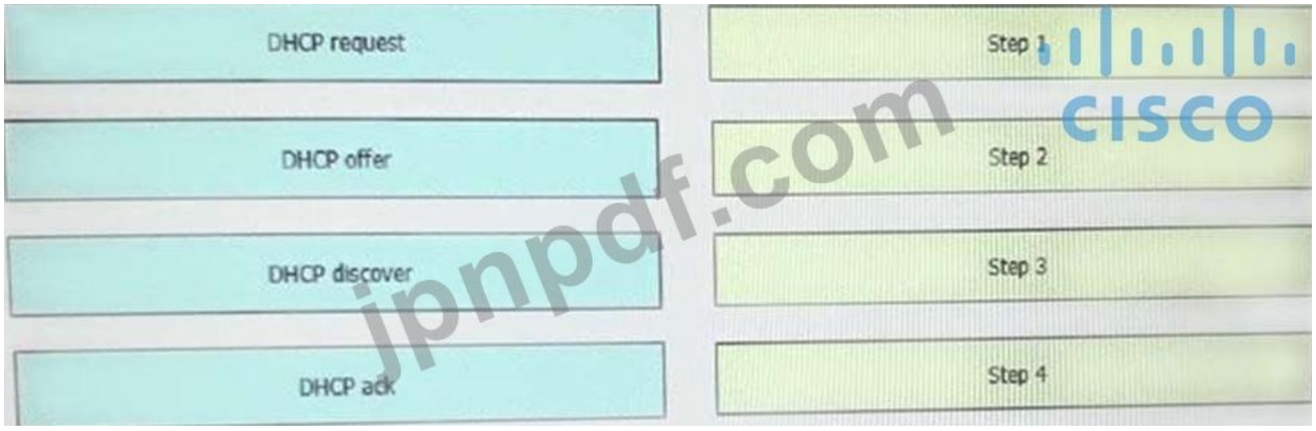
ファブリック データ プレーンに使用されるトンネリング テクノロジーは、Virtual Extensible LAN (VXLAN) に基づいています。
VXLAN カプセル化は UDP ベースです。つまり、任意の IP ベースのネットワーク (レガシーまたはサードパーティ) によって転送でき、SD-Access ファブリックのオーバーレイ ネットワークを作成できます。LISP は SD-Access ファブリックのコントロール プレーンですが、データ プレーンに LISP データ カプセル化を使用しません。代わりに、VXLAN カプセル化を使用します。これは、LISP では元のイーサネット ヘッダーをカプセル化して MAC-in-IP カプセル化を実行できるためです。VXLAN を使用すると、SD-Access ファブリックがレイヤ 2 およびレイヤ 3 の仮想トポロジ (オーバーレイ) をサポートし、組み込みのネットワーク セグメンテーション (VRF インスタンス/VN) と組み込みのグループベースを備えた任意の IP ベースのネットワーク上で動作できるようになります。ポリシー。
参考: CCNP および CCIE Enterprise Core ENCOR 350-401 公式認定ガイド

最新問題**: 113**
左側の特性を、右側で説明されているオーケストレーション ツールにドラッグ アンド ドロップします。

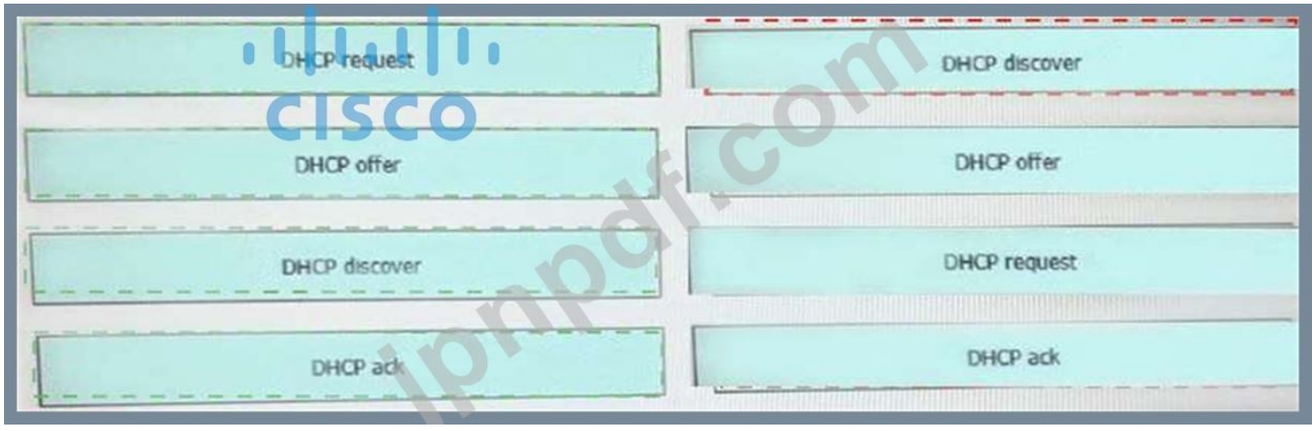
Answer:

最新問題**: 114**

クライアントと AP の間で交換される DHCP メッセージを、右側の交換順序にドラッグ アンド ドロップします。



Answer:



説明

DHCP クライアントと DHCP サーバーの間では、DHCPDISCOVER、DHCPO FFER、DHCPREQUEST、および DHCPACKNOWLEDGEMENT の 4 つのメッセージが送信されます。
このプロセスは、DORA (Discover、Offer、Request、Acknowledgement) と略されることがよくあります。

最新問題: **115**
ルータの WAN インターフェイスに適用される送信アクセス リストは、IP アドレス 10.10.10.1 のワークステーションから送信される http トラフィックを除くすべてのトラフィックを許可しますか?
A)

```
ip access-list extended 100
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

B)

```
ip access-list extended 200
deny tcp host 10.10.10.1 eq 80 any
permit ip any any
```

C)

```
ip access-list extended NO_HTTP
deny tcp host 10.10.10.1 any eq 80
```

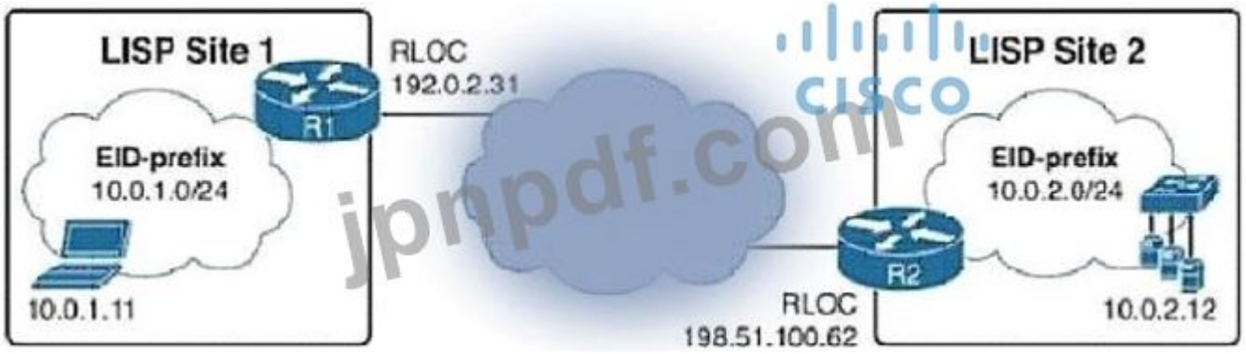
D)

```
ip access-list extended 10
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

A. オプション A
B. オプション C
C. オプション D
D. オプション B
Answer: A (メーッセージを残す**)**

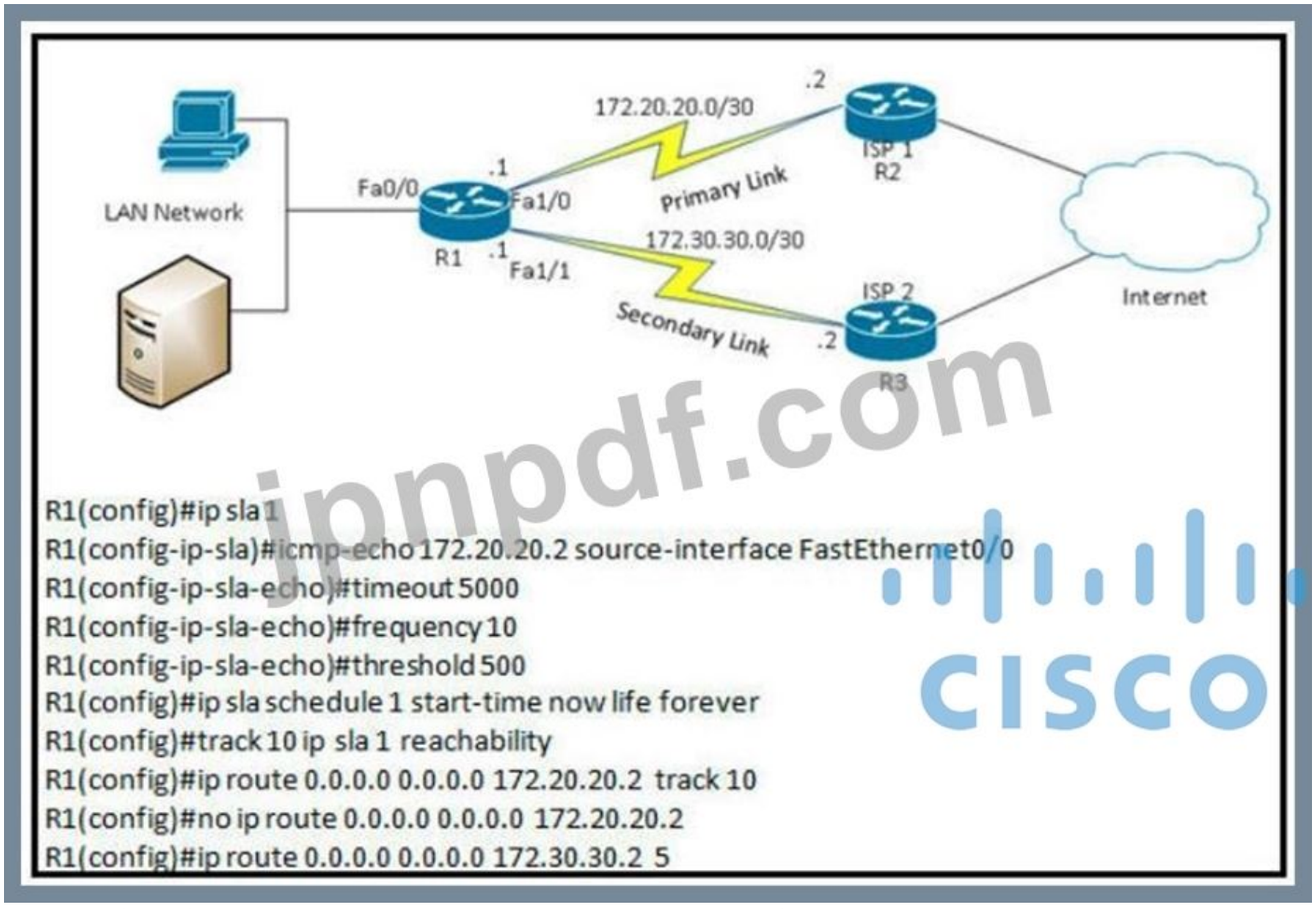
最新問題: **116**
EIGRP OTP 実装における LISP カプセル化に関する記述のうち、正しいものはどれですか?
A. LISP はネクストホップを学習します
B. OTP は LISP カプセル化を使用してネイバーからルートを取得します
C. OTP は動的マルチポイント トンネリングに LISP カプセル化を使用します。
D. OTP は LISP コントロール プレーンを維持します
Answer: D (メーッセージを残す**)**
説明
EIGRP オーバー ザ トップ ソリューションを使用すると、異なる EIGRP サイト間の接続を確保できます。この機能は、コントロール プレーンで EIGRP を使用し、データ プレーンで Locator ID Separation Protocol（LISP）カプセル化を使用して、基盤となる WAN アーキテクチャ全体でトラフィックをルーティングします。EIGRP は、ネットワーク内のカスタマー エッジ (CE) デバイス間でルートを分散するために使用され、WAN アーキテクチャ全体で転送されるトラフィックは LISP でカプセル化されます。
EIGRP OTP はデータ プレーンに LISP のみを使用します。EIGRP は引き続きコントロール プレーンに使用されます。したがって、データとコントロール プレーン トラフィックの両方をカプセル化する必要があるた

め、OTP が動的マルチポイント トンネリングに LISP カプセル化を使用しているとは言えません。-> 「OTP は動的マルチポイント トンネリングに LISP カプセル化を使用する」という回答は正しくありません。
OTP では、EIGRP は LISP コントロール プレーン プロトコルの代替として機能します（したがって、EIGRP は LISP ではなくネクスト ホップを学習します -> 「LISP がネクスト ホップを学習する」という回答は正しくありません）。ネイティブ LISP マッピング サービスで EID から RLOC への動的なマッピングを行う代わりに、サービス プロバイダー クラウド上で OTP を実行する EIGRP ルーターは、ターゲット セッションを作成し、サービス プロバイダーによって提供された IP アドレスを RLOC として使用し、ルートを EID として交換します。
例を挙げてみましょう:



R1 と R2 が相互に OTP を実行した場合、R1 は EIGRP を通じて R2 からネットワーク 10.0.2.0/24 について学習し、プレフィックス 10.0.2.0/24 を EID プレフィックスとして扱い、アドバタイジング ネクスト ホップを取得します。
この EID プレフィックスの RLOC として 198.51.100.62 を使用します。同様に、R2 は EIGRP を通じてネットワーク 10.0.1.0/24 について R1 から学習し、プレフィックス 10.0.1.0/24 を EID プレフィックスとして扱い、アドバタイジング ネクスト ホップ 192.0.2.31 をこの EID プレフィックスの RLOC として取得します。両方のルータで、この情報は LISP マッピング テーブルにデータを入力するために使用されます。パケットが
10.0.1.0/24 から
10.0.2.0/24 が R1 に到着すると、通常の LISP と同じように LISP マッピング テーブルを使用して、パケットを LISP カプセル化して 198.51.100.62 に向けてトンネリングする必要があることを検出します (逆も同様)。LISP データ プレーンは OTP で再利用され、変更されません。ただし、ネイティブ LISP のマッピングおよび解決メカニズムは EIGRP に置き換えられます。

最新問題**: 117**
出品物を参照してください。



IP SLA 追跡が失敗する 2 つの理由は何ですか? (2つお選びください)

A. 送信元インターフェイスが正しく構成されていません。

B. デフォルト ルートのネクスト ホップ IP アドレスが間違っています

C. 閾値が間違っています

D. icmp-echo の場合、宛先は 172.30 30 2 である必要があります。

E. R1 LAN ネットワークに戻るルートが R2 にありません

Answer: B,E (メーッセージを残す)

最新問題**: 118**

展示を参照してください。

VTY ユーザーにはどの権限レベルが割り当てられますか?

A. 7

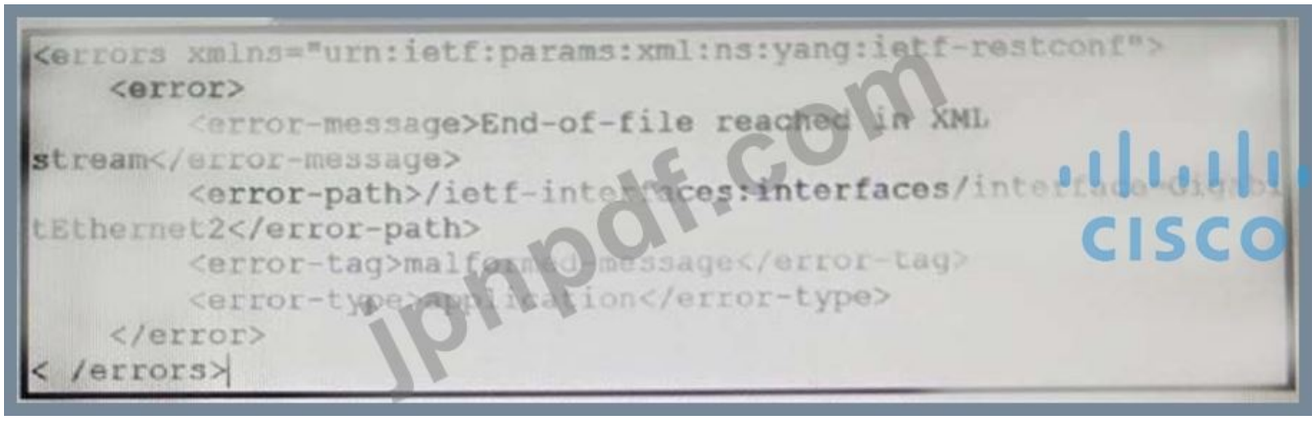
B. 13

C. 1

D. 15

Answer: C (メーッセージを残す**)**

最新問題**: 119**



展示を参照してください。エンジニアはアプリケーションで XML を使用して、RESTCONF 対応デバイスに情報を送信しています。リクエストを送信した後、エンジニアはこの応答メッセージと HTTP 応答コード 400 を受け取ります。これらの応答はエンジニアに何を伝えるのでしょうか?

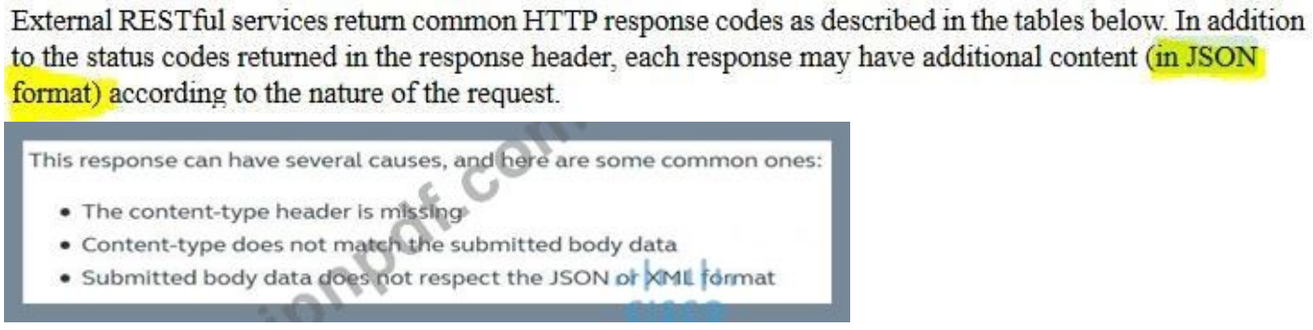
A. 送信された Accept ヘッダーは application/xml でした

B. PUT の代わりに POST を使用して更新しました

C. 送信された Content-Type ヘッダーは application/xml でした。

D. JSONボディが使用されました

Answer: C (メーッセージを残す**)**



最新問題**: 120**

CEF スイッチングは、Cisco デバイスのプロセス スイッチングとどのように異なりますか?

A. CEF スイッチングは、ラインカード上の専用メモリ内の隣接テーブルを並べ替えることでメモリを節約し、プロセス スイッチングはすべてのテーブルをメイン メモリに保存します。

B. CEF スイッチングでは CDP プロトコルによって構築された隣接テーブルが使用され、プロセス スイッチングではルーティング テーブルが使用されます。

C. CEF スイッチングは専用のハードウェア プロセッサを使用し、プロセス スイッチングはメイン プロセッサを使用します。
D. CEF スイッチングは、MAC アドレス検索に IS-IS に基づく独自のプロトコルを使用し、プロセス スイッチングは MAC アドレス テーブルで使用します。
Answer: B (メーッセージを残す**)**
説明
シスコ エクスプレス フォワーディング（CEF）スイッチングは、デマンド キャッシングに関連する問題に対処することを目的とした、独自の形式のスケーラブルなスイッチングです。CEF スイッチングでは、従来ルート キャッシュに保存されていた情報が複数のデータ構造に分割されます。CEF コードは、ギガビット ルート プロセッサ（GRP）だけでなく、ラインカードなどのスレーブ プロセッサでもこれらのデータ構造を維持できます。12000ルーター。効率的なパケット転送のために最適化されたルックアップを提供するデータ構造には次のものがあります。
* 転送情報ベース（FIB）テーブル - CEF は FIB を使用して、IP 宛先プレフィックス ベースのスイッチング決定を行います。FIB は概念的にはルーティング テーブルまたは情報ベースに似ています。IP ルーティング テーブルに含まれる転送情報のミラー イメージを維持します。ネットワーク内でルーティングまたはトポロジの変更が発生すると、IP ルーティング テーブルが更新され、これらの変更が FIB に反映されます。FIB は、IP ルーティング テーブル内の情報に基づいてネクストホップ アドレス情報を維持します。
FIB エントリとルーティング テーブル エントリの間には 1 対 1 の相関関係があるため、FIB にはすべての既知のルートが含まれており、高速スイッチングや最適なスイッチングなどのスイッチング パスに関連するルート キャッシュのメンテナンスの必要がなくなります。
* 隣接テーブル - ネットワーク内のノードは、リンク層を介して単一ホップで相互に到達できる場合、隣接していると言われます。FIB に加えて、CEF は隣接テーブルを使用して、レイヤ 2 アドレス指定情報を先頭に付加します。隣接関係テーブルは、すべての FIB エントリのレイヤ 2 ネクストホップ アドレスを維持します。
CEF は、次の 2 つのモードのいずれかで有効にできます。
* 中央 CEF モード - CEF モードが有効な場合、CEF FIB と隣接テーブルはルート プロセッサ上に常駐し、ルート プロセッサがエクスプレス フォワーディングを実行します。ラインカードが CEF スイッチングに使用できない場合、または分散 CEF スイッチングと互換性のない機能を使用する必要がある場合は、CEF モードを使用できます。
* 分散 CEF（dCEF）モード - dCEF が有効な場合、ラインカードは FIB および隣接関係テーブルの同一のコピーを維持します。ラインカードは独自に高速転送を実行できるため、メイン プロセッサであるギガビット ルート プロセッサ（GRP）がスイッチング動作に関与する必要がなくなります。これは、Cisco 12000 シリーズ ルータで使用できる唯一のスイッチング方式です。
dCEF は、プロセス間通信（IPC）メカニズムを使用して、ルート プロセッサとラインカード上の FIB と隣接テーブルの同期を確保します。
CEF スイッチングの詳細については、『Cisco Express Forwarding (CEF) White Paper』を参照してください。

最新問題**: 121**
展示を参照してください。

WLC 管理者は、ローミング クライアントが関連付けられているコントローラのモビリティ ロール アンカーが [クライアント（Clients）] > [詳細（Detail）] で設定されていることを確認します。どのタイプのローミングがサポートされていますか?

A. レイヤ 2 インターコントローラ

B. コントローラ内

C. レイヤ 3 インターコントローラ

D. 間接的

Answer: C (メーッセージを残す)

最新問題: **122**

同じインターフェイス上の他の VLAN トラフィックを無視しながら、インターフェイス ギガビットイーサネット 0/3 上の VLAN 3 からの発信トラフィックをキャプチャするように RSPAN を設定するコマンド セットはどれですか?

A)

```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 3
```

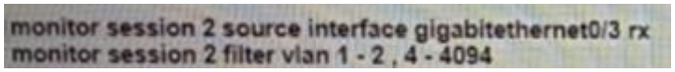
B)

```
monitor session 2 source interface gigabitethernet0/3 tx
monitor session 2 filter vlan 1 - 2 , 4 - 4094
```

C)

```
monitor session 2 source interface gigabitethernet0/3 rx
monitor session 2 filter vlan 3
```

D)



A. オプション A
B. オプション D
C. オプション C
D. オプション B
Answer: A (メーッセージを残す**)**

最新問題**: 123**
企業がオンプレミス展開ではなくクラウド展開を選択する 2 つの理由は何ですか? (2つ選択してください)
A. クラウド環境では、技術的な問題は会社が管理します。オンプレミス環境では、技術的な問題を解決するためにサービス プロバイダーに依存します。
B. クラウドのコストは、消費されるリソースの量に応じて上下に調整されます。ハードウェア、電力、およびスペースに関するオンプレミスのコストは、使用状況に関係なく継続的に発生します。
C. クラウド導入には資本支出プロセスのため、長い実装時間が必要です。オンプレミスの導入は、運用支出プロセスを使用して迅速に完了できます。
D. クラウド リソースは、需要の増加に合わせて自動的に拡張されます。オンプレミスでは追加の資本支出が必要です。
E. クラウド環境では、企業はデータへのアクセスを完全に制御できます。オンプレミスでは、サービス プロバイダーの停止によるデータへのアクセスのリスクが発生します
Answer: B,D (メーッセージを残す**)**

最新問題**: 124**
エンジニアは、定義されている他のすべての認証方法が失敗した場合に、ユーザーがローカル認証を使用してログインできるようにするログイン認証方法を有効にする必要があります。どの構成を適用する必要がありますか?
A. 認証ログイン CONSOLE グループ半径ローカル有効なし
B. aaa 認証ログイン CONSOLE グループ radius local-case Enable aaa
C. aaa 認証ログイン CONSOLE グループ tacacs+ ローカル有効化
D. aaa 認証ログイン CONSOLE グループ radius ローカル イネーブル
Answer: (解答を表示する**)**

最新問題**: 125**
AP がワイヤレス LAN コントローラを検出するために使用する 2 つの方法はどれですか? (2つお選びください。)
A. ローカルサブネット上でブロードキャストします。
B. Cisco Discovery Protocol ネイバー
C. DNS ルックアップ cisco-DNA-PRIMARY.localdomain
D. DHCP オプション 43
E. 他の AP にクエリを実行します

Answer: (解答を表示する**)**

最新問題**: 126**
Cisco DNA Center REST API が PUT を /dna/intent/api/v1/network-device エンドポイントに送信します 応答コード 504 を受信します コードは何を示していますか?
A. Web サーバーが利用できません
B. ユーザーには、このエンドポイントにアクセスする権限がありません。
C. 設定された間隔に基づいて応答がタイムアウトしました
D. ユーザー名とパスワードが正しくありません
Answer: C (メーッセージを残す**)**

最新問題**: 127**
2 台のルーターの Gig0/0 インターフェイスは、1G イーサネット リンクに直接接続されています。DR/BDR 関係を維持せずに OSPF 隣接関係を確立するには、両方のルーターのインターフェイスにどの設定を適用する必要がありますか?
A)

```
interface Gig0/0
ip ospf network point-to-multipoint
```

B)

```
interface Gig0/0
ip ospf network point-to-point
```

C)

```
interface Gig0/0
ip ospf network broadcast
```

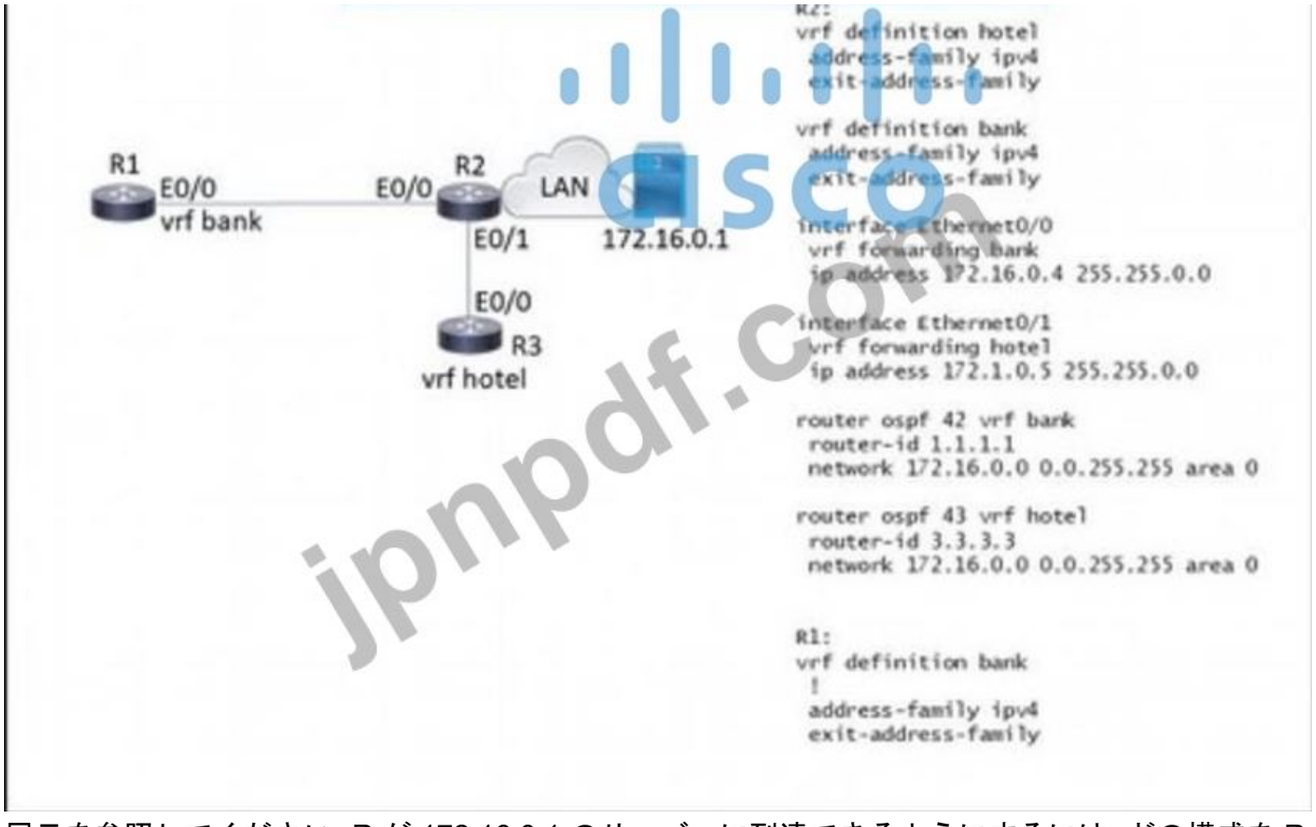
D)

```
interface Gig0/0
 ip ospf network non-broadcast
```

A. オプション A
B. オプション B
C. オプション C
D. オプション D
Answer: (解答を表示する**)**
説明
cisco_R3#show run int e0/0.50
建物構成...
現在の構成: 189 バイト
！
インターフェイス Ethernet0/0.50
カプセル化 dot1Q 50
IP アドレス 10.111.10.1 255.255.255.252

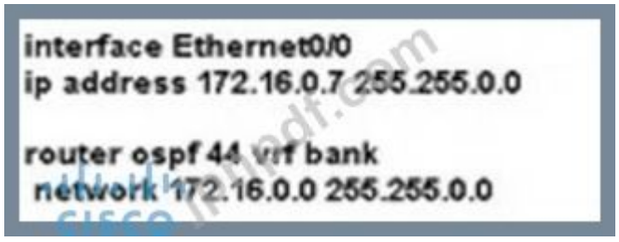
ip ospf ネットワーク ポイントツーポイント <<<<<<<<<<<<<<<<<<<<
IP OSPF 1 エリア 22
bfd 間隔 999 min_rx 999 乗数 3
終わり
cisco_R3#show ip ospf ネイバー
ネイバー ID プリステート デッド タイム アドレス インターフェイス
192.168.255.2 1 フル/ドロザー 00:00:33 192.168.255.2 イーサネット 0/0.10
200.200.200.200 1 フル/DR 00:00:34 192.168.255.22 イーサネット0/0.10
5.5.5.5 0 フル/ - 00:00:34 10.111.10.2 Ethernet0/0.50 <<<<<<<<<<<<<<<<<< cisco_R3#

最新問題**: 128**
z

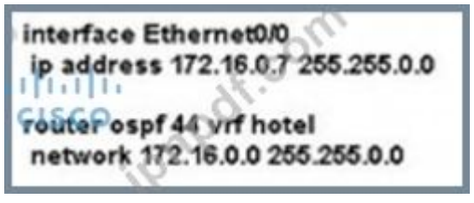


展示を参照してください。R が 172.16.0.1 のサーバーに到達できるようにするには、どの構成を R に適用する必要がありますか?

A.
```
interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf bank
 network 172.16.0.0 0.0.255.255 area 0
```

B.


C.


D.


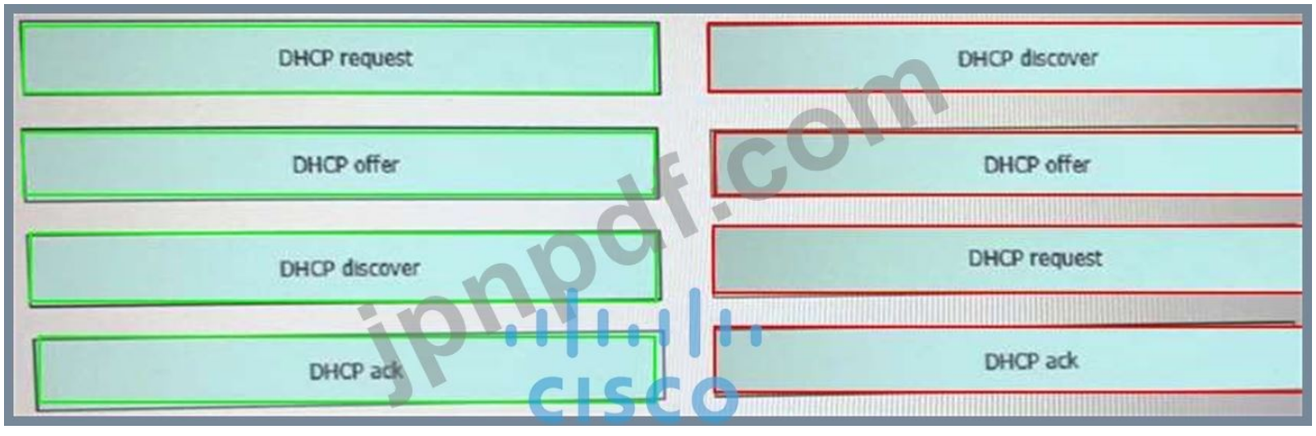
Answer: C (メッセージを残す)

最新問題**: 129**
CAPWAP 検出を試行するときに、アクセス ポイントはどの DNS ルックアップを実行しますか?
A. CISCO-DNA-CONTROLLER.local
B. CAPWAP-CONTROLLER.local
C. CISCO-CONTROLLER.local
D. CISCO-CAPWAP-CONTROLLER.local
Answer: D (メッセージを残す)
Lightweight AP (LAP) は、ドメイン ネーム サーバー (DNS) を通じてコントローラを検出できます。アクセス ポイント AP)でこれを行うには、CISCO-LWAPP-CONTROLLER.localdomain に応答してコントローラ IP アドレスを返すように DNS を設定する必要があります。localdomain は AP ドメイン名です。AP は、DHCP サーバから IP アドレスと DNS 情報を受信すると、DNS に接続して CISCO-CAPWAP-CONTROLLER.localdomain を解決します。DNS がコントローラの IP アドレスのリストを送信すると、AP はコントローラに検出要求を送信します。
AP は、DNS 名 CISCO-CAPWAP-CONTROLLER.localdomain の解決を試みます。AP がこの名前を 1 つ以上の IP アドレスに解決できる場合、AP は解決された IP アドレスにユニキャスト CAPWAP Discovery メッセージを送信します。CAPWAP Discovery Request メッセージを受信した各 WLC は、ユニキャスト CAPWAP DiscoveryResponse で AP に応答します。

最新問題**: 130**

クライアントと AP の間で交換される DHCP メッセージを、右側の交換順序にドラッグ アンド ドロップします。

Answer:



最新問題**: 131**

展示を参照してください。

展示を参照してください。ネットワーク管理者は、switch1 と switch2 の間の問題をトラブルシューティングするために RSPAN を設定しました。スイッチはインターフェイス GigabitEthernet 1/1 を使用して接続されます。外部パケット キャプチャ デバイスは、switch2 インターフェイスの GigabitEthernet 1/2 に接続されています。この構成を完了するには、どの 2 つのコマンドを追加する必要がありますか? (2つお選びください)

```
switch2(config)# monitor session 1 source remote vlan 70
switch2(config)# monitor session 1 destination interface GigabitEthernet1/2

switch2(config)# monitor session 1 source remote vlan 70
switch2(config)# monitor session 1 destination interface GigabitEthernet1/1

switch1(config)# interface GigabitEthernet 1/1
switch1(config-if)# switchport mode access
switch1(config-if)# switchport access vlan 10

switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)# switchport mode access
switch2(config-if)# switchport access vlan 10

switch2(config)# monitor session 2 destination vlan 10

switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-80
```

A. オプション E
B. オプション D
C. オプション C
D. オプション B
E. オプション A
Answer: (解答を表示する**)**

最新問題**: 132**

```
Switch2#
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/23, putting Fa0/23 in err-disable
state
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/24, putting Fa0/24 in err-disable
state
Switch2#


Switch1#show etherchannel summary

!output omitted

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------
1      Po2(SD)         LACP      Fa1/0/23(D)


Switch2#show etherchannel summary

!output omitted

Group  Port-channel  Protocol    Ports
------+-------------+-----------+------------------------
1      Po1(SD)           -        Fa0/23(D)   Fa0/24(D)
```

展示を参照してください。エンジニアはスイッチ 1 とスイッチ 2 の間で EtherChannel を設定しており、スイッチ 2 のコンソール メッセージに気づきました。出力に基づいて、どのアクションがこの問題を解決しますか?

A. Switch2 のメンバー ポートを少なく設定します。

B. 両方のスイッチで同じポート チャネル インターフェイス番号を設定します。

C. 両方のスイッチで同じ EtherChannel プロトコルを設定します。

D. Switch1 にさらにメンバー ポートを設定します。

Answer: (解答を表示する**)**

説明

この場合、Switch2 でネゴシエーション プロトコルを使用せずに EtherChannel を使用しています。その結果、反対側のスイッチもそれぞれのポートで EtherChannel 動作用に設定されていない場合、スイッチング ループが発生する危険性があります。EtherChannel Misconfiguration Guard は、EtherChannel にバンドルされているすべてのポートを無効にすることで、ループの発生を防止しようとします。

最新問題**: 133**

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
209.165.201.6   209.165.201.1   QM_IDLE           1001 ACTIVE
```

展示を参照してください。IPsec VPN を設定した後、エンジニアは show コマンドを入力して ISAKMP SA ステータスを確認します。ステータスは何を示していますか?

A. ISAKMP SA が認証されており、クイックモードで使用できます。

B. ピアは鍵を交換しましたが、ISAKMP SA は認証されていないままです。

C. VPN ピアは ISAKMP SA のパラメータについて合意しました

D. ISAKMP SA は作成されましたが、形成が継続されていません。

Answer: A (メーッセージを残す**)**

説明

ISAKMP SA が認証されました。ルーターがこの交換を開始した場合、この状態はすぐに QM_IDLE に移行し、クイック モード交換が開始されます。

https://www.ciscopress.com/articles/article.asp?p=606584

最新問題**: 134**

展示を参照してください。

```
SwitchC#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally       : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Transparent
VTP Domain Name                 : cisco.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MDS digest                      : 0xES 0x28 0x5D 0x3E 0x2F 0xES 0xAD 0x2B
Configuration last modified by 0.0.0.0 at 1-10-19 09:01:38

SwitchC#show vlan brief

VLAN  Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1     default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6,
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10,
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14,
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18,
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22,
                                                 Fa0/23, Fa0/24, Po1
110 Finance                          active
210 HR                               active    Fa0/1
310 Sales                            active    Fa0/2
[...output omitted...]

SwitchC#show int trunk
Port        Mode         Encapsulation      Status        Native vlan
Gig1/1      on           802.1q             trunking      1
Gig1/2      on           802.1q             trunking      1

Port        Vlans allowed on trunk
Gig1/1      1-1005
Gig1/2      1-1005

Port        Vlans allowed and active in management domain
Gig1/1      1, 110, 210, 310
Gig1/2      1, 110, 210, 310

Port        Vlans in spanning tree forwarding state and not pruned
Gig1/1      1, 110, 210, 310
Gig1/2      1, 110, 210, 310

SwitchC#show run interface port-channel 1
interface Port-channel 1
 description Uplink_to_Core
 switchport mode trunk
```

SwitchC は、HR と Sales をコア スイッチに接続します。ただし、ビジネス ニーズでは、Finance VLAN からのトラフィックがこのスイッチを通過しないことが必要です。

この要件を満たすコマンドはどれですか?

A. SwitchC(config)#インターフェイス ポート チャネル 1

SwitchC(config-if)#switchport トランク許可 vlan 削除 110

B. SwitchC(config)#インターフェイス ポート チャネル 1

SwitchC(config-if)#switchport トランク許可 VLAN 追加 210,310
C. SwitchC(config)#vtp プルーニング VLAN 110
D. SwitchC(config)#vtp プルーニング
Answer: A (メーッセージを残す**)**

最新問題**: 135**
展示を参照してください。

```
Router#show ip ospf interface
GigabitEthernet0/1.40 is up, line protocol is up
  Internet Address 10.3.5.254/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
        0         1       no        no        Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 10.3.5.254
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 172.16.30.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
        0         1       no        no        Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.11.29/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 172.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID  Cost  Disabled  Shutdown  Topology Name
        0         1       no        no        Base
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
  Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
```

ネットワーク エンジニアは OSPF を構成し、ルーターの構成を確認します。OSPF 隣接関係を確立できるインターフェイスはどれですか?
A. ギガビットイーサネット 0/1 およびギガビットイーサネット 0/1.40
B. GigabitEthernet0/1のみ

C. GigabttEthernet0/0 のみ
D. ギガビット イーサネット 0/0 およびギガビット イーサネット 0/1
Answer: C (メーッセージを残す**)**

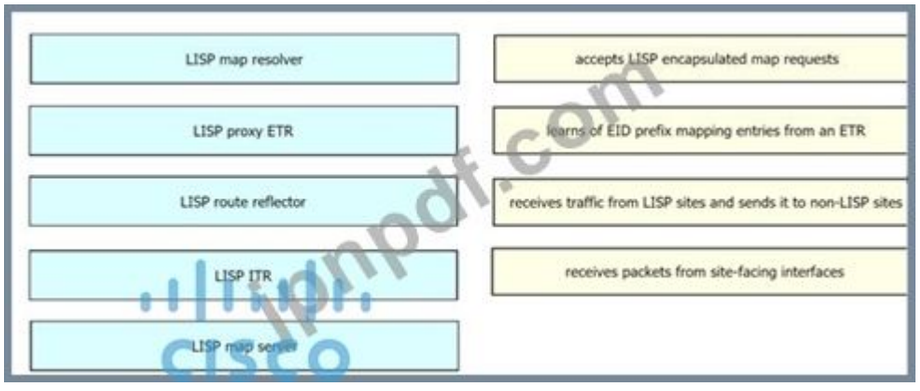
最新問題**: 136**
左側の脅威防御ソリューションを右側の説明にドラッグ アンド ドロップします。

Answer:

最新問題**: 137**
展示を参照してください。すべてのリンクが機能していると仮定すると、PC1 は DSW1 に到達するためにどのパスをたどりますか?
A. PC1 は ALSW1 から DSW1 に移動します

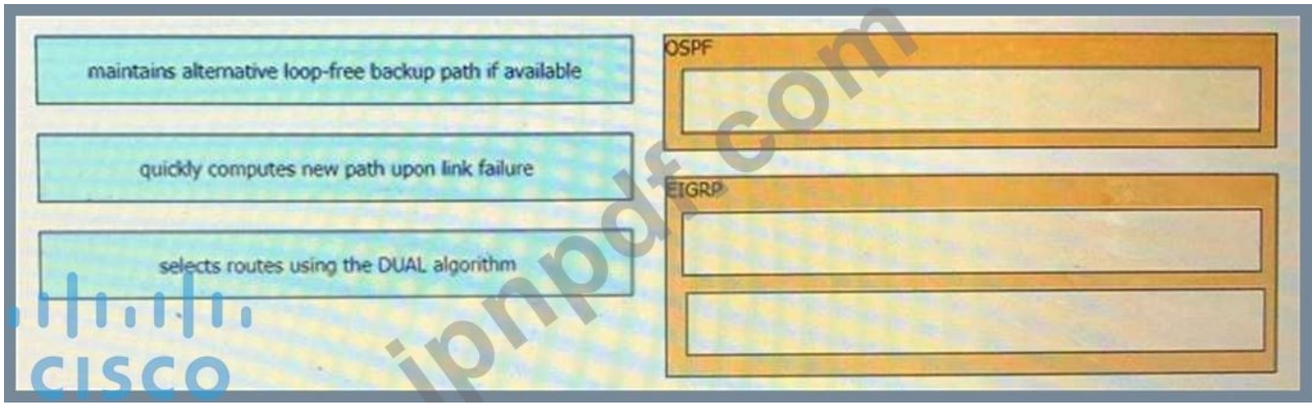
B. PC1 は、ALSW1、DSW2、ALSW2、DSW1 と進みます。
C. PC1 は ALSW1、DSW2、コア、DSW1 に移行します。
D. PC1 は ALSW1、DSW2、DSW1 と進みます。
Answer: D (メーッセージを残す)
説明
上記のトポロジでは、DSW2 の優先順位が最も低い 24576 であることがわかります。つまり、DSW2 は VLAN 10 のルート ブリッジであるため、この VLAN のすべてのトラフィックは必ずこれを通過する必要があります。すべての DSW2 ポートがフォワーディング状態である必要があります。と：
+ DSW1 と ALSW1 の間の直接リンクは STP によってブロックされます。+ DSW1 と ALSW2 間の直接リンクも STP によってブロックされます。
したがって、PC1 は次のパスを経由する必要があります: PC1 -> ALSW1 -> DSW2 -> DSW1。

最新問題: **138**
LISP コンポーネントを左側から、右側で実行される機能にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。



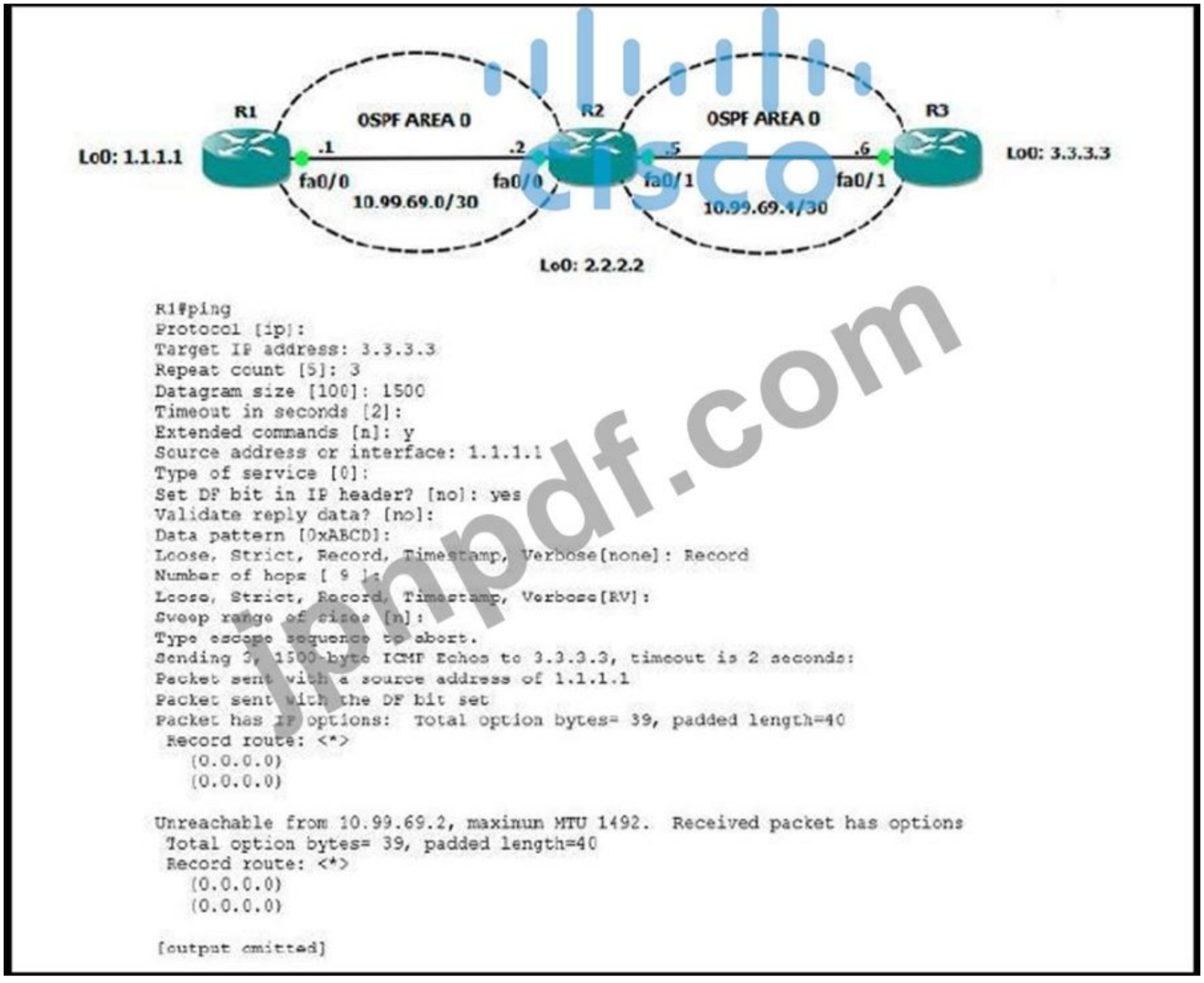
Answer:

最新問題: **139**
特性を左側から右側に説明されているルーティング プロトコルにドラッグ アンド ドロップします。



Answer:

最新問題**: 140**
展示を参照してください。



R1 は R3 fa0/1 インターフェイスに ping を送信できます。拡張 ping が失敗するのはなぜですか?

A. コマンドが受け付ける最大パケットサイズは 1476 バイトです。

B. R3 には 10.99.69.0/30 への戻りルートがありません。

C. R2 と R3 には OSPF 隣接関係がありません。

D. DF ビットがセットされました

Answer: D (メーッセージを残す)

説明

DF ビットが設定されている場合、ルーターはパケットを断片化できません。以下の出力から、1500 バイトで ping を送信したのに対し、R2 の最大 MTU は 1492 バイトであることがわかります。したがって、これらの ICMP パケットはドロップされました。

注: 記録オプションでは、パケットが通過するホップ (最大 9 つ) のアドレスが表示されます。

最新問題**: 141**

展示を参照してください。

```
Router#show access-lists
Extended IP access list 100
  10 permit ip 192.168.0.0 0.0.255.255 any
  20 permit ip 172.16.0.0 0.0.15.255 any
```

アクセス リストの機能に影響を与えることなく、インターフェイス GigabitEthernet0/1 の 172.20.10.1 からのすべてのトラフィックを許可し、ログに記録するには、どのコマンド セットを追加する必要がありますか?

A. オプション A
B. オプション D
C. オプション C
D. オプション B
Answer: B (メーッセージを残す**)**

最新問題**: 142**
同じ LAN セグメント内に複数のルーターがある場合、どのルーターが IGMP クエリアに選出されますか?
A. 稼働時間が最も短いルーター
B. IP アドレスが最も小さいルーター
C. IP アドレスが最も大きいルーター
D. 稼働時間が最も長いルーター
Answer: B (メーッセージを残す**)**
クエリ メッセージは、次のように IGMP クエリアを選択するために使用されます。1. IGMPv2 デバイスが起動すると、各デバイスは、メッセージの送信元 IP アドレス フィールドにインターフェイス アドレスを指定して、一般的なクエリ メッセージを全システム グループ アドレス 224.0.0.1 にマルチキャストします。。2. IGMPv2 デバイスが一般クエリ メッセージを受信すると、デバイスはメッセージ内の送信元 IP アドレスと自身のインターフェイス アドレスを比較します。サブネット上で最も小さい IP アドレスを持つデバイスが IGMP クエリアとして選出されます。3. すべてのデバイス (クエリアを除く) がクエリ タイマーを開始します。クエリ タイマーは、IGMP クエリアから一般的なクエリ メッセージを受信するたびにリセットされます。クエリ タイマーが期限切れになると、IGMP クエリアがダウンしたとみなされ、新しい IGMP クエリアを選出するために選出プロセスが再度実行されます。

最新問題: **143**
クライアント デバイスは、アトリウム内の異なるフロアにあるアクセス ポイント間をローミングします。アクセス ポイントは同じコントローラに接続され、ローカル モードで設定されます。アクセス ポイントは異なる AP グループに属し、異なる IP アドレスを持ちますが、グループ内のクライアント VLAN は同じです。どのタイプのローミングが発生しますか?
A. コントローラ間
B. サブネット間
C. VLAN内
D. コントローラ内
Answer: (解答を表示する**)**
説明
モビリティ (ローミング) とは、無線 LAN クライアントが、あるアクセス ポイントから別のアクセス ポイントへの接続をシームレスに安全に、かつ遅延を最小限に抑えて維持できる機能のことです。クライアント ローミングの一般的なタイプは次の 3 つです。
コントローラ内ローミング: 各コントローラは、同じコントローラによって管理されるアクセス ポイント間での同じコントローラ クライアント ローミングをサポートします。このローミングは、セッションが維持されている間クライアントに対して透過的であり、クライアントは同じ DHCP 割り当てまたはクライアント割り当ての IP アドレスを使用し続けます。
コントローラ間ローミング：複数のコントローラの導入では、同じモビリティ グループおよび同じサブネット上のコントローラによって管理されるアクセス ポイント間でのクライアント ローミングがサポートされます。このローミングは、セッションが維持され、コントローラ間のトンネルにより、セッションがアクティブである限り、同じ DHCP またはクライアントによって割り当てられた IP アドレスを使用し続けることができるため、クライアントに対して透過的です。
サブネット間ローミング：複数のコントローラの導入では、異なるサブネット上の同じモビリティ グループ内のコントローラによって管理されるアクセス ポイント間でのクライアント ローミングがサポートされます。このローミングは、セッションが維持され、コントローラ間のトンネルにより、セッションがアクティブである限り、クライアントは同じ DHCP 割り当てまたはクライアント割り当ての IP アドレスを使用し続けることができるため、クライアントに対して透過的です。

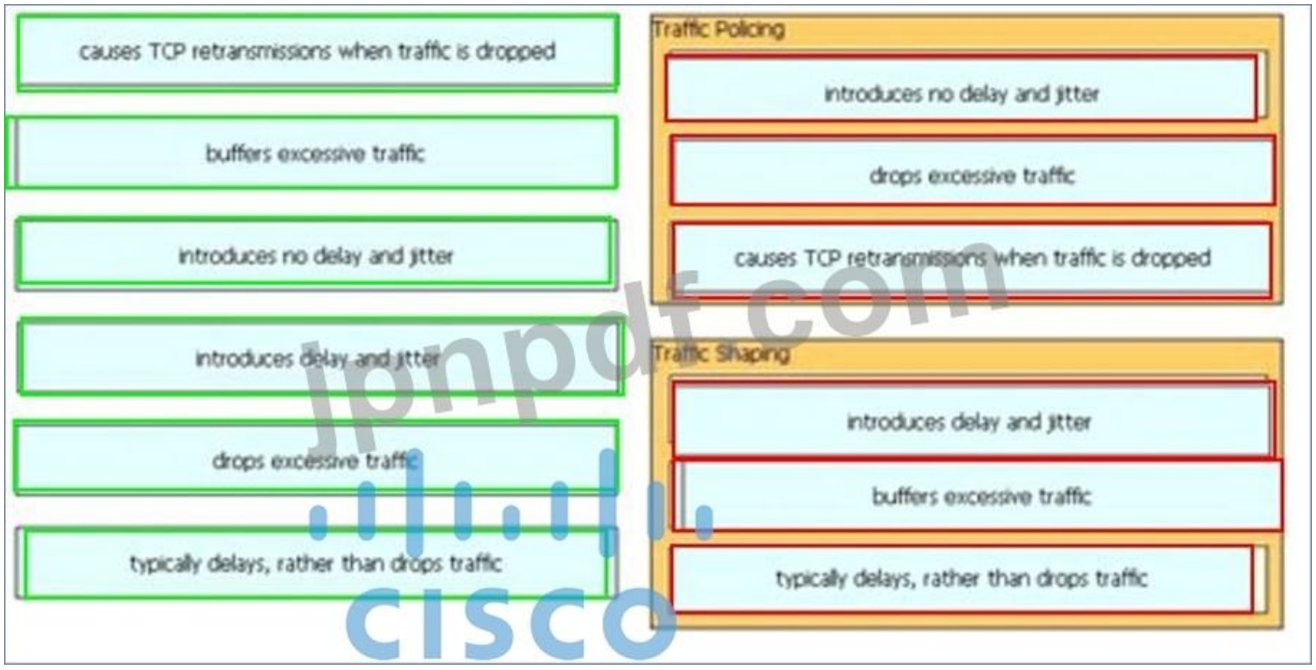
最新問題: **144**
Cisco DNA Center テレメトリ機能によってどのような利点が得られますか?
A. ネットワークデバイスのインベントリを作成します。
B. ユーザーエクスペリエンスを向上させます
C. 導入ネットワーク構成を支援します。
D. ネットワークセキュリティを向上させます。
Answer: A (メーッセージを残す**)**

最新問題: **145**
GRE/IP トンネルでの断片化のリスクを最小限に抑えるために調整されている TCP 設定はどれですか?

A. MTU
B. ウィンドウサイズ
C. MRU
D. MSS
Answer: D (メーッセージを残す)
説明
TCP 最大セグメント サイズ (TCP MSS) は、ホストが単一の TCP/IP データグラムで受け入れることができるデータの最大量を定義します。この TCP/IP データグラムは IP 層で断片化されている可能性があります。MSS 値は、TCP SYN セグメントでのみ TCP ヘッダー オプションとして送信されます。TCP 接続の各側は、MSS 値を相手側に報告します。一般に信じられていることに反して、MSS 値はホスト間でネゴシエートされません。送信ホストは、単一の TCP セグメント内のデータのサイズを、受信ホストによって報告された MSS 以下の値に制限する必要があります。
TCP MSS は、TCP 接続の 2 つのエンドポイントでの断片化を処理しますが、これら 2 つのエンドポイント間の中間に小さい MTU リンクがある場合は処理しません。
PMTUD は、エンドポイント間のパスの断片化を回避するために開発されました。これは、パケットの送信元から宛先までのパスに沿った最低 MTU を動的に決定するために使用されます。
参照: http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulationgre/25885-pmtud-ipfrag.html (このリンクには、TCP MSS が IP フラグメンテーションを回避する方法の例がいくつかありますが、長すぎるため、読みたい場合はこのリンクにアクセスしてください) 注: IP フラグメンテーションには、データグラムを多数のデータグラムに分割することが含まれます。後で再び組み立てることができる部品。

最新問題: **146**
左側の説明を右側の QoS コンポーネントにドラッグ アンド ドロップします。


Answer:



最新問題**: 147**
クライアント デバイスは、アトリウム内の異なるフロアにあるアクセス ポイント間をローミングします。アクセス ポイントは、ローカル モードで同じコントローラおよび設定に接続されました。アクセス ポイントの IP アドレスは異なりますが、グループ内のクライアント VLAN は同じです。どのような種類のローミングが発生しますか?
A. コントローラ間
B. サブネット間
C. VLAN内
D. コントローラ内
Answer: B (メーッセージを残す**)**
説明
モビリティ (ローミング) とは、無線 LAN クライアントが、あるアクセス ポイントから別のアクセス ポイントへの接続をシームレスに安全に、かつ遅延を最小限に抑えて維持できる機能のことです。クライアント ローミングの一般的なタイプは次の 3 つです。
コントローラ内ローミング: 各コントローラは、同じコントローラによって管理されるアクセス ポイント間での同じコントローラ クライアント ローミングをサポートします。このローミングは、セッションが維持されている間クライアントに対して透過的であり、クライアントは同じ DHCP 割り当てまたはクライアント割り当ての IP アドレスを使用し続けます。
コントローラ間ローミング：複数のコントローラの導入では、同じモビリティ グループおよび同じサブネット上のコントローラによって管理されるアクセス ポイント間でのクライアント ローミングがサポートされます。このローミングは、セッションが維持され、コントローラ間のトンネルにより、セッションがアクティブである限り、同じ DHCP またはクライアントによって割り当てられた IP アドレスを使用し続けることができるため、クライアントに対して透過的です。

サブネット間ローミング：複数のコントローラの導入では、異なるサブネット上の同じモビリティ グループ内のコントローラによって管理されるアクセス ポイント間でのクライアント ローミングがサポートされます。このローミングは、セッションが維持され、コントローラ間のトンネルにより、セッションがアクティブである限り、クライアントは同じ DHCP 割り当てまたはクライアント割り当ての IP アドレスを使用し続けることができるため、クライアントに対して透過的です。

最新問題: **148**
返された構成を JSON 形式のファイルとして保存するには、どの Python コード スニペットをスクリプトに追加する必要がありますか?

```
import json
import requests

Creds = ("admin", "S!416190947$Ptx")
Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

BaseURL = https://cpe/restconf/data"
URL = BaseURL + "Cisco-IOS-XE-native/interface/GigabitEthernet"

Response = requests.get(URL, auth = Creds, headers = Headers, verify = False)
```

A)

```
with open("ifaces.json", "w") as OutFile:
  OutFile.write(Response)
```

B)

```
with open("ifaces.json", "w") as OutFile:
  OutFile.write(Response.text)
```

C)

```
with open("ifaces.json", "w") as OutFile:
  JSONResponse = json.loads(Response.text)
  OutFile.write(JSONResponse)
```

D)

```
with open("ifaces.json", "w") as OutFile:
 OutFile.write(Response.json())
```

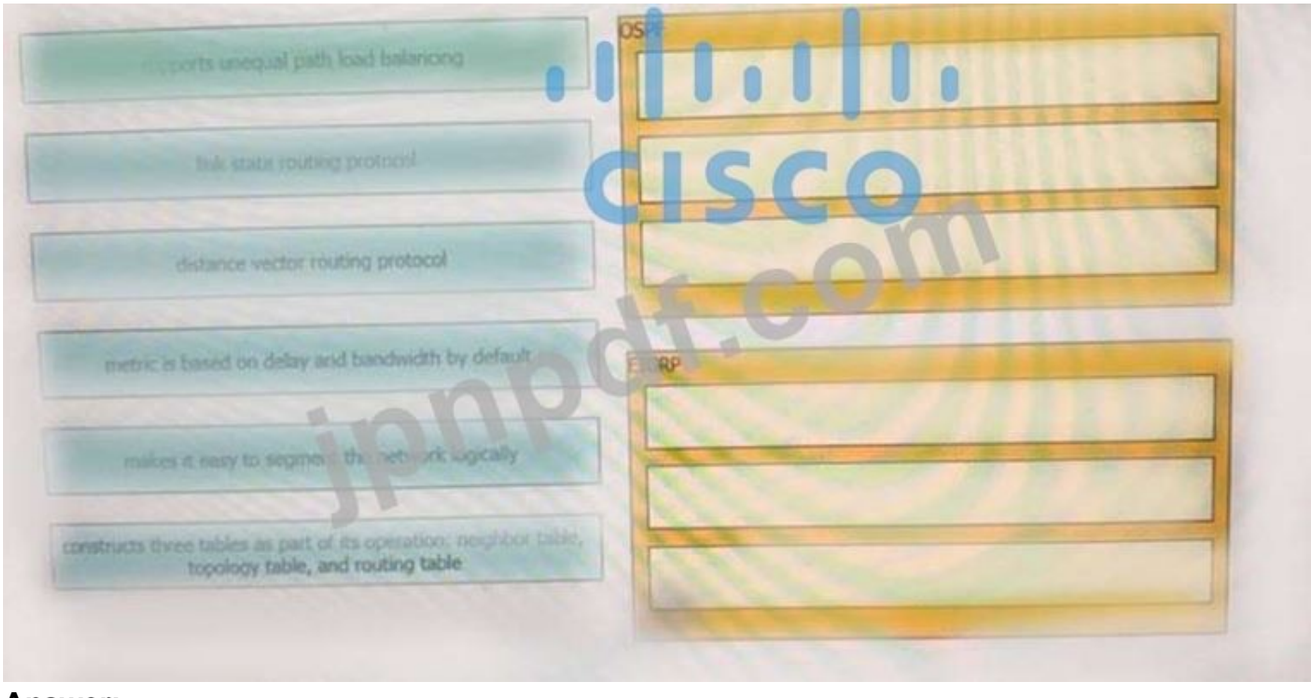
A. オプション C
B. オプション D
C. オプション A
D. オプション B
Answer: A (メーッセージを残す**)**

最新問題: **149**
Cisco TrustSec は、ネットワーク全体にスケーラブルで安全な通信を提供するためにどの機能を使用しますか?
A. スイッチ上の各ポートに割り当てられたセキュリティ グループ タグ ACL
B. ネットワーク上の各ポートに割り当てられたセキュリティグループのタグ番号
C. スイッチ上の各ユーザーに割り当てられたセキュリティ グループ タグ番号
D. ネットワーク上の各ルーターに割り当てられたセキュリティ グループ タグ ACL
Answer: B (メーッセージを残す**)**
Cisco TrustSec はタグを使用して論理グループの特権を表します。このタグはセキュリティ グループ タグ（SGT）と呼ばれ、アクセス ポリシーで使用されます。SGT は理解されており、Cisco スイッチ、ルータ、および

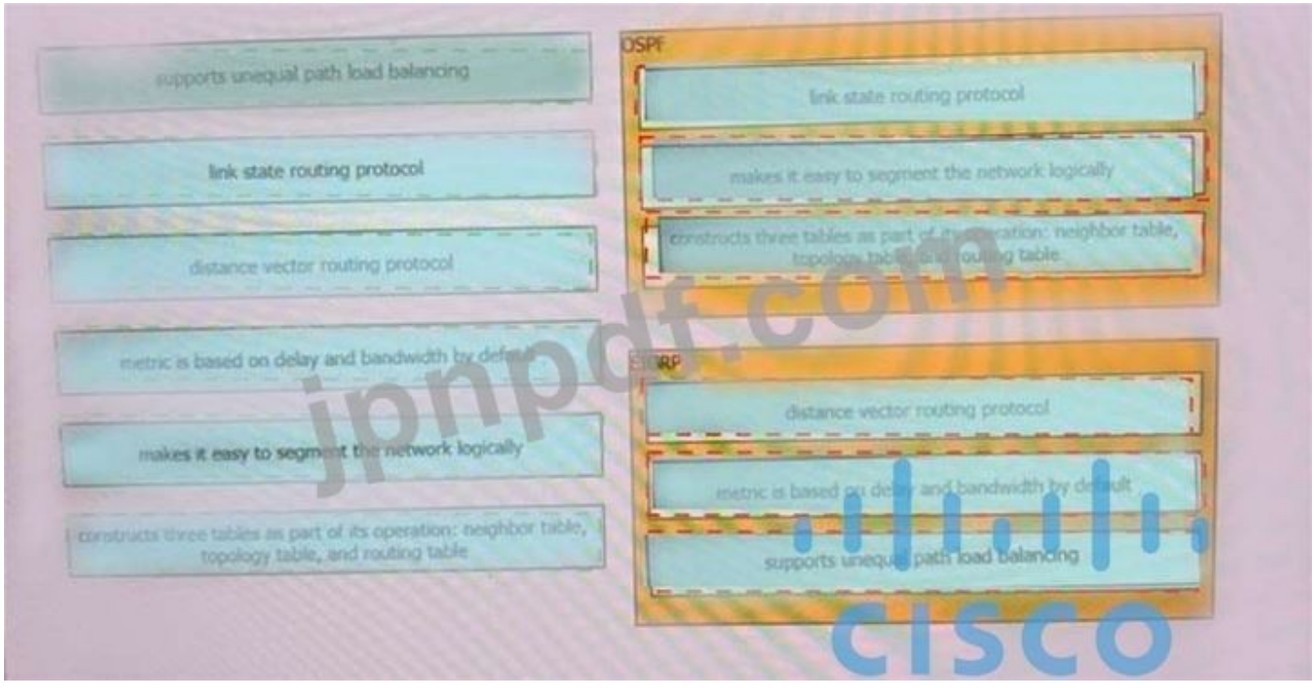
ファイアウォールによってトラフィックを強制するために使用されます。Cisco TrustSec は、分類、伝播、施行の 3 つのフェーズで定義されます。
ユーザーとデバイスがネットワークに接続すると、ネットワークは特定のセキュリティ グループを割り当てます。このプロセスは分類と呼ばれます。分類は、認証の結果に基づいて行うか、SGT を IP、VLAN、またはポート プロファイルに関連付けることによって行うことができます (-> 「スイッチ上の各ポートに割り当てられたセキュリティ グループ タグ ACL」と答え、「割り当てられたセキュリティ グループ タグ番号」と答えます) 「スイッチ上の各ユーザーに割り当てられている」は「スイッチ上に割り当てられている」だけなので正しくありません。「ネットワーク上の各ルーターに割り当てられているセキュリティ グループ タグ ACL」も「各ルーターに割り当てられている」と書かれているので正しくありません。")。

最新問題: **150**
CEF とプロセス スイッチングの違いは何ですか?
A. CEF よりもプロセスの切り替えが高速です。
B. CEF は、プロセス スイッチングが管理するには複雑すぎるパケットを処理します。
C. CEF はプロセス スイッチングよりも CPU を集中的に使用します。
D. CEF は FIB と隣接テーブルを使用して転送を決定しますが、プロセス スイッチングは各パケットをパントします。
Answer: (解答を表示する**)**

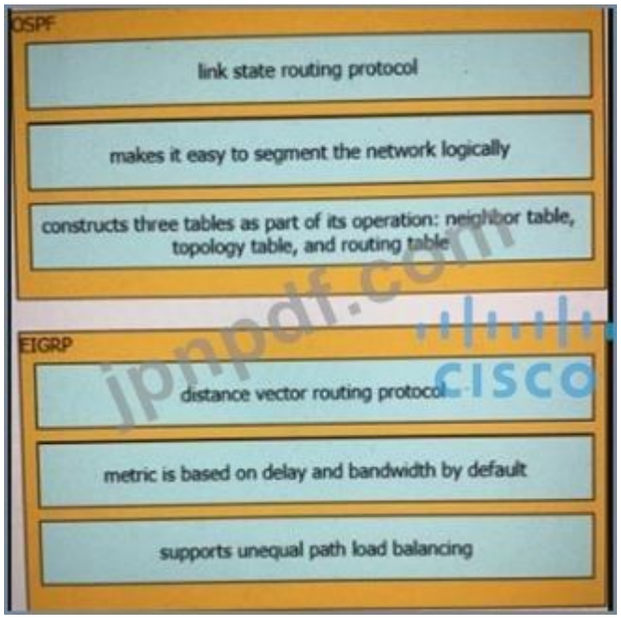
最新問題: **151**
説明を左側から、右側に説明されているルーティング プロトコルにドラッグ ドロップします。



Answer:

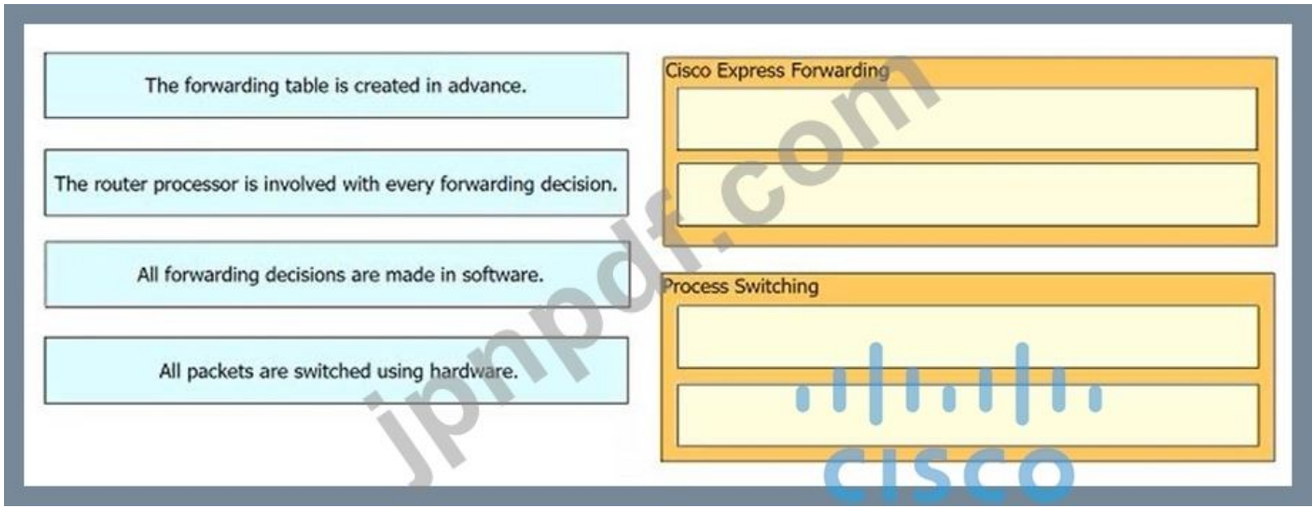


説明

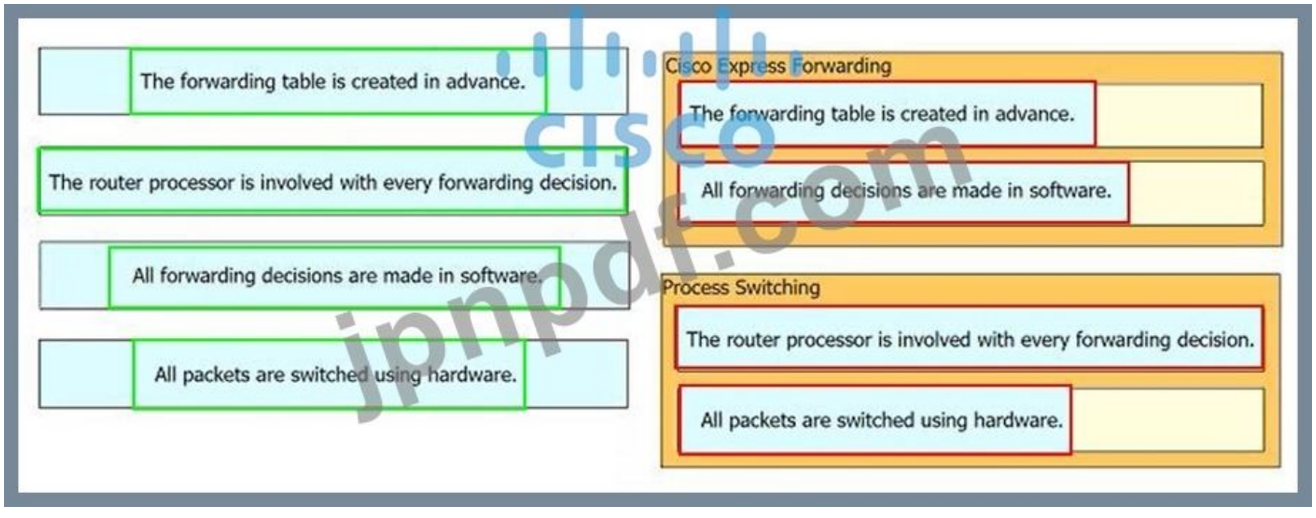


最新問題**: 152**

特性を左側から右側に説明されている切り替えメカニズムにドラッグ アンド ドロップします。



Answer:



最新問題**: 153**

私の出品物を参照してください。

```
switch > enable
switch # configure terminal
switch(config)# interface GigabitEthernet 1/10
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 10,20,30
switch(config-if)# exit
switch (config)# monitor session 1 type erspan-source
switch(config-mon-erspan-src)# description source1
switch(config-mon-erspan-src)# source vlan 10
switch(config-mon-erspan-src)# source vlan 20
switch(config-mon-erspan-src)# filter vlan 30
switch(config-mon-erspan-src)# destination
switch(config-mon-erspan-src-dst)# erspan-id 100
switch(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
switch(config-mon-erspan-src-dst)# ip prec 5
switch(config-mon-erspan-src-dst)# ip ttl 32
switch(config-mon-erspan-src-dst)# mtu 1500
switch(config-mon-erspan-src-dst)# ip address 10.10.0.1
switch(config-mon-erspan-src-dst)# vrf 1
switch(config-mon-erspan-src-dst)# no shutdown
switch(config-mon-erspan-src-dst)# end
```

エンジニアはトランクを設定し、VLAN を監視するための ESPAN セッションの設定に進みます10。20. および 30. この構成を完了するにはどのコマンドを追加する必要がありますか?

A. デバイス(config.mon.erspan.stc)# フィルタなし VLAN 30

B. Devic(config.mon.erspan.src-dst)# no vrf 1
C. デバイス(config.mon-erspan.Src-dst)# mtu 1460
D. Devic(config.mon.erspan.src-dst)# erspan id 6
Answer: (解答を表示する**)**

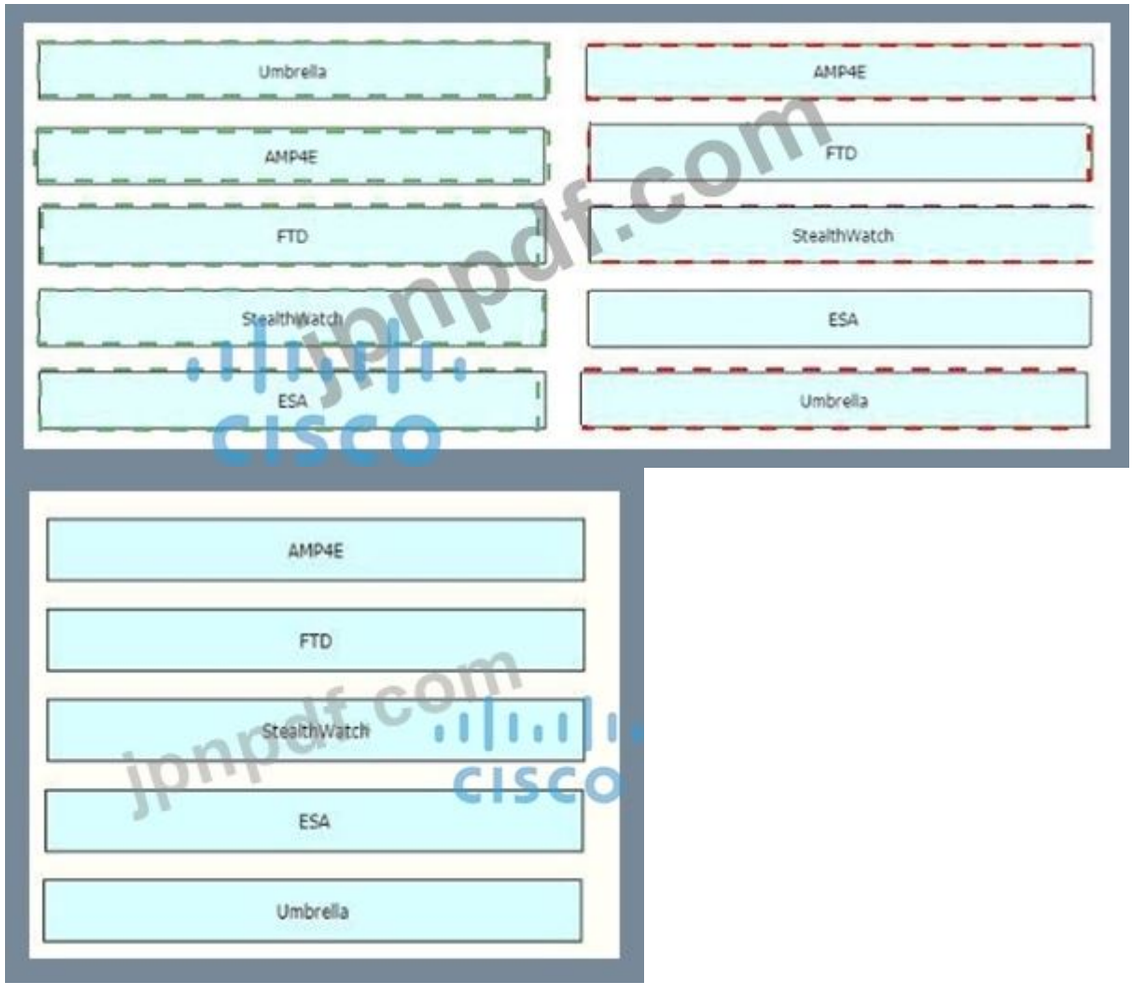
最新問題**: 154**
展示を参照してください。

Python コード出力ではどの HTTP JSON 応答が得られますか?
A. KeyError 'kickstart_ver_str'
B. 名前エラー: 名前 「json」が定義されていません
C. 7.61
D. 7.0(3)I7(4)
Answer: D (メッセージを残す**)**

最新問題**: 155**
VXLAN の VTEP の機能はどのアクションですか?
A. IPv4 から IPv6 VXLAN へのトラフィックのトンネリング
B. VXLAN イーサネット フレームのカプセル化とカプセル化解除
C. ローカル VXLAN イーサネット セグメントでの暗号化通信を許可します。
D. IPv6 から IPv4 VXLAN へのトラフィックのトンネリング
Answer: B (メッセージを残す**)**

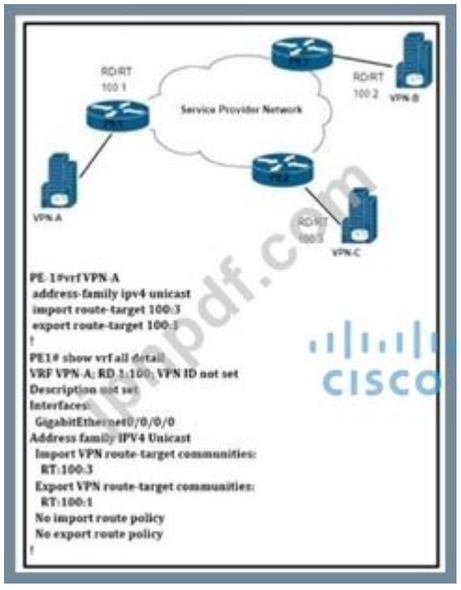
最新問題**: 156**
左側の脅威防御ソリューションを右側の説明にドラッグ アンド ドロップします。

Answer:



最新問題: **157**

展示を参照してください。



VPN-A はポイントツーポイント トラフィックを VPN-B に送信し、VPN-C からのみトラフィックを受信します
VPN-B はポイントツーポイント トラフィックを VPN-C に送信し、VPN-A からのみトラフィックを受信します
どの構成が適用されますか?

A)

PE-2

```
vrf VPN-B
 address-family ipv4 unicast
 import route-target 100:1
 export route-target 100:2
```

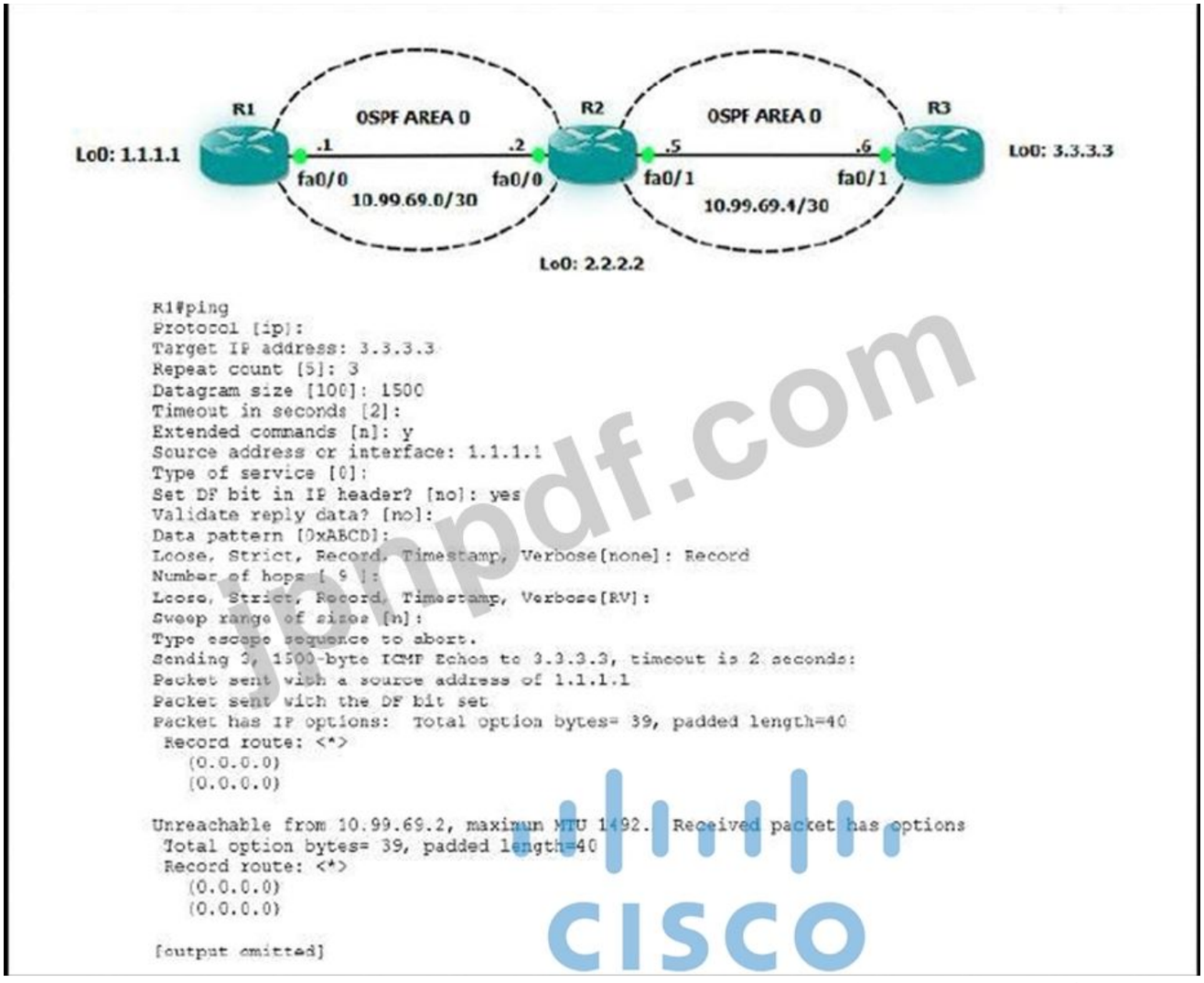
B)

PE-3

```
vrf VPN-B
 address-family ipv4 unicast
 import route-target 100:1
 export route-target 100:2
```

A. オプション A
B. オプション B
Answer: (解答を表示する**)**

最新問題**: 158**
展示を参照してください。



R1 は R3 fa0/1 インターフェイスに ping を送信できます。拡張 ping が失敗するのはなぜですか?

A. コマンドが受け付ける最大パケットサイズは 1476 バイトです。

B. R3 には 10.99.69.0/30 への戻りルートがありません。

C. R2 と R3 には OSPF 隣接関係がありません。

D. DF ビットがセットされました

Answer: D (メーッセージを残す)

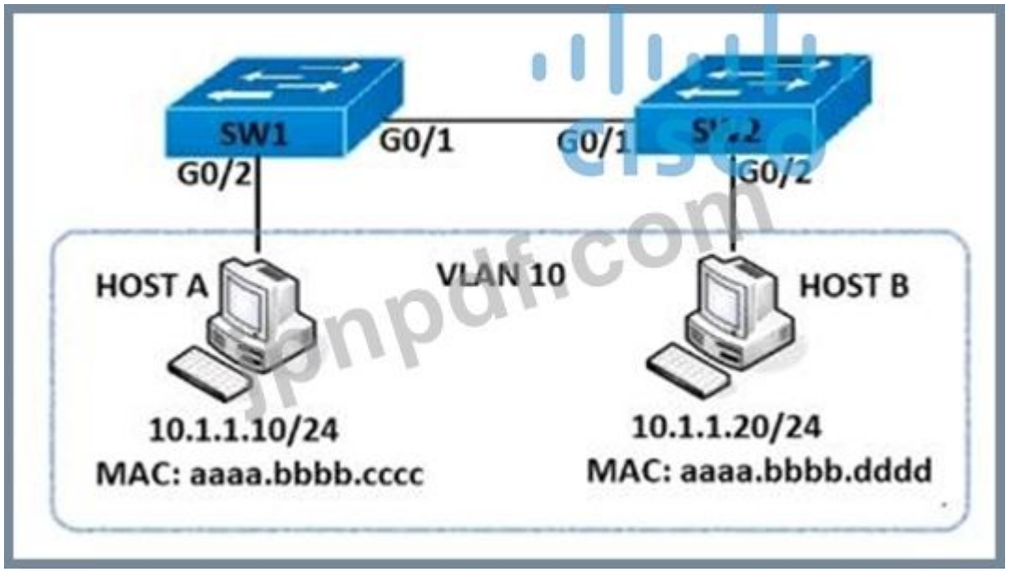
説明

DF ビットが設定されている場合、ルーターはパケットを断片化できません。以下の出力から、1500 バイトで ping を送信したのに対し、R2 の最大 MTU は 1492 バイトであることがわかります。したがって、これらの ICMP パケットはドロップされました。

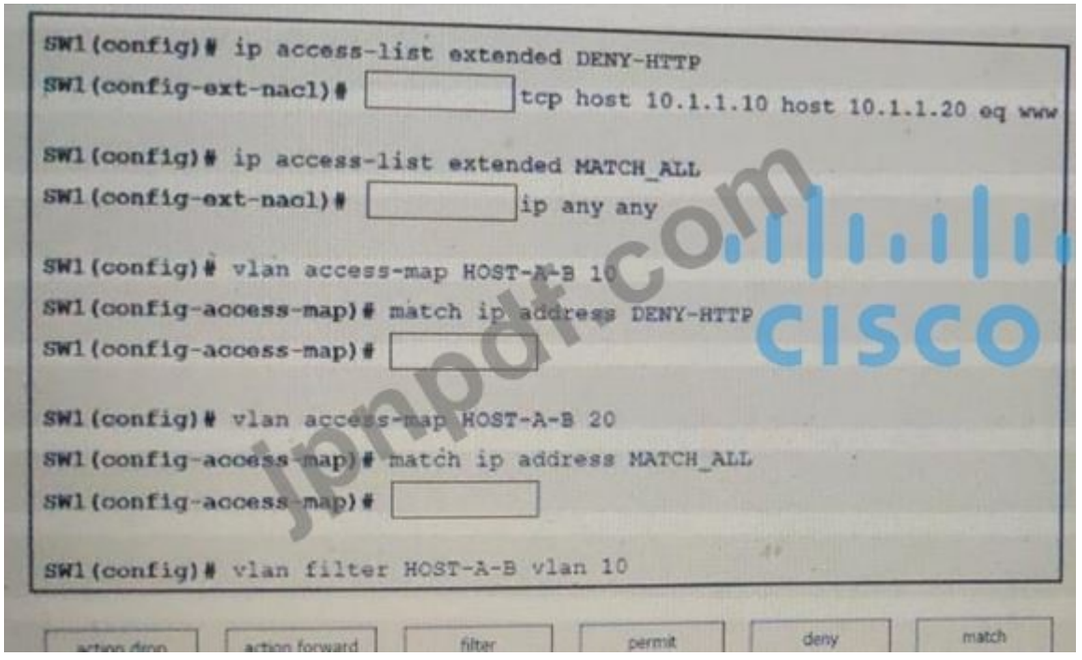
注: 記録オプションでは、パケットが通過するホップ (最大 9 つ) のアドレスが表示されます。

最新問題**: 159**

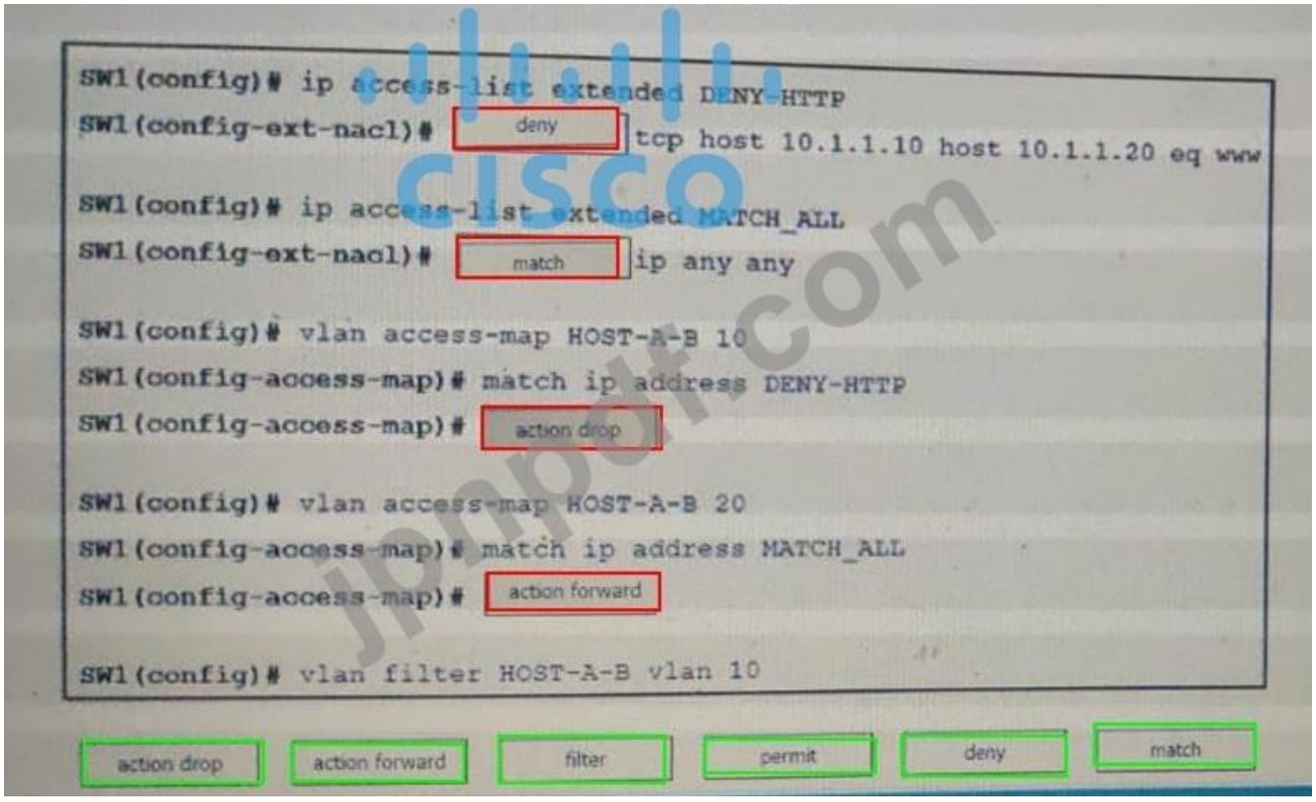
展示を参照してください。



これらの結果を達成するには、エンジニアはホスト A からホスト B への HTTP トラフィックを拒否し、ホスト間の他のすべての通信を許可し、コマンドを構成にドラッグ アンド ドロップする必要があります。一部のコマンドは複数回使用できます。すべてのコマンドが使用されるわけではありません。

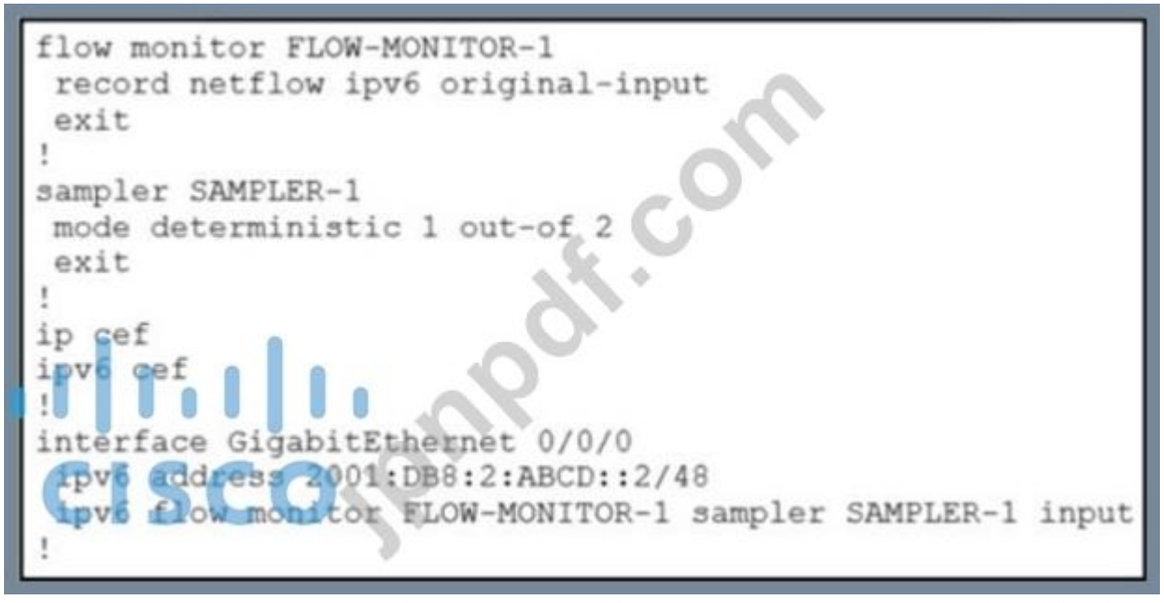


Answer:



最新問題: **160**

展示を参照してください。



ルータの Flexible NetFlow 設定にサンプラー機能を導入すると、どのような影響がありますか?

A. コレクターへの NetFlow アップデートの送信頻度が 50% 低下します。

B. IPv4 パケットは 2 つおきに検査のためにコレクターに転送されます。

C. CPU とメモリの使用率は、完全な NetFlow に必要な量と比較して削減されます。

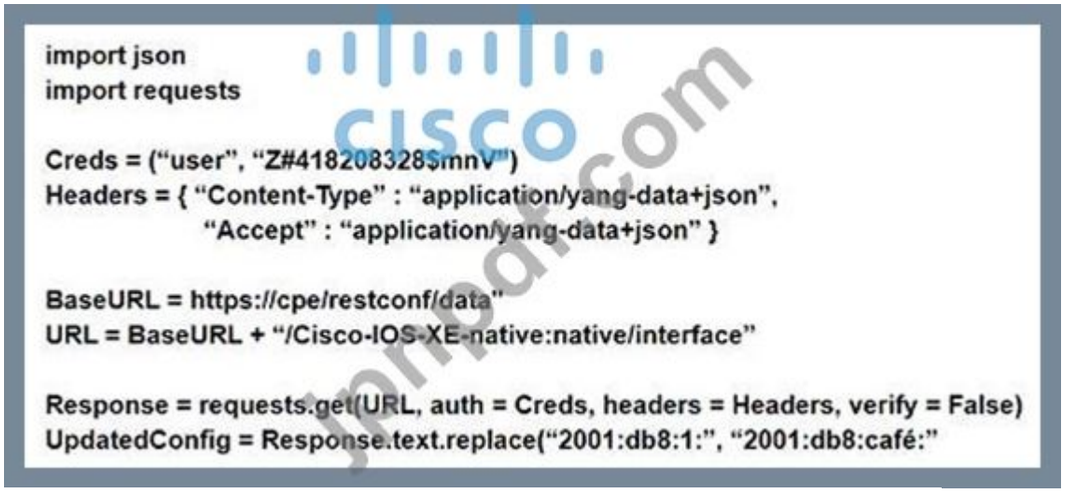
D. サンプリングデータの解像度は上がりますが、ルータの性能もより高くなります。

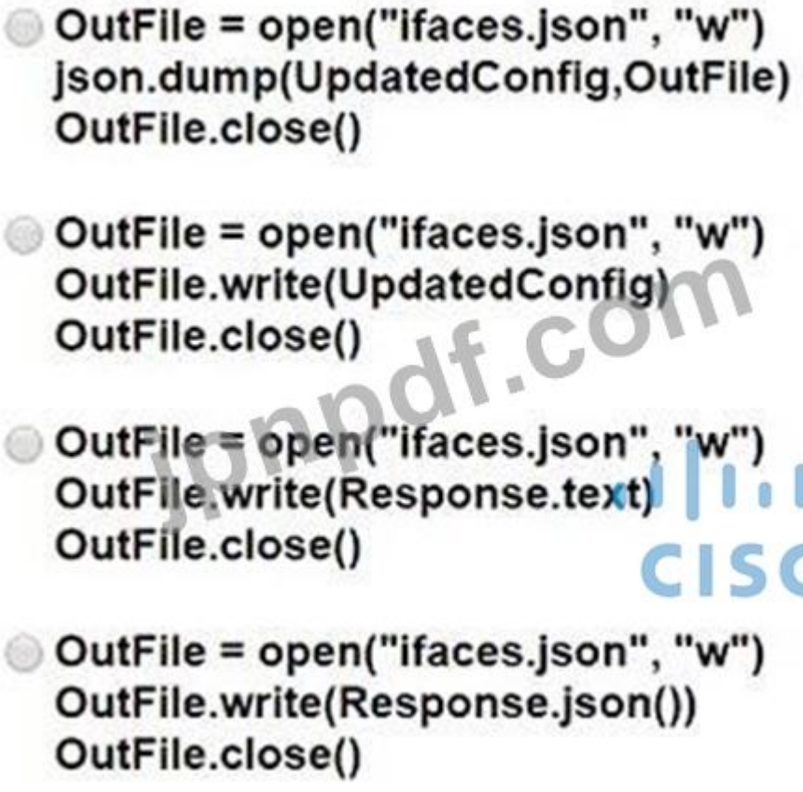
Answer: A (メーッセージを残す**)**

参考: https://github.com/aabc/pkt-netflow

最新問題: **161**

変更されたインターフェイス構成をローカルの JSON 形式のファイルに保存するには、どの Python コード スニペットをスクリプトに追加する必要がありますか?





A. オプション D
B. オプション B
C. オプション A
D. オプション C
Answer: B (メーッセージを残す**)**

最新問題: **162**

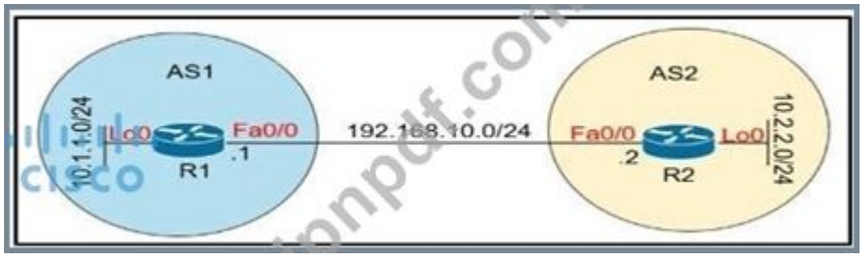
エンジニアが Cisco DMA Center の API に対してコードを実行すると、プラットフォームは次の出力を返します。応答は何を示していますか?

A. 認証資格情報が正しくありません
B. URL 文字列が正しくありません。
C. Cisco DNA Center API ポートが正しくありません
D. HTTPメソッドが間違っています
Answer: (解答を表示する**)**
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

最新問題**: 163**
私の出品物を参照してください。

「この Python スクリプトは何をしますか?」の展示を参照してください。
A. ライト データベースから特定の IP アドレスのユーザー名を読み取ります。
B. 特定の IP アドレスの RAOIUS ユーザー名を入力します。
C. 特定の IP アドレスの TACACS* ユーザー名を入力します。
D. 特定の IP アドレスのユーザー名をライト データベースに書き込みます
Answer: D (メーッセージを残す**)**

最新問題**: 164**
展示を参照してください。



これら 2 つの直接接続された隣接ルータ間に EBGP ネイバーシップを確立し、BGP を介して 2 つのルータのループバック ネットワークを交換する構成はどれですか?

A)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

B)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

C)

```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.10.2 remote-as 2
R1(config-router)#network 10.0.0.0 mask 255.0.0.0

R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.10.1 remote-as 1
R2(config-router)#network 10.0.0.0 mask 255.0.0.0
```

D)

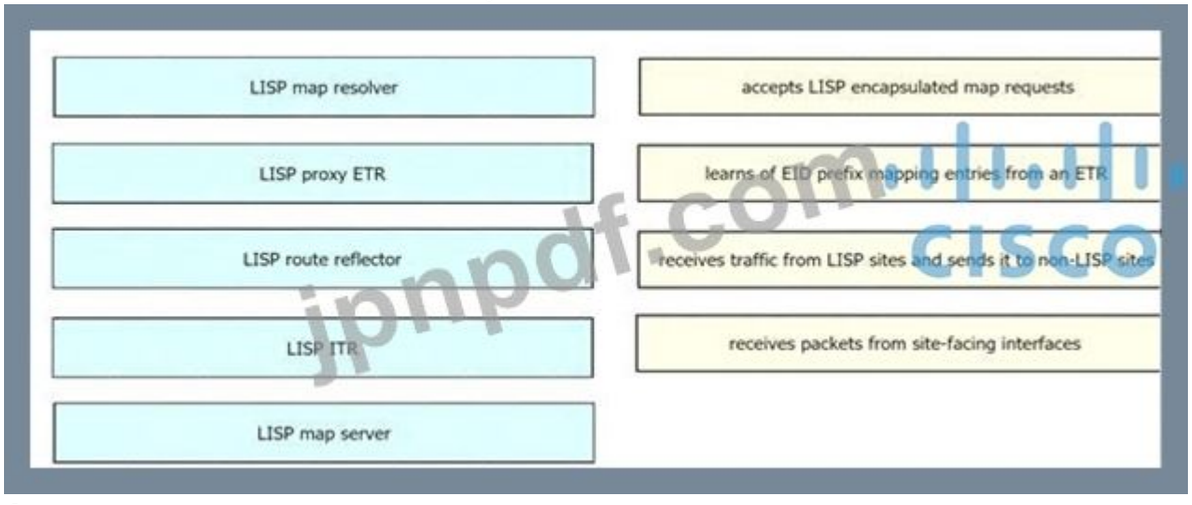
```
R1(config)#router bgp 1
R1(config-router)#neighbor 10.2.2.2 remote-as 2
R1(config-router)#neighbor 10.2.2.2 update-source lo0
R1(config-router)#network 10.1.1.0 mask 255.255.255.0

R2(config)#router bgp 2
R2(config-router)#neighbor 10.1.1.1 remote-as 1
R2(config-router)#neighbor 10.1.1.1 update-source lo0
R2(config-router)#network 10.2.2.0 mask 255.255.255.0
```

A. オプション A

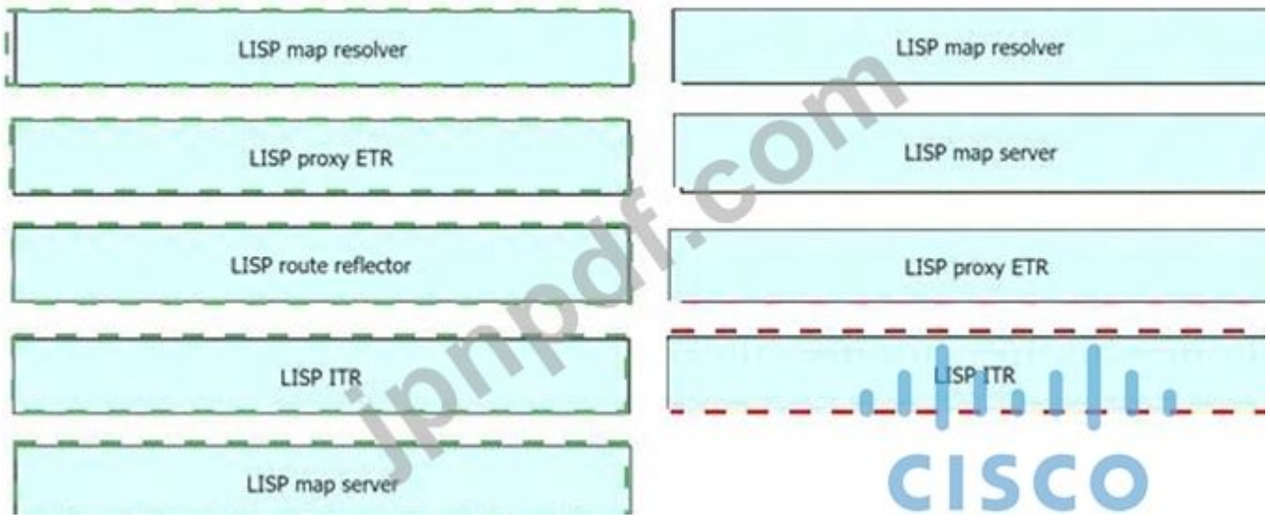
B. オプション B
C. オプション C
D. オプション D
Answer: A (メーッセージを残す**)**
説明
BGP では、「network」コマンドで正しいネットワークとサブネット マスクをアドバタイズする必要があります (この場合、R1 ではネットワーク 10.1.1.0/24、R2 ではネットワーク 10.2.2.0/24)。BGP はルーティング アドバタイズメントにおいて非常に厳密です。つまり、BGP はルーティング テーブルに正確に存在するネットワークのみをアドバタイズします。この場合、「network xx0.0 Mask 255.255.0.0」というコマンドを入力すると、「ネットワーク x.0.0.0 マスク 255.0.0.0」または「ネットワーク xxxx マスク 255.255.255.255」の場合、BGP は何もアドバタイズしません。
直接リンクを介して eBGP 隣接関係を確立するのは簡単です。ただし、ループバック インターフェイス経由で eBGP ネイバーシップを確立する場合に何が必要かを見てみましょう。次の 2 つのコマンドが必要になります。
+ R1 上のコマンド「neighbor 10.1.1.1 ebgp-multihop 2」および「neighbor 10.2.2.2 ebgpmultihop」
R1 では 2"。このコマンドは TTL 値を 2 に増やし、BGP アップデートが 2 ホップ離れた BGP ネイバーに到達できるようにします。
+ 'R1 (config) #router bgp 1 と応答します
R1 (構成ルーター) #neighbor 192.168.10.2 リモートとして 2
R1 (config-router) #network 10.1.1.0 マスク 255.255.255.0
R2 (構成) #router bgp 2
R2 (構成ルーター) #neighbor 192.168.10.1 リモートとして 1
R2 (config-router) #network 10.2.2.0 マスク 255.255.255.0
ワイヤレスの簡単な概要
Cisco アクセス ポイント（AP）は、自律モードまたは軽量モードの 2 つのモードのいずれかで動作できます。
+ 自律: 自給自足かつスタンドアロン。小規模な無線ネットワークに使用されます。
+ 軽量: Cisco 軽量 AP (LAP) が機能するには、ワイヤレス LAN コントローラ (WLC) に接続する必要があります。
LAP と WLC は、CAPWAP トンネルの論理ペアを介して相互に通信します。
- Control and Provisioning for Wireless Access Point（CAPWAP）は、AP と WLC 間のセットアップ、認証、および操作のための制御メッセージングの IETF 標準です。CAPWAP は、次の違いを除いて LWAPP に似ています。
+CAPWAP は、認証と暗号化に Datagram Transport Layer Security (DTLS) を使用して、AP とコントローラ間のトラフィックを保護します。LWAPP は AES を使用します。
+ CAPWAP には、動的な最大伝送単位 (MTU) 検出メカニズムがあります。
+ CAPWAP は、UDP ポート 5246 (制御メッセージ) および 5247 (データ メッセージ) で実行されます。LAP は、次の 6 つの異なるモードのいずれかで動作します。
+ ローカル モード (デフォルト モード): ノイズ フロアと干渉を測定し、未使用のチャネルで 180 秒ごとに侵入検知 (IDS) イベントをスキャンします。
+ FlexConnect (以前はハイブリッド リモート エッジ AP (H-REAP) として知られていました) モード: データ トラフィックをローカルでスイッチし、コントローラに戻さないようにします。FlexConnect AP は、WLC（ロー

カル スイッチ)に接続されていない場合でも、スタンドアロン クライアント認証を実行し、VLAN トラフィックをローカルで切り替えることができます。FlexConnect AP は、ユーザ ワイヤレス データと制御トラフィックの両方を集中型 WLC（中央スイッチ)にトンネリング (CAPWAP 経由)することもできます。
+ モニター モード: クライアントとインフラストラクチャ間のデータ トラフィックは処理されません。位置情報サービス (LBS)、不正 AP 検出、IDS のセンサーのように機能します。
+ 不正検出モード: 不正 AP を監視します。データはまったく扱いません。
+ スニファー モード: スニファーとして実行し、特定のチャネル上のすべてのパケットをキャプチャしてリモート マシンに転送します。リモート マシンでは、プロトコル分析ツール (Wireshark、Airopeek など) を使用してパケットを確認し、問題を診断できます。トラブルシューティングの目的でのみ使用されます。
+ ブリッジ モード: WLAN と有線インフラストラクチャをブリッジします。
Mobility Express は、実際の WLAN コントローラの代わりにアクセス ポイント (AP) をコントローラとして使用する機能です。ただし、このソリューションは、専用 WLC に投資したくない小規模から中規模、またはマルチサイトのブランチ ロケーションにのみ適しています。Mobility Express WLC は最大 100 の Aps をサポートできます

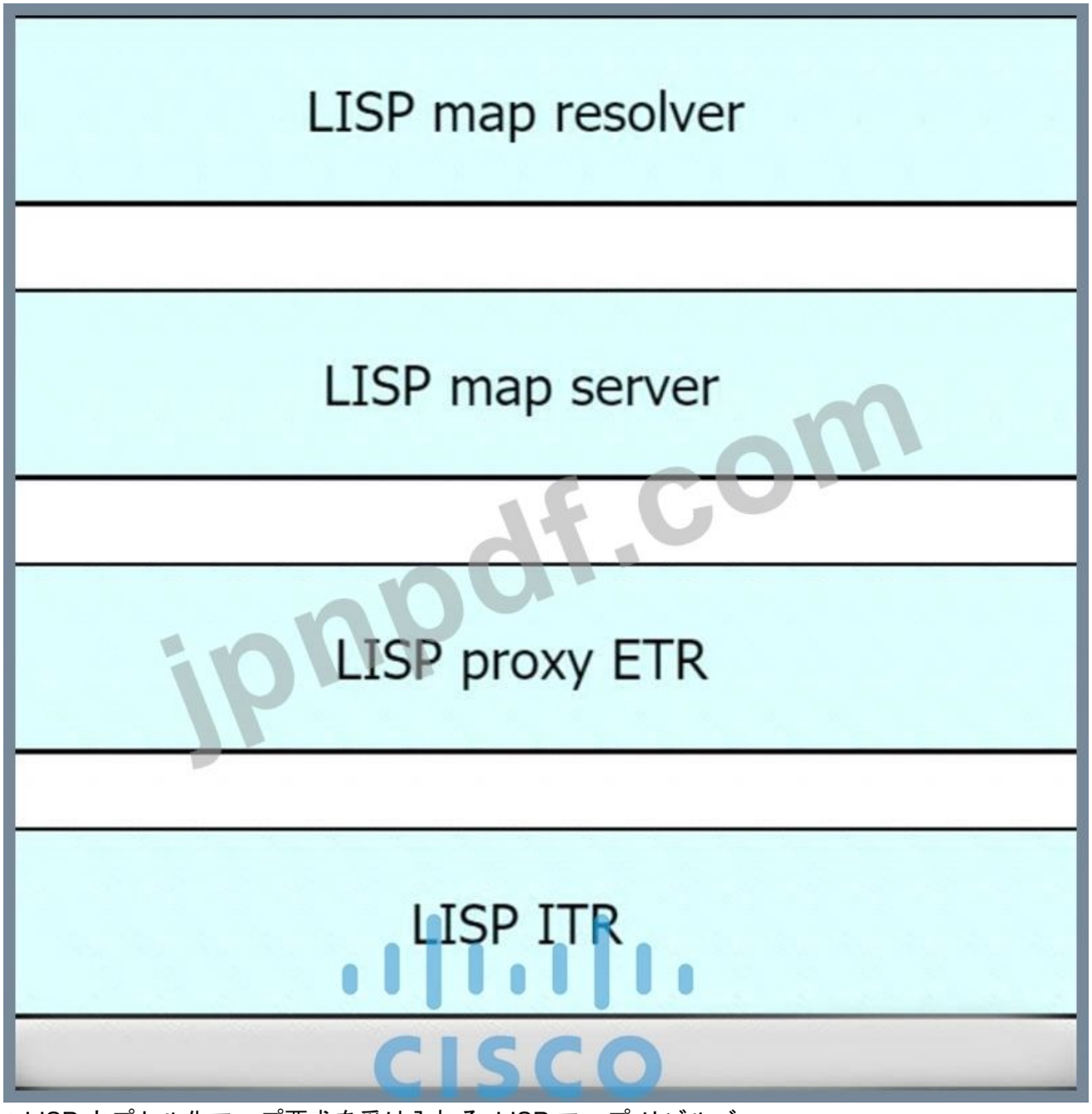
最新問題**: 165**
LISP コンポーネントを左側から、右側で実行される機能にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。



Answer:


LISP map resolver
LISP proxy ETR
LISP route reflector
LISP ITR
LISP map server
LISP map resolver
LISP map server
LISP proxy ETR
LISP ITR
CISCO

説明



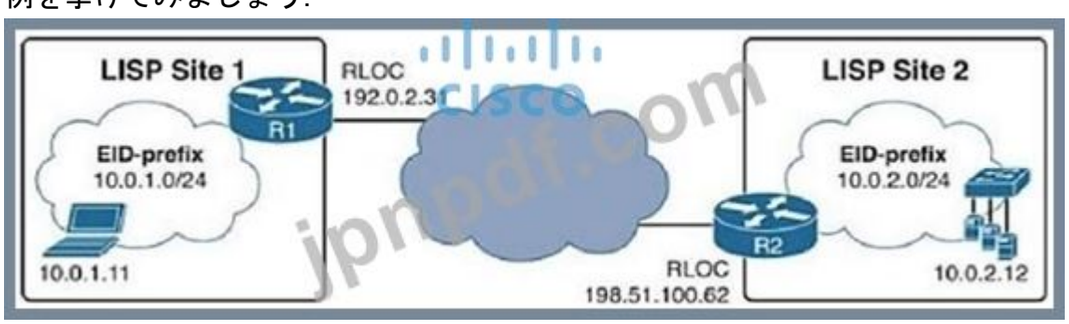
+ LISP カプセル化マップ要求を受け入れる: LISP マップ リゾルバー
+ ETR から EID プレフィックス マッピング エントリを学習します: LISP マップ サーバー
+ LISP サイトからトラフィックを受信し、非 LISP サイトに送信します: LISP プロキシ ETR
+ サイト側インターフェイスからパケットを受信: LISP ITR

説明

ITR は、宛先 EID を宛先 RLOC にマッピングし、ITR RLOC の送信元 IP アドレスと出力トンネル ルーター (ETR) の RLOC の宛先 IP アドレスを含む追加のヘッダーで元のパケットをカプセル化する機能です。
カプセル化後、元のパケットは LISP パケットになります。
ETR は、LISP でカプセル化されたパケットを受信し、カプセル化を解除して、ローカル EID に転送する機能です。この機能には EID から RLOC へのマッピングも必要なため、『マップ サーバー』の IP アドレスと認証用のキー (パスワード) を指定する必要があります。

LISP プロキシ ETR (PETR) は、非 LISP サイトに代わって ETR 機能を実装します。PETR は通常、LISP サイトが非 LISP サイトにトラフィックを送信する必要があるが、ルーティング可能な EID をパケット ソースとして受け入れないサービス プロバイダーを介して LISP サイトが接続されている場合に使用されます。PETR は ETR と同様に機能しますが、EID が非 LISP サイトの宛先にトラフィックを送信する点が異なります。
Map Server (MS) は、認証キーの登録と EID から RLOC へのマッピングを処理します。ETR は、設定されているすべての Map Server に定期的な Map-Register メッセージを送信します。
マップ リゾルバ (MR): LISP カプセル化マップ リクエスト (通常は ITR から) を受け入れる LISP コンポーネントで、宛先 IP アドレスが EID 名前空間の一部であるかどうかを迅速に判断します。

最新問題: **166**
EIGRP OTP 実装における LISP カプセル化に関する記述のうち、正しいものはどれですか?
A. LISP はネクストホップを学習します
B. OTP は LISP カプセル化を使用してネイバーからルートを取得します
C. OTP は動的マルチポイント トンネリングに LISP カプセル化を使用します。
D. OTP は LISP コントロール プレーンを維持します
Answer: (解答を表示する**)**
説明
EIGRP オーバー ザ トップ ソリューションを使用すると、異なる EIGRP サイト間の接続を確保できます。この機能は、コントロール プレーンで EIGRP を使用し、データ プレーンで Locator ID Separation Protocol (LISP) カプセル化を使用して、基盤となる WAN アーキテクチャ全体でトラフィックをルーティングします。EIGRP は、ネットワーク内のカスタマー エッジ (CE) デバイス間でルートを分散するために使用され、WAN アーキテクチャ全体で転送されるトラフィックは LISP でカプセル化されます。
EIGRP OTP はデータ プレーンに LISP のみを使用します。EIGRP は引き続きコントロール プレーンに使用されます。したがって、データとコントロール プレーン トラフィックの両方をカプセル化する必要があるため、OTP が動的マルチポイント トンネリングに LISP カプセル化を使用しているとは言えません。-> 「OTP は動的マルチポイント トンネリングに LISP カプセル化を使用する」という回答は正しくありません。
OTP では、EIGRP は LISP コントロール プレーン プロトコルの代替として機能します (したがって、EIGRP は LISP ではなくネクスト ホップを学習します -> 「LISP がネクスト ホップを学習する」という回答は正しくありません)。ネイティブ LISP マッピング サービスで EID から RLOC への動的なマッピングを行う代わりに、サービス プロバイダー クラウド上で OTP を実行する EIGRP ルーターは、ターゲット セッションを作成し、サービス プロバイダーによって提供された IP アドレスを RLOC として使用し、ルートを EID として交換します。
例を挙げてみましょう:



R1 と R2 が相互に OTP を実行した場合、R1 は EIGRP を通じて R2 からネットワーク 10.0.2.0/24 について学習し、プレフィックス 10.0.2.0/24 を EID プレフィックスとして扱い、アドバタイジング ネクスト ホップ 198.51.100.62 をこの EID プレフィックスの RLOC。同様に、R2 は EIGRP を通じてネットワーク 10.0.1.0/24 について R1 から学習し、プレフィックス 10.0.1.0/24 を EID プレフィックスとして扱い、アドバタイジング ネクスト ホップ 192.0.2.31 をこの EID プレフィックスの RLOC として取得します。両方のルータで、この情報は LISP マッピング テーブルにデータを入力するために使用されます。
10.0.1.0/24 から 10.0.2.0/24 へのパケットが R1 に到着すると、R1 は通常の LISP と同じように LISP マッピング テーブルを使用して、パケットが LISP カプセル化され、198.51.100.62 に向かってトンネリングされる必要があることを検出します。逆に。LISP データ プレーンは OTP で再利用され、変更されません。ただし、ネイティブ LISP のマッピングおよび解決メカニズムは EIGRP に置き換えられます。
参照: CCIE ルーティングおよびスイッチング V5.0 公式認定ガイド、第 1 巻、第 5 版

最新問題: **167**
BFD に関する次の記述のうち、正しいものはどれですか? （選択肢を2つ選択してください。）
A. BFD は、ルーティング プロトコルに依存せずに、障害が発生したピアをバイパスできます。
B. BFD は OSPF、EIGRP、BGP、および IS-IS によってサポートされます。
C. BFD はルーティング プロトコル タイマーよりも多くの CPU リソースを消費します。
D. BFD は物理インターフェイスでのみサポートされます。
E. BFD は 1 秒未満でリンク障害を検出します。
F. BFD は、インターフェイスごとにルーティング プロトコルごとに 1 つのセッションを作成します。
Answer: B,E (メーッセージを残す**)**

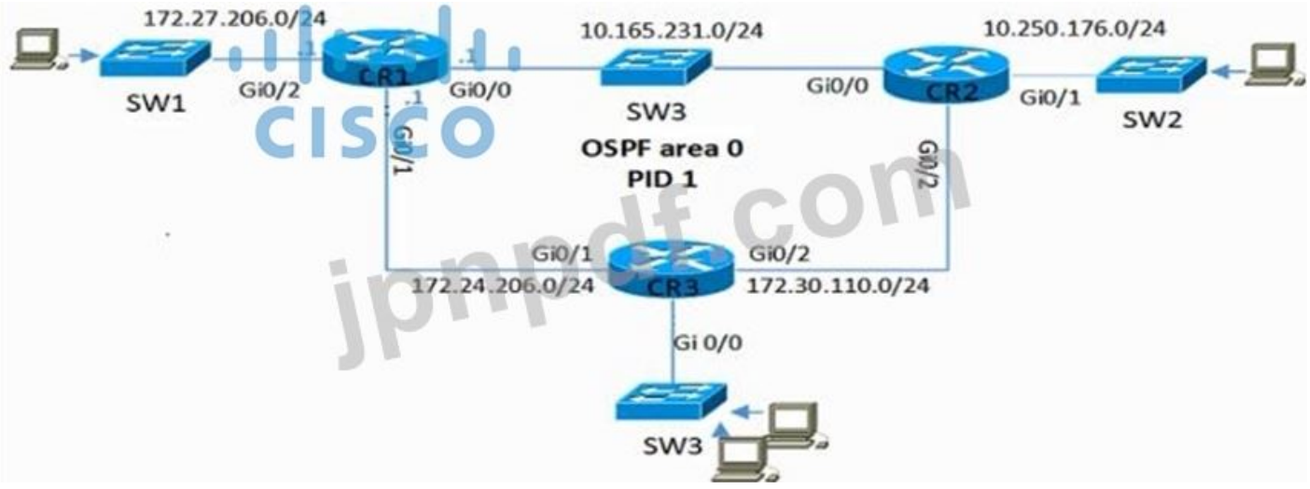
最新問題: **168**
展示を参照してください。

IP SLA はルーターで設定されます。エンジニアは、IP SLA に問題がある場合にインターフェイスをシャットダウンし、再度起動するように EEM アプレットを設定する必要があります。
エンジニアはどの構成を使用する必要がありますか?
A. イベント マネージャ アプレット EEM_IP_SLA
イベントトラック10の状態がダウンしています
B. イベント マネージャ アプレット EEM_IP_SLA
イベント トラック 10 の状態が到達不能です
C. イベント マネージャ アプレット EEM_IP_SLA
イベント sla 10 状態に到達できません
D. イベント マネージャ アプレット EEM_IP_SLA
イベント sla 10 状態ダウン
Answer: (解答を表示する**)**
-ip sla 10 は、3 秒ごとに IP 192.168.10.20 に ping を実行し、接続がまだ確立されていることを確認します。この IP SLA に問題がある場合は、-event track 10 state down コマンドを使用して EEM アプレットを設定できます。

最新問題**: 169**
エンジニアはルータ上に新しいループバック インターフェイスを設定し、そのインターフェイスを OSPF で fa4 としてアドバタイズする必要があります。このタスクを実行できるコマンド セットはどれですか?
A.
```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf 100 area 0
```
B.
```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network point-to-point
R2(config-if)# ip ospf 100 area 0
```
C.
```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network point-to-multipoint
R2(config-if)# router ospf 100
R2(config-router)# network 172.22.2.0 0.0.0.255 area 0
```
D.
```
R2(config)# interface Loopback0
R2(config-if)# ip address 172.22.2.1 255.255.255.0
R2(config-if)# ip ospf network broadcast
R2(config-if)# ip ospf 100 area 0
```
Answer: A (メーッセージを残す**)**
ステップ 1.interfaceoopbacknumberグローバル コンフィギュレーション コマンドを使用して、ループバック インターフェイスを作成します。
ステップ 2. 説明を追加します。これはオプションですが、ネットワークを文書化するために必要なコンポーネントです。
ステップ 3. IP アドレスを設定します。
たとえば、次のコマンドは、 この章の前半で示した）に示す R1 ルータのループバック インターフェイスを設定します。
R1# 設定端末
R1(config)# インターフェイス ループバック 0
R1(config-if)# IP アドレス 10.0.0.1 255.255.255.0

R1(config-if)# 終了
R1(構成)#

最新問題: **170**
展示を参照してください。



CR2 と CR3 は OSPF で設定されました。CR1 に適用される場合の構成。CR1 は CR2 および CR3 と OSPF 情報を交換できますが、他のネットワーク デバイスや CR1 に追加された新しいインターフェイスとは交換できませんか?

A)

```
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
passive-interface GigabitEthernet0/2
```

B)

```
router ospf 1
network 10.165.231.0  0.0.0.255 area 0
network 172.27.206.0 0.0.0.255  area 0
network 172.24.206.0  0.0.0.255  area 0
```

C)

```
interface Gi0/2
ip ospf 1 area 0

router ospf 1
passive-interface GigabitEthernet0/2
```

```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 172.16.0.0 0.15.255.255 area 0
passive-interface GigabitEthernet0/2
```

A. オプション B
B. オプション A
C. オプション C

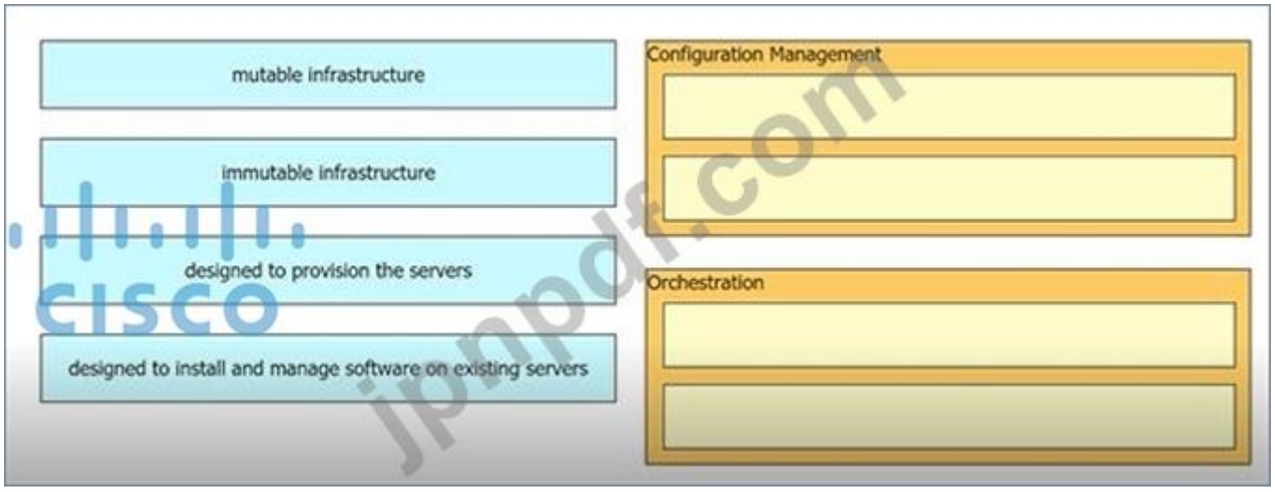
D. オプション D
Answer: (解答を表示する)

最新問題: **171**
有効な JSON ファイルを表示する展示はどれですか?

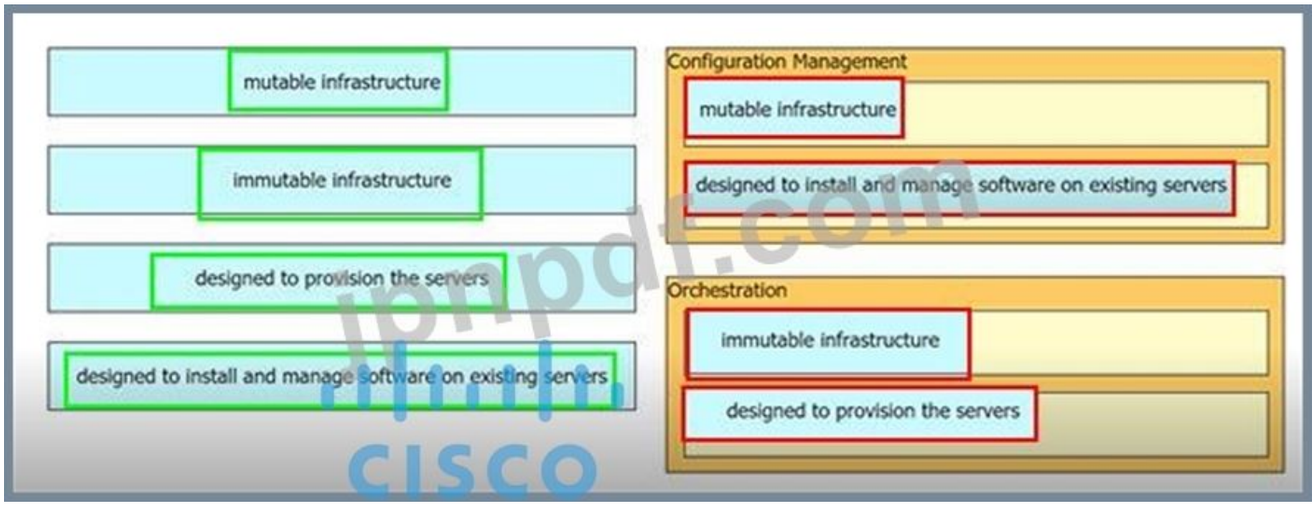
A. オプション B
B. オプション A
C. オプション C
D. オプション D
Answer: (解答を表示する)

最新問題: **172**
ネットワーク管理者が GRE トンネルを設定した後、次のシステム ログ メッセージが表示されます。
%TUN-5-RECURDOWN 再帰的ルーティングによりインターフェイス トンネル 0 が一時的に無効になりました
トンネル 0 が無効になっているのはなぜですか?
A. ダイナミックルーティングが有効になっていないため
B. トンネルの宛先への最適なパスはトンネル自体を通過するためです。
C. ルーターが出力転送インターフェイスを再帰的に識別できないため
D. トンネルがトンネルの宛先に到達できないため
Answer: B (メーッセージを残す)

最新問題: **173**
左側の特性を右側のオーケストレーション ツール分類にドラッグ アンド ドロップします。

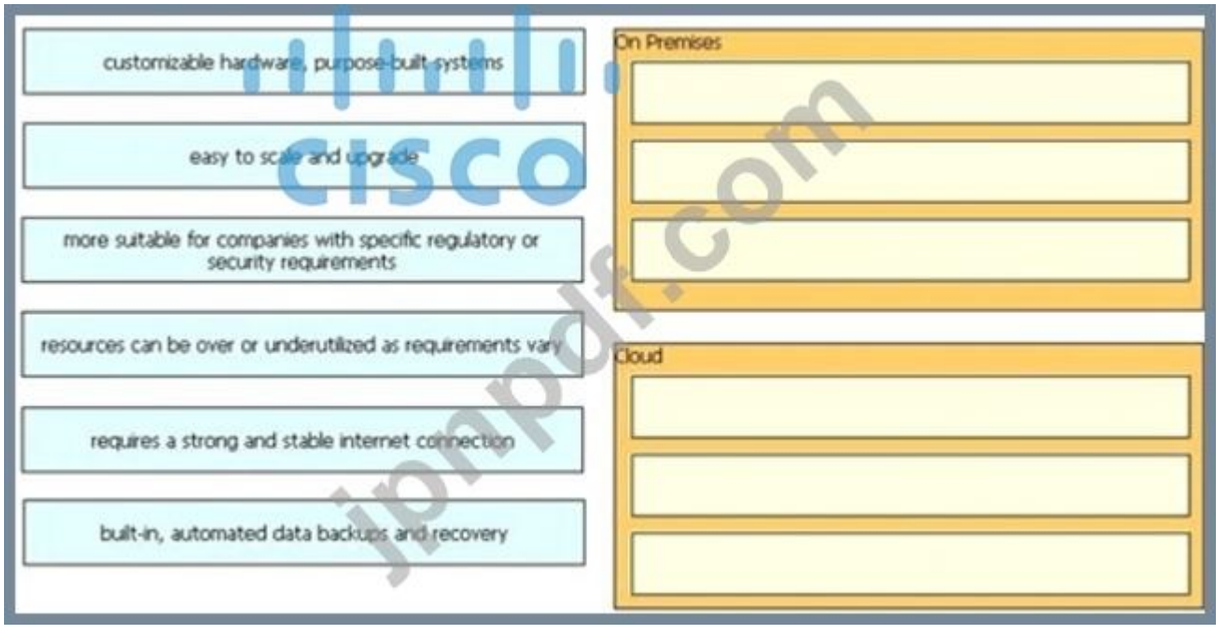


Answer:

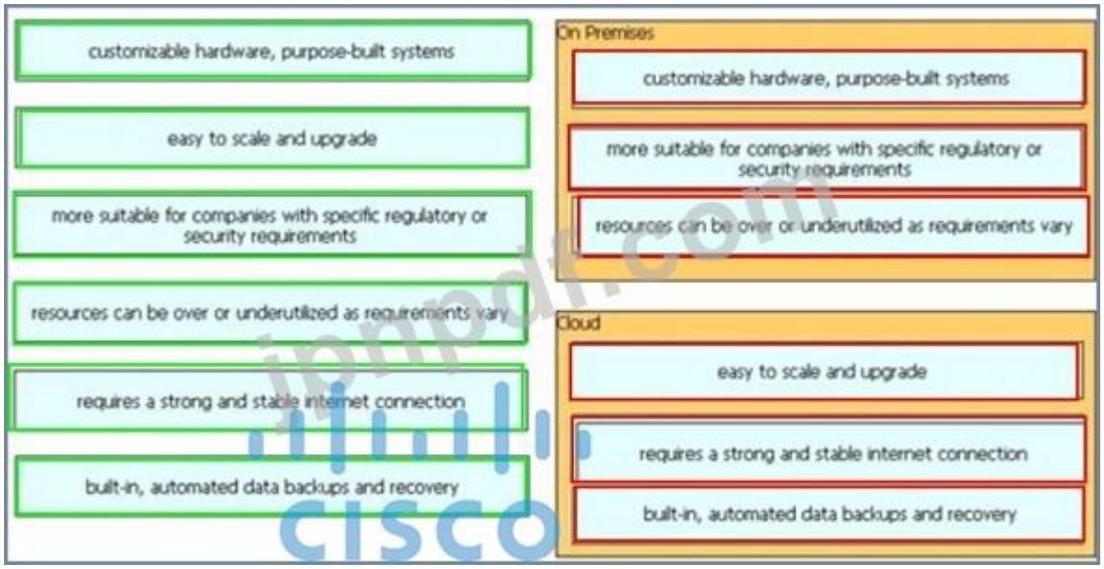


最新問題**: 174**

左側の特性を右側の適切なインフラストラクチャ展開タイプにドラッグ アンド ドロップします。

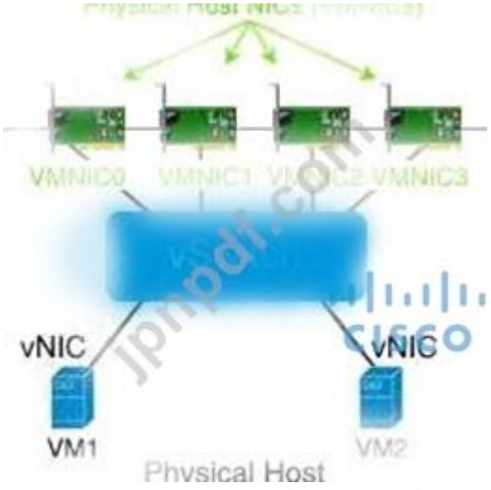


Answer:



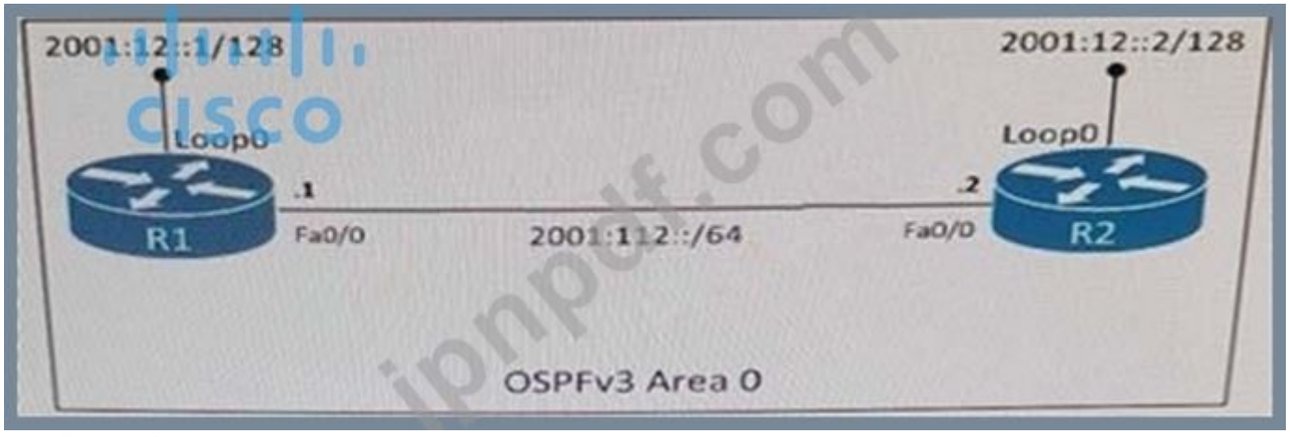
最新問題: **175**
仮想マシン環境でブロードキャスト放射が発生する 2 つの理由は何ですか? (2つお選びください。)
A. vSwitch はブロードキャスト パケットを処理するためにサーバー CPU に割り込む必要があります。
B. 仮想マシン環境では、レイヤー 2 ドメインが大きくなる可能性があります。
C. 仮想マシンは主にブロードキャスト モードを通じて通信します。
D. vSwitch とネットワーク スイッチ間の通信はブロードキャスト ベースです。
E. vSwitch とネットワーク スイッチ間の通信はマルチキャスト ベースです。
Answer: B,C (メーッセージを残す**)**
説明
ブロードキャスト放射とは、コンピュータ ネットワーク上のブロードキャスト トラフィックとマルチキャスト トラフィックの蓄積です。極端な量のブロードキャスト トラフィックはブロードキャスト ストームを構成します。
ブロードキャスト ドメイン内で確認すべきブロードキャスト トラフィックの量は、ブロードキャスト ドメインのサイズに正比例します。したがって、仮想マシン環境のレイヤー 2 ドメインが大きすぎる場合、ブロードキャスト放射が発生する可能性があります -> ブロードキャスト放射を減らすために VLAN を使用する必要があります。
また、仮想マシンがブロードキャスト経由で通信しすぎる場合は、ブロードキャスト
放射線が発生する可能性があります。
ブロードキャスト放射のもう 1 つの理由は、ネットワーク スイッチから物理サーバーまでのトランク (VLAN を拡張するため) を使用することです。
ハイパーバイザーにおける仮想化の構造についての注意:
ハイパーバイザーは、仮想マシン (VM) が同じホスト上の他の VM と通信するために使用する仮想スイッチ (vSwitch) を提供します。vSwitch をホストの物理 NIC に接続して、VM が外部へのレイヤー 2 アクセスを取得できるようにすることもできます。
各 VM には、仮想 NIC (vNIC) が提供され、

仮想スイッチ。複数の vNIC を 1 つの vSwitch に接続できるため、物理ホスト上の VM は、物理スイッチを経由せずにレイヤー 2 で相互に通信できます。



vSwitch はスパニングツリー プロトコルを実行しませんが、vSwitch は実行します。
他のループ防止メカニズムを実装します。たとえば、
1 つの VMNIC から入ったフレームは、VMNIC から出ることはありません。
別の VMNIC カードからの物理ホスト。

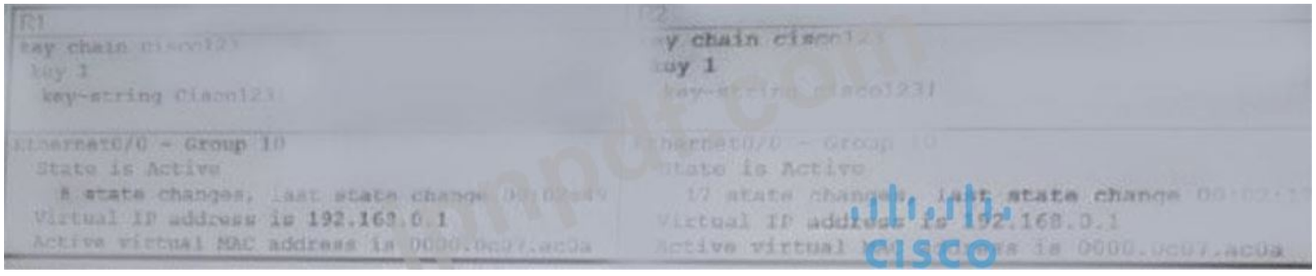
最新問題: **176**
展示を参照してください。R2 のインターフェイス Fa0/0 にデフォルトで適用される IPv6 OSPF ネットワークタイプはどれですか?



A. ブロードキャスト
B. イーサネット
C. マルチポイント
D. ポイントツーポイント
Answer: (解答を表示する**)**
ブロードキャスト ネットワーク タイプは、OSPF 対応イーサネット インターフェイスのデフォルトです (一方、ポイントツーポイントは、HDLC および PPP カプセル化を備えたシリアル インターフェイスのデフォルトの OSPF ネットワーク タイプです)。
参照: https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch08s15.html

最新問題: **177**
スケーラビリティを提供する Cisco NGFW の展開オプションはどれですか?
A. タップ
B. クラスタリング
C. インラインタップ
D. 高可用性
Answer: (解答を表示する**)**
説明
クラスタリングを使用すると、複数の Firepower Threat Defense（FTD）ユニットを 1 つの論理デバイスとしてグループ化できます。
クラスタリングは、Firepower 9300 および Firepower 4100 シリーズの FTD デバイスでのみサポートされます。クラスターは、単一デバイスのすべての利便性 (管理、ネットワークへの統合) を提供しながら、複数のデバイスのスループットと冗長性の向上を実現します。}

最新問題: **178**
展示を参照してください。



エンジニアは、冗長構成で新しいルーターのペアを設置しています。ハードウェア障害が発生した場合にトラフィックが中断されないことを保証するプロトコルはどれですか?
A. HSRPv2
B. GLBP
C. VRRP
D. HSRPv1
Answer: B (メーッセージを残す**)**

最新問題: **179**
展示を参照してください。

管理者は、err-disabled 状態に移行し続ける EtherChannel のトラブルシューティングを行います。問題を解決するにはどの 2 つのアクションを実行する必要がありますか? (2つお選びください。)

A. スイッチをリロードして、EtherChannel の再ネゴシエーションを強制します。

B. インターフェイス Gi1/0/2 と Gi1/0/3 が同じ隣接スイッチに接続されていることを確認します。

C. ポート チャネル 1 のスイッチポート パラメータが隣接スイッチのポート チャネルのパラメータと一致していることを確認します。

D. 隣接スイッチ上の対応するポート チャネル インターフェイスの名前が Port-channel1 であることを確認します。

E. Gi1/0/2 および Gi/0/3 の隣接インターフェイスが同じ EtherChannel のメンバーとして設定されていることを確認します。

Answer: (解答を表示する**)**

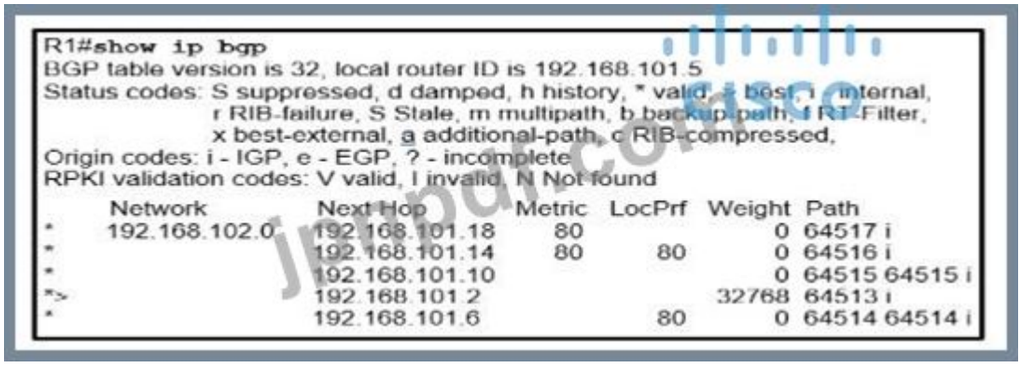
errdisable の原因

この機能は、スイッチがポート上で過剰な衝突または遅延衝突を検出したという特殊な衝突状況を処理するために初めて実装されました。スイッチが連続して 16 回の衝突に遭遇するため、フレームがドロップされると過剰な衝突が発生します。レイト コリジョンは、ワイヤ上のすべてのデバイスがワイヤが使用中であることを認識した後に発生します。このようなタイプのエラーの考えられる原因は次のとおりです。

仕様外のケーブル (長すぎる、間違ったタイプ、または欠陥がある) 不良なネットワーク インターフェイス カード (NIC) カード (物理的な問題またはドライバーの問題がある) ポートの二重化の誤り ポートの二重化の誤りは、ポートの二重化の誤りが原因となる一般的な原因です。直接接続された 2 つのデバイス (たとえば、スイッチに接続された NIC) 間で速度とデュプレックスを適切にネゴシエートできないためにエラーが発生します。LAN 内で衝突が発生するのは半二重接続のみです。イーサネットのキャリアセンス多元接続 (CSMA) の性質により、衝突がトラフィックの少数の割合を超えない限り、半二重では衝突が発生するのは正常です。

最新問題**: 180**

展示を参照してください。



192.168.101.2 に障害が発生した場合、どの IP アドレスが 192.168.102 0/24 のアクティブなネクスト ホップになりますか?

A. 192.168.101.18

B. 192.168.101.6

C. 192.168.101.10

D. 192.168.101.14

Answer: (解答を表示する**)**

上記の出力に示されている ｢>｣は、ネクスト ホップ 192.168.101.2 のパスが現在の最適なパスであることを示しています。

パス選択属性：重み > ローカル設定 > 発信元 > AS パス > 発信元 > MED > 外部 > IGP コスト > eBGP ピアリング > ルーター ID BGP は重みが最も高いパスを優先しますが、ここでの重みはすべて 0 です（これは、そうでないすべてのルートを示します）。ローカルルーターによって生成されるため）、ローカル設定を確認する必要があります。答え

LOCAL_PREF (LocPrf 列) のない ｢192.168.101.18｣パスは、デフォルト値が 100 であることを意味します。

したがって、ネクスト ホップ 192.168.101.18 を持つ 2 つの次善のパスを見つけることができます。

192.168.101.10。

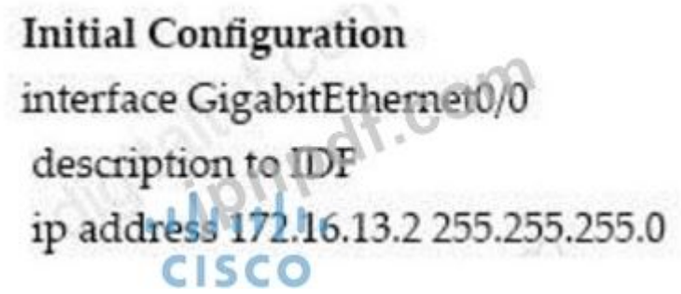
次のパス選択属性である Originate に移動する必要があります。BGP は、ローカル ルーターが発信したパス（｢ネクスト ホップ 0.0.0.0｣で示される) を優先します。しかし、2 つの最良の道はいずれも自分自身で生み出したものではありません。

ネクスト ホップ 192.168.101.18 の AS パスは、ネクスト ホップの AS パスよりも短いです

192.168.101.10 の場合、ネクストホップ 192.168.101.18 が次善のパスとして選択されます。

最新問題**: 181**

エンジニアは、VRRP グループ 10 のインターフェイス GigabitEthernet0/0 を設定する必要があります。ルーターがグループ内で最も高い優先順位を持つ場合、マスターの役割を引き受ける必要があります。このタスクを実行するには、どのコマンド セットを初期設定に追加する必要がありますか?



A. vrrp 10 ip 172.16.13.254
VRRP 10 プリエンプト
B. スタンバイ 10 ip 172.16.13.254
スタンバイ 10 プライオリティ 120
C. vrrp グループ 10 ip 172.16.13 254.255.255.255.0
vrrp グループ 10 優先度 120
D. スタンバイ 10 ip 172.16.13.254 255.255.255.0
スタンバイ 10 プリエンプト
Answer: A (メーッセージを残す**)**
実際、VRRP ではデフォルトでプリエンプションが有効になっているため、-vrrp 10 preempt コマンドは必要ありません。デフォルトの優先度は 100 なので、設定する必要もありません。ただし、グループの仮想 IP アドレスを構成する正しいコマンドは -vrrp 10 ip {ip-address} (-vrrp group 10 ip ... ではない) であり、このコマンドにはサブネット マスクが含まれていないことに注意してください。

最新問題**: 182**
OSPF では、ASBR ルーターを指すのはどの LAS タイプですか?
A. タイプ2
B. タイプ3
C. タイプ1
D. タイプ4
Answer: (解答を表示する**)**