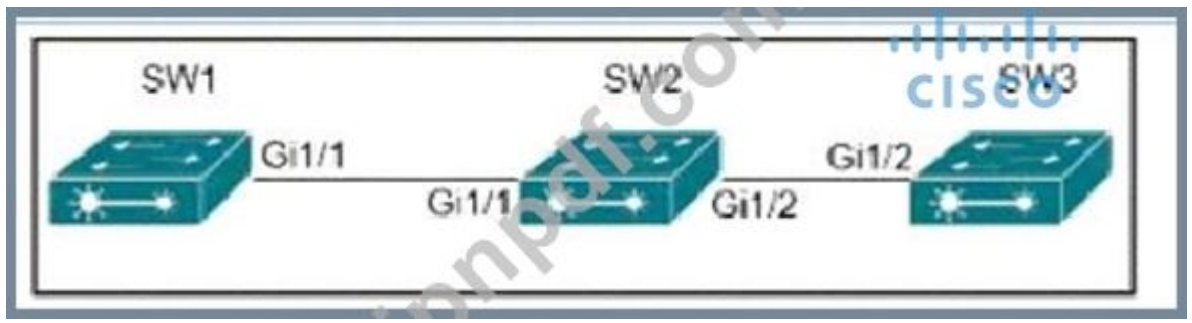
Cisco.350-401.v2023-03-10.q435

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:	435
バージョン:	v2023-03-10
アクセス数:	3243
ページビュー数:	4350
https://www.jpnpdf.com/Cisco.350-401.v2023-03-10.q435-mondaishu.html	

最新問題: 1



会社のポリシーにより、VLAN 10 は SW1 と SW2 でのみ許可されるように制限されています。他のすべての VLAN は、3 つのスイッチすべてに配置できます。管理者は、VLAN 10 が SW3 に伝播したことに気付きました。問題を修正する構成はどれですか?

A)

```
SW1(config)#int gi1/1
SW1(config)#switchport trunk allowed vlan 1-9,11-4094
```

B)

```
SW2(config)#int gi1/2
SW2(config)#switchport trunk allowed vlan 10
```

ハ)

```
SW2(config)#int gi1/2
SW2(config)#switchport trunk allowed vlan 1-9,11-4094
```

D)

```
SW1(config)#int gi1/1
SW1(config)#switchport trunk allowed vlan 10
```

A. オプション A
B. オプション C
C. オプション B

D. オプション D
Answer: (解答を表示する**)**

最新問題**: 2**
ルーターが 100 kbps を受け入れる SSH の量を制限する構成はどれですか?
A)

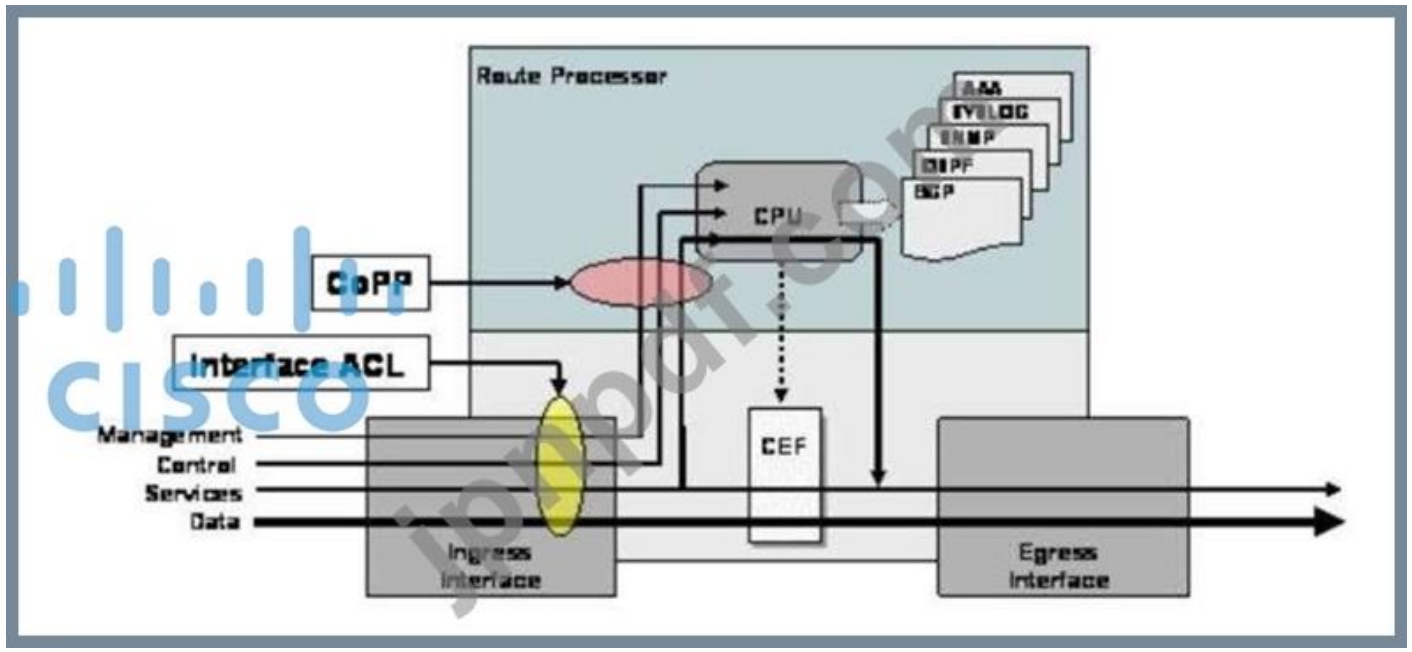
B)

ハ）

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: (解答を表示する**)**
CoPP は、ルート プロセッサを処理することにより、ネットワーク デバイス上のルート プロセッサを保護します。

独自のイングレス インターフェイスを持つ個別のエンティティとしてのリソース (および一部の実装、出口も)。CoPP は、宛先のトラフィックをポリシングするために使用されます。
次のようなルータのルート プロセッサ。
+ OSPF、EIGRP、BGP などのルーティング プロトコル。
+ HSRP、VRRP、GLBP などのゲートウェイ冗長プロトコル。
+ telnet、SSH、SNMP、RADIUS などのネットワーク管理プロトコル。



したがって、SSH を処理するために CoPP を適用する必要があります。
管理プレーン。CoPP は「control-plane」コマンドの下に置く必要があります。

最新問題: **3**
展示を参照してください。

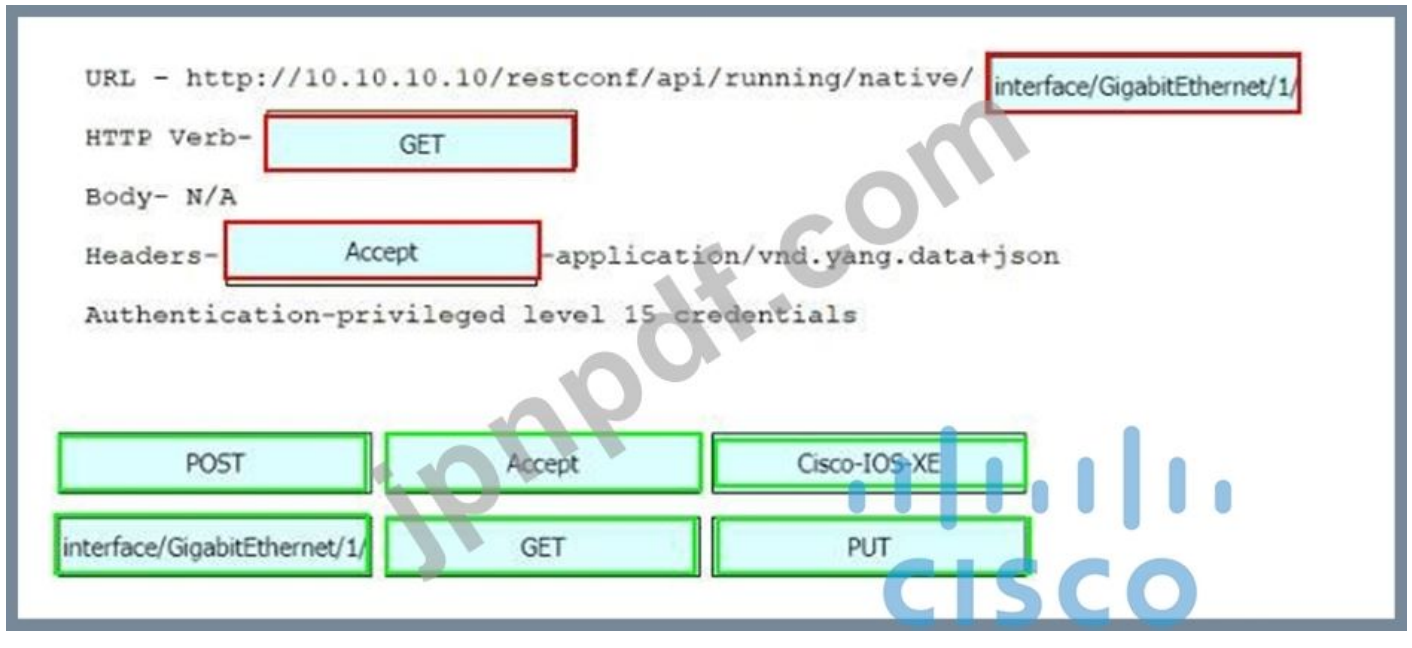
```
with manager.connect(host=192.168.0.1, port=22,
                     username='admin', password='password1', hostkey_verify=True,
                     device_params={'name':'nexus'}) as m:
```

コードのスニペットは何を達成しますか?
A. Cisco Nexus デバイスへの一時的な接続を作成し、API 呼び出しに使用するトークンを取得します。
B. ホスト キーが正しい場合、トンネルを開き、ログイン情報をカプセル化します。
C. Cisco Nexus デバイスへの ncclient 接続を開き、コンテキストの間維持します。
D. 保存されている SSH キーを使用して SSH 接続を作成し、パスワードは無視されます。
Answer: C (メーッセージを残す)
説明
ncclient は、NETCONF プロトコルに関するクライアント側のスクリプト作成とアプリケーション開発を容易にする Python ライブラリです。
上記の Python スニペットは、ncclient を使用して、Nexus デバイス (NETCONF サーバーでもある) に接続し、NETCONF セッションを確立します。

最新問題: **4**

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、このレスポンスを返すリクエストを作成します 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: **5**
出品物参照。

セグメント 192.168.0.0/24 の指定ルーターはどのルーターですか?

A. このセグメントは、非ブロードキャスト ネットワーク タイプであるため、指定ルーターがありません。

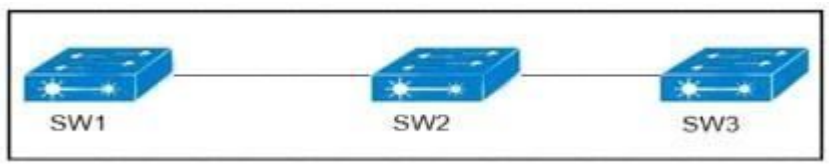
B. ルーター ID が低いため、ルーター シカゴ

C. ルーター ID が大きいため、Router NewYork

D. このセグメントは、p2p ネットワーク タイプであるため、代表ルーターがありません。

Answer: (解答を表示する**)**

最新問題: **6**
出品物参照。



VLAN 50 および 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、SW1 は VTP サーバです SW3 が VLAN からのみフレームを受信することを保証するコマンド
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) を受信しないはずです。
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) でプルーニングを設定する必要があることにも注意してください。

最新問題: **7**
Cisco SD-Access 展開でデータ プレーンの転送を担当するプロトコルはどれですか?
A. VXLAN
B. IS-IS
C. OSPF
D. LISP
Answer: (解答を表示する**)**
説明
SD-Access では、コントロール プレーンは LISP (Locator/ID Separation Protocol) に基づいており、データ プレーンは VXLAN (Virtual Extensible LAN)、ポリシー TrustSec に基づいており、管理プレーンは有効であり、
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#:~:text=In%20SD%

最新問題: **8**
展示を参照してください。

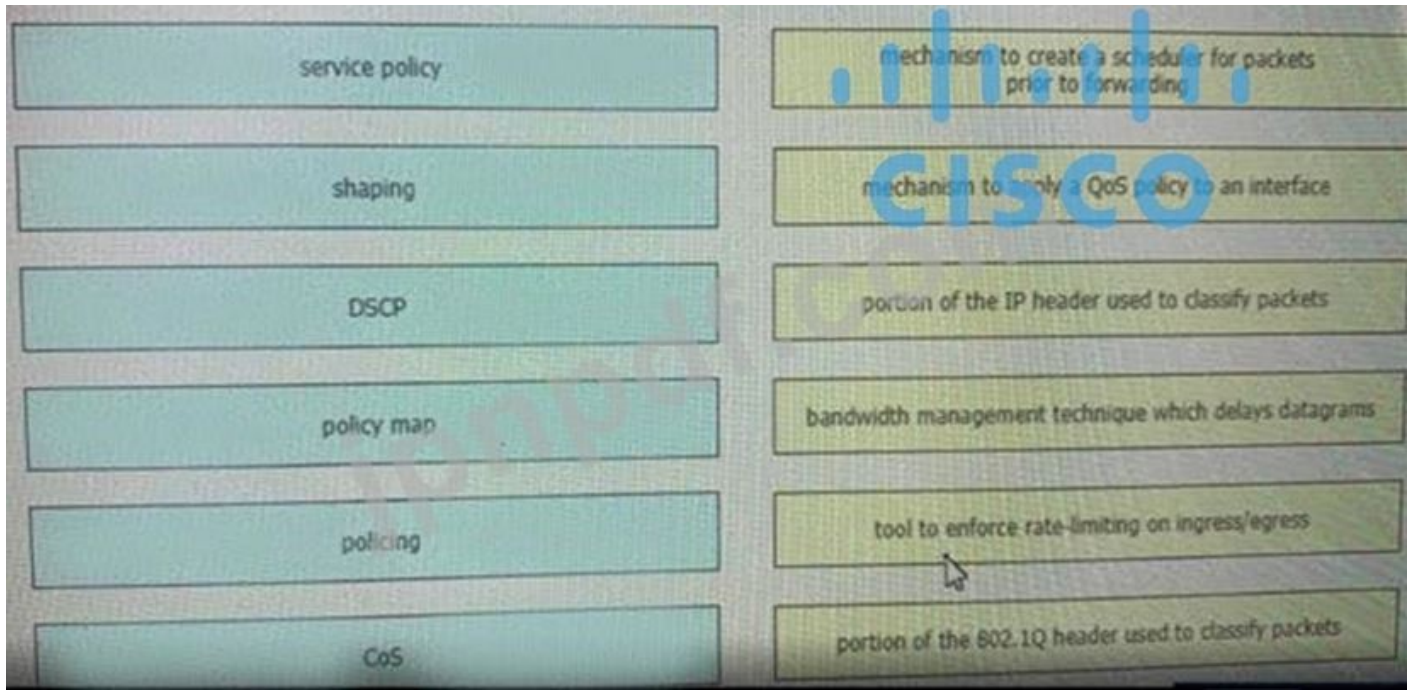
```
R1#show ip bgp
BGP table version is 32, local router ID is 192.168.101.5
Status codes: S suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
*    192.168.102.0    192.168.101.18           80             0 64517 i
*                     192.168.101.14           80         80  0 64516 i
*                     192.168.101.10                          0 64515 64515 i
*>                    192.168.101.2                    32768  64513 i
*                     192.168.101.6                       80  0 64514 64514 i
```

192.168.101.2 に障害が発生した場合、192.168.102 0/24 のアクティブなネクスト ホップになるのはどの IP アドレスですか?
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**)**
説明
上記の出力に示されている ｢>｣は、ネクスト ホップが 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。
パス選択の属性: Weight > Local Preference > Originate > AS Path > Origin > MED > External > IGP Cost > eBGP Peering > Router IDローカル ルーターによって発信されたもの) であるため、ローカル プリファレンス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 ホップが 192.168.101.18 である 2 つの次善のパスを見つけることができます。
192.168.101.10。
次のパス選択属性に移動する必要があります: Originate。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 つの最良の方法はいずれも、自分で作成したものではありません。

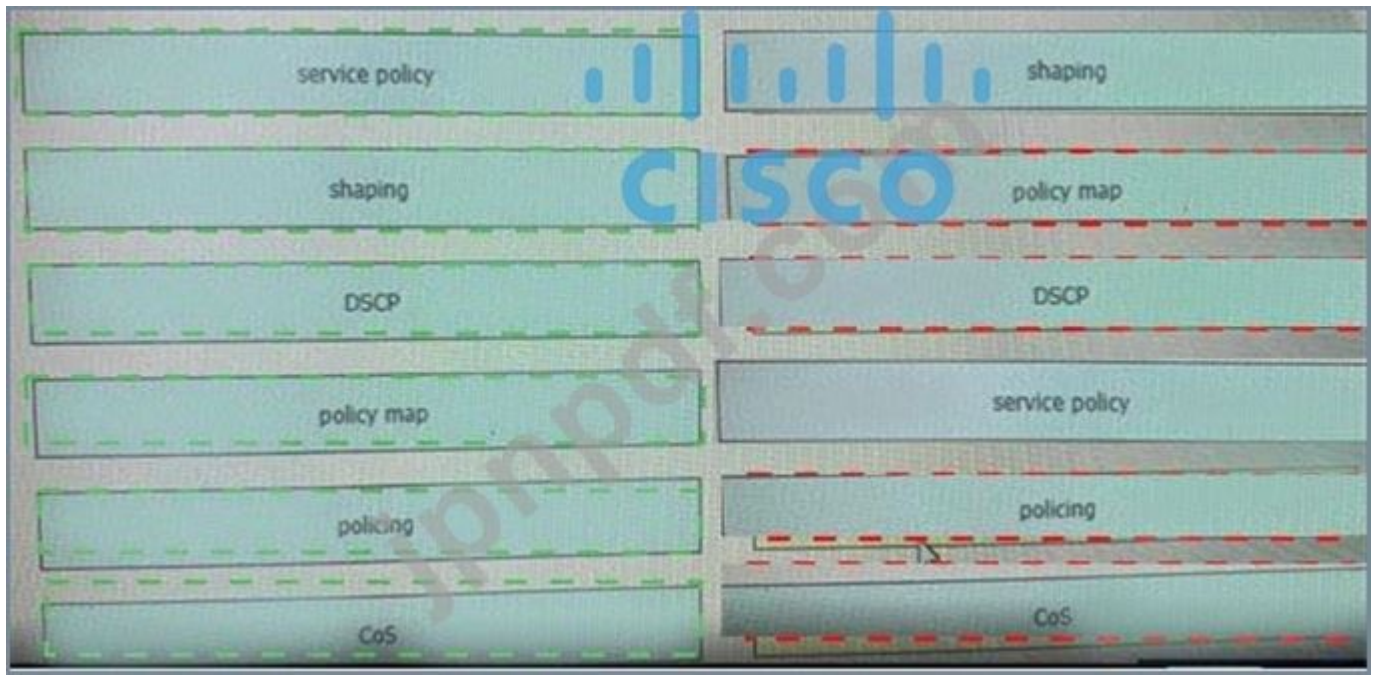
ネクスト ホップ 192.168.101.18 の AS パスは、ネクスト ホップの AS パスよりも短い
192.168.101.10 の場合、ネクスト ホップ 192.168.101.18 が次善のパスとして選択されます。

最新問題: **9**
3 層の階層型キャンパス ネットワーク設計において、コア層の設計のベスト プラクティスはどれですか?
A. コア デバイス間に冗長なレイヤ 3 ポイント ツー ポイント リンクを提供して、より予測可能で高速なコンバージェンスを実現します。
B. 802.IX、DHCP スヌーピング、VACL、ポート セキュリティなどの高度なネットワーク セキュリティ機能を提供します。
C. 重要なネットワーク トラフィックのマーキング、キューイング、分類などの QoS 優先順位付けサービスを提供します。
D. アクセス レイヤー デバイスの冗長アグリゲーションと、VRRP などのファースト ホップ冗長プロトコルを提供します。
Answer: A (メーッセージを残す**)**

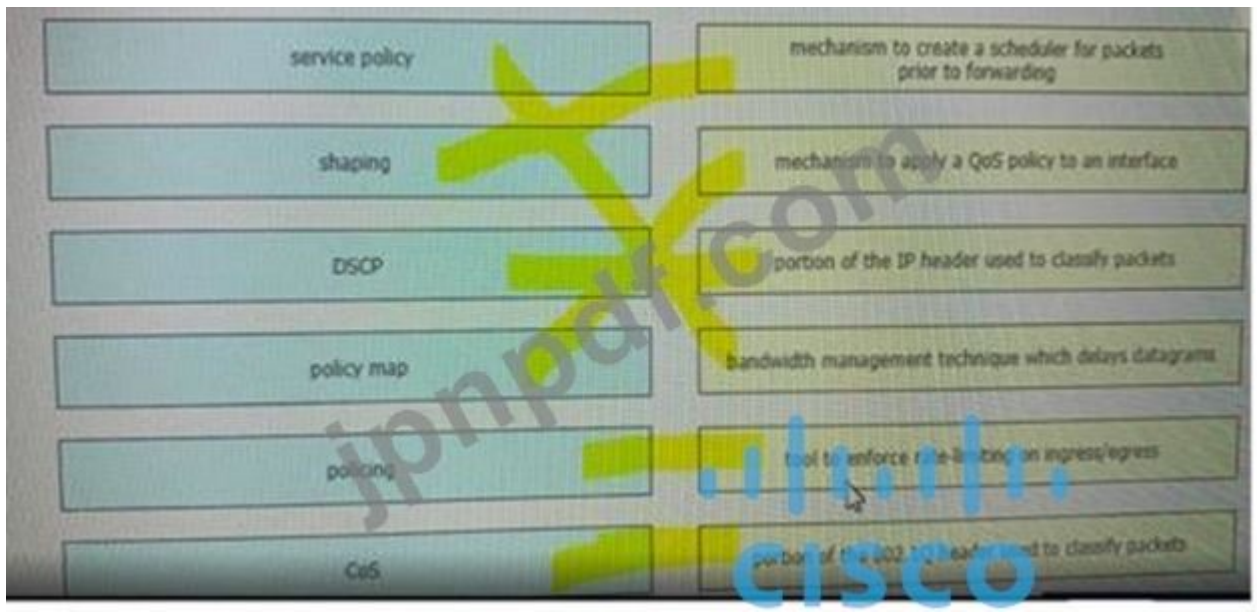
最新問題: **10**
Qos メカニズムを左から右の正しい説明にドラッグ アンド ドロップします。



Answer:

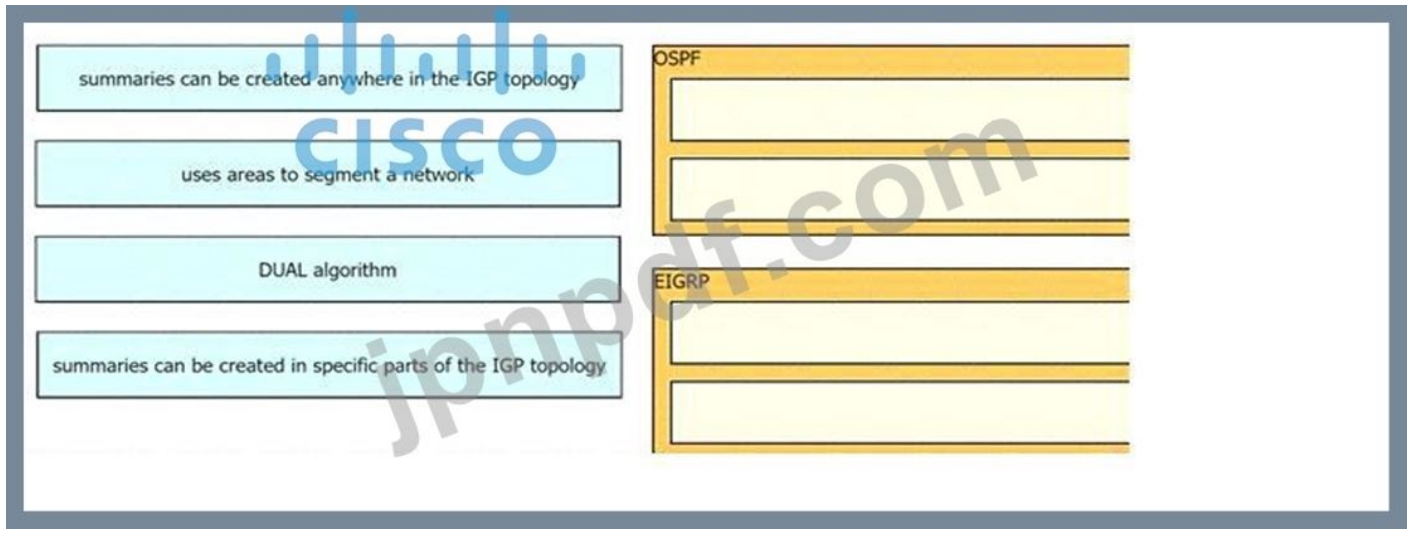


説明

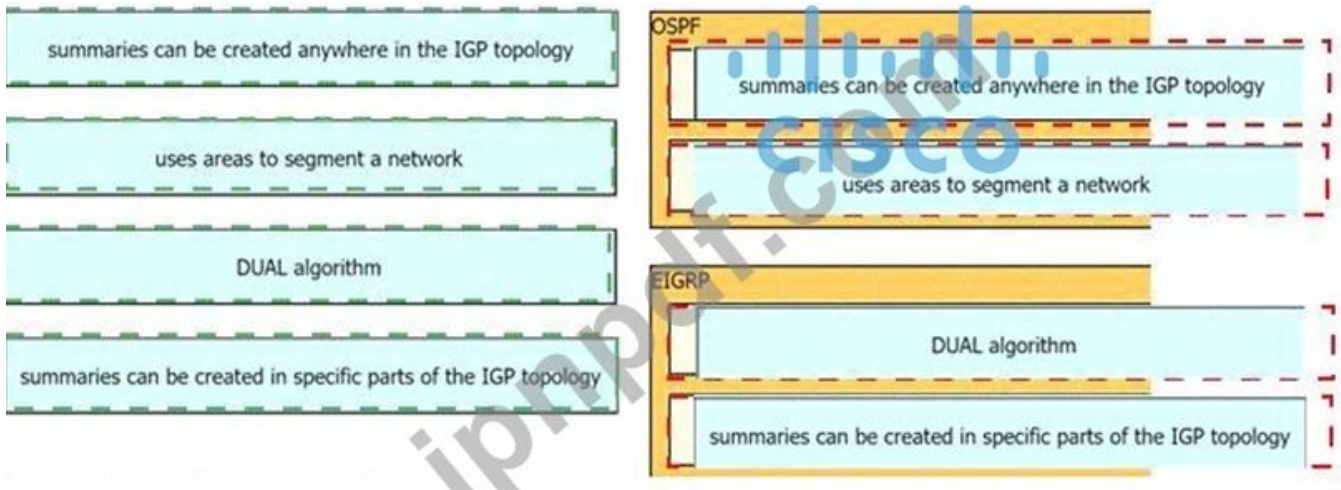


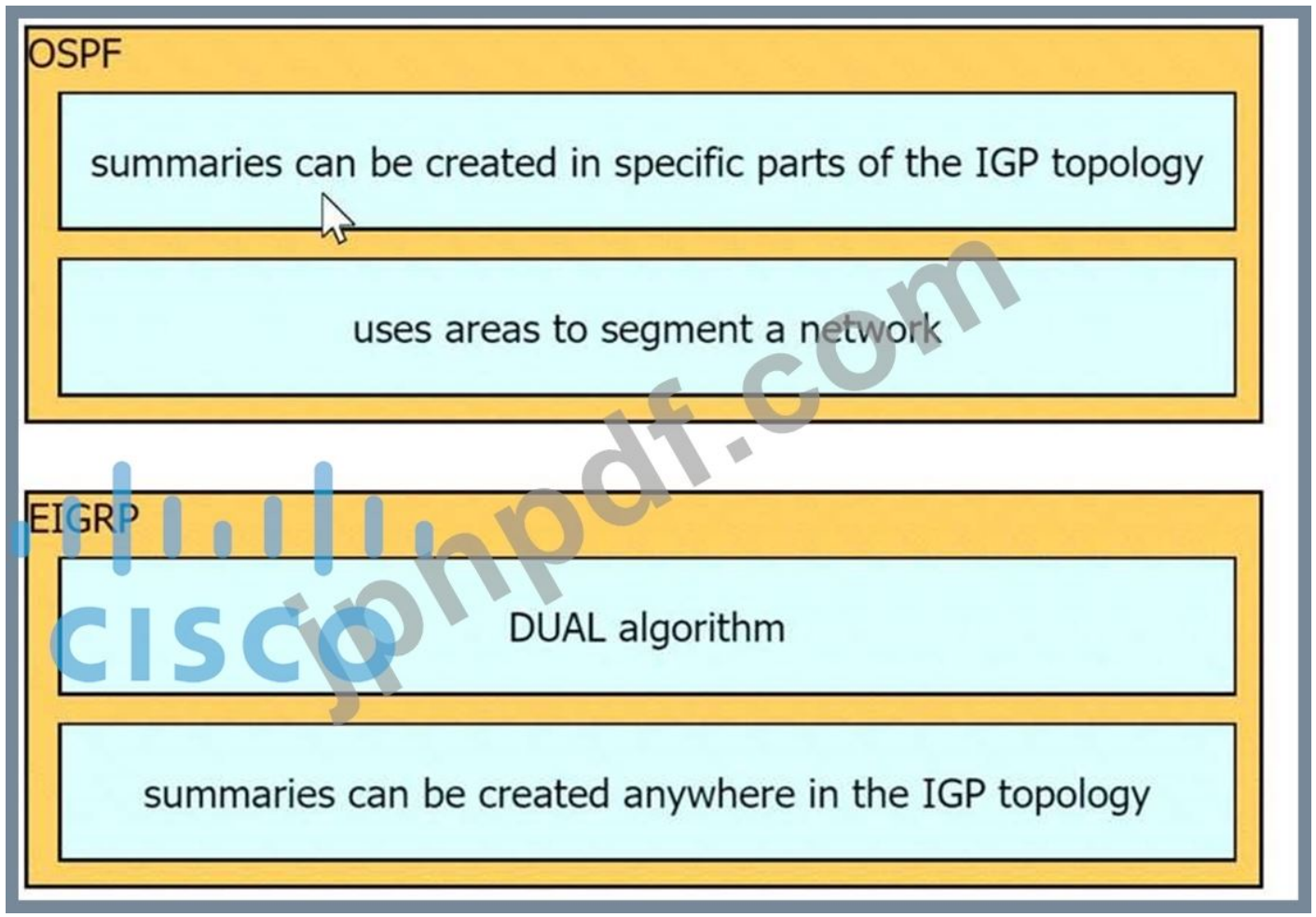
最新問題: **11**

復号化を左側から、右側に記述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。


summaries can be created anywhere in the IGP topology
uses areas to segment a network
DUAL algorithm
summaries can be created in specific parts of the IGP topology
OSPF
EIGRP

Answer:


summaries can be created anywhere in the IGP topology
uses areas to segment a network
DUAL algorithm
summaries can be created in specific parts of the IGP topology
OSPF
summaries can be created anywhere in the IGP topology
uses areas to segment a network
EIGRP
DUAL algorithm
summaries can be created in specific parts of the IGP topology



最新問題: **12**

展示を参照してください。

技術者が monitor session 1 destination remote vlan 233 コマンドを追加すると、どのような結果になりますか?

A. RSPAN トラフィックは VLAN 222 および 223 に送信されます。

B. RSPAN VLAN は VLAN 223 に置き換えられます。

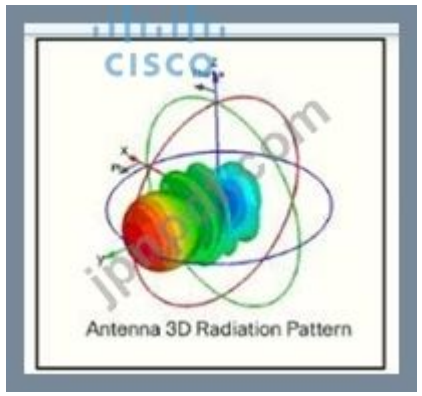
C. RSPAN トラフィックは、VLAN 222 と 223 の間で分割されます。

D. 2 つの宛先を構成するためにエラーがフラグ付けされます。

Answer: (解答を表示する**)**

最新問題: **13**

展示を参照してください。



放射パターンはどのタイプのアンテナを表していますか?

A. 八木

B. 多方向

C. 方向パッチ

D. 無指向性

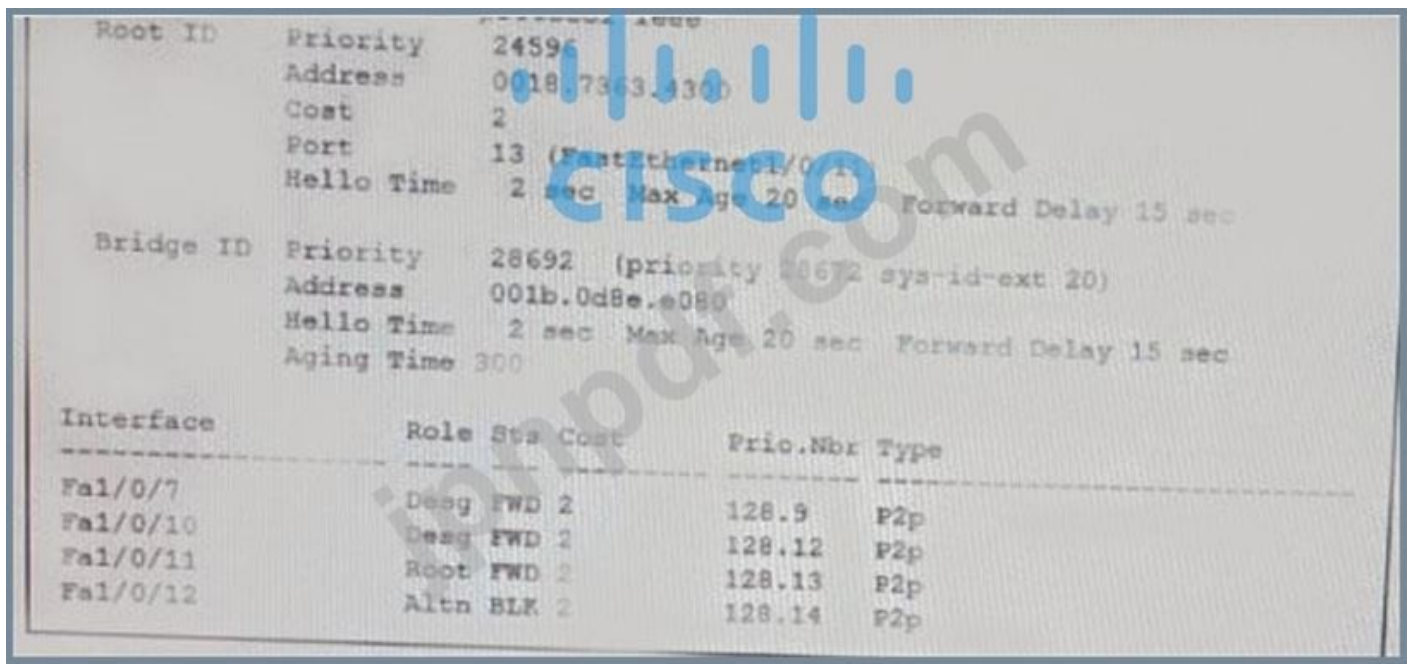
Answer: A (メーッセージを残す**)**

説明

八木アンテナは、単純なアンテナ (通常はダイポールまたはダイポールのようなアンテナ) を駆動し、長さと間隔が厳密に制御された一連の非駆動素子を使用してビームを成形することによって形成されます。

最新問題: 14

展示を参照してください。



出力は、スイッチのスパニング ツリー構成について何を確認しますか?

A. スパニング ツリー モードの stp ieee コマンドがこのスイッチで入力されました

B. このスイッチのスパニング ツリー動作モードは PVST です。

C. このスイッチのスパニング ツリー動作モードは PVST+ です。

D. このスイッチのスパニング ツリー動作モードは IEEE です。

Answer: C (メーッセージを残す)

最新問題**: 15**

EIGRP ではサポートされているが、OSPF ではサポートされていない機能は?

A. 等コスト ロード バランシング

B. 経路フィルタリング

C. 不等コスト負荷分散

D. 経路集約

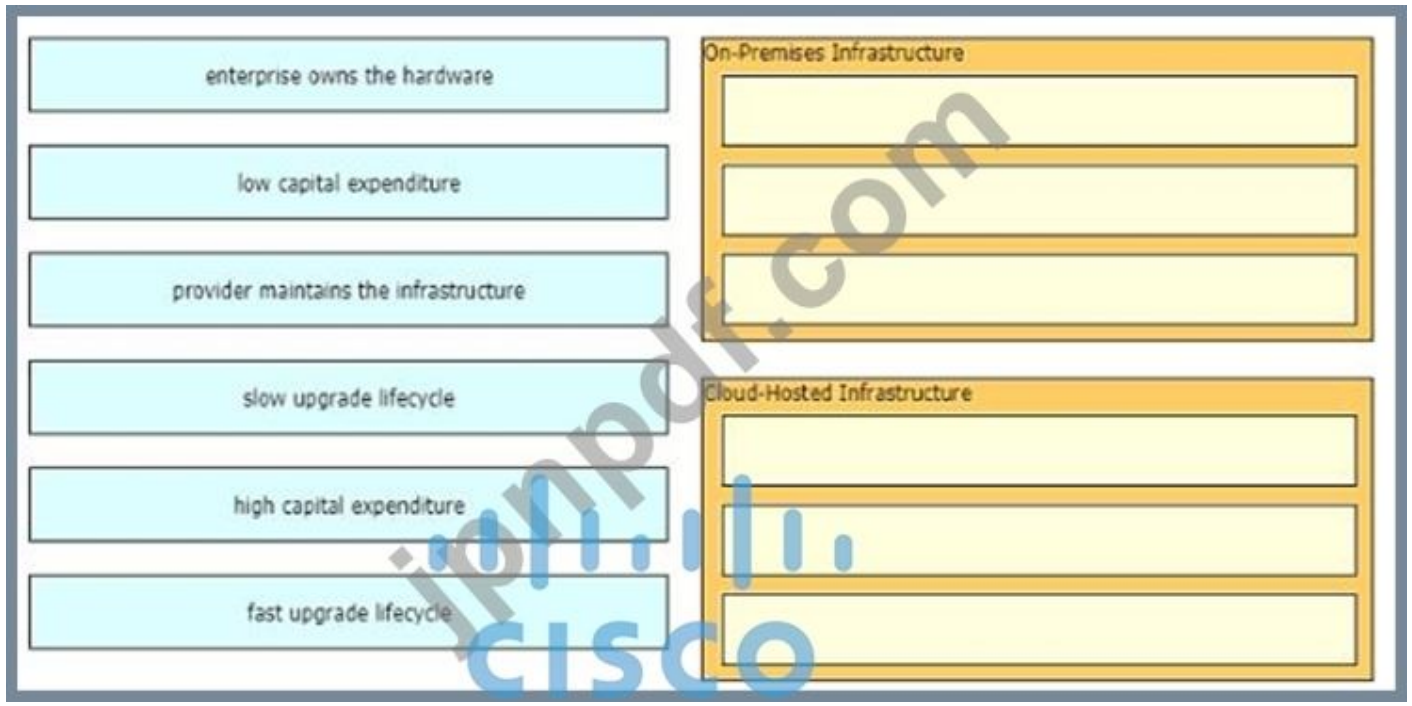
Answer: (解答を表示する)

EIGRP は 「分散 ...」による不等コスト ロード バランシングをサポートしますが、OSPF は等コストのみをサポートします。

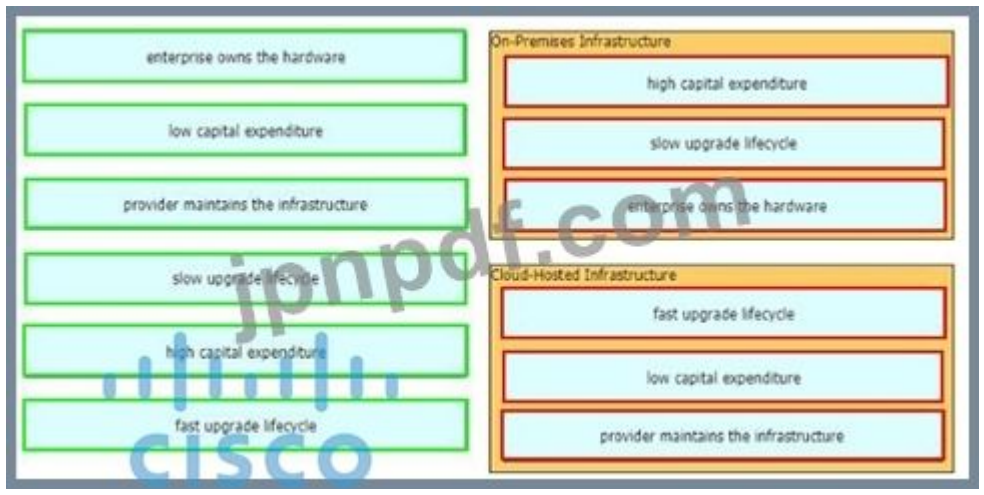
負荷分散。

最新問題**: 16**

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



Answer:



有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

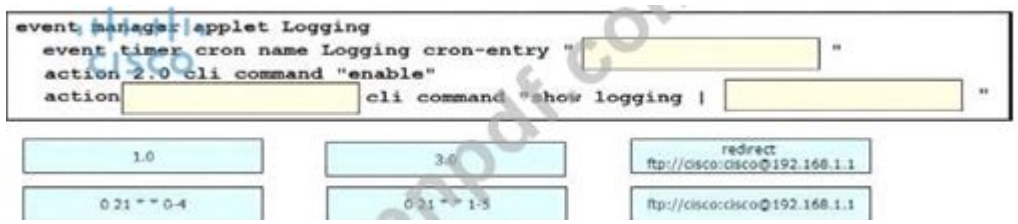
最新問題: **17**
CAPWAP AP にワイヤレス コントローラのアドレスを提供する DHCP オプションはどれですか?
A. 43
B. 66
C. 69
D. 150
Answer: A (メーッセージを残す**)**
説明

DHCP Option 43

DHCP option 43 is an option used for providing Wireless LAN Controller IP addresses to the AP. The DHCP option 43 is used to notify the AP to convert into CAPWAP AP.

最新問題**: 18**
マルチキャスト RP について正しい説明はどれですか?
A. RP は、プロトコルに依存しないマルチキャスト デンス モードを使用する場合にのみ必要です。
B. RP は、プロトコルに依存しないマルチキャスト スパース モードとデンス モードに必要です。
C. デフォルトでは、RP はソースおよびレシーバーとのセッションを維持するために定期的に必要です。
D. デフォルトでは、RP はソースおよびレシーバーとの新しいセッションを開始する場合にのみ必要です。
Answer: (解答を表示する**)**
ランデブー ポイント (RP) は、Protocol Independent Multicast Sparse Mode (PIM-SM) を実行しているネットワークでのみ必要です。
デフォルトでは、RP はソースおよびレシーバーとの新しいセッションを開始する場合にのみ必要です。
参照：
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html 参考までに、PIM-SM では、明示的に要求したアクティブな受信者を持つネットワーク セグメントのみマルチキャスト データがトラフィックに転送されます。マルチキャスト データを配信するこの方法は、PIM デンス モード (PIM-DM) モデルとは対照的です。PIM-DM では、マルチキャスト トラフィックは最初にネットワークのすべてのセグメントにフラッディングされます。ダウンストリーム ネイバーまたは直接接続された受信者を持たないルーターは、不要なトラフィックをプルーニングします。

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、日曜日から木曜日の午後 9 時までにアプライアンスで発生したすべてのログを表示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。

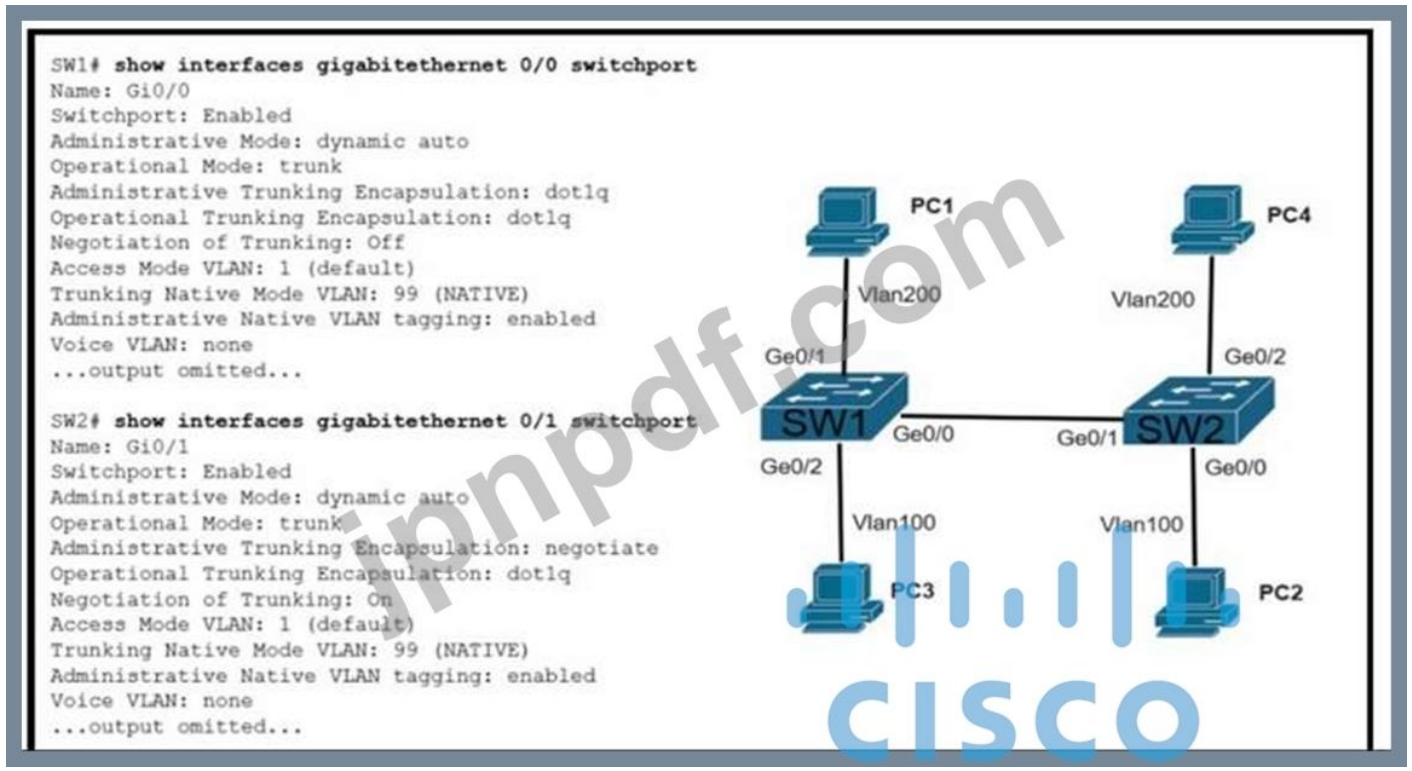


Answer:

最新問題**: 20**
タイプ 2 ハイパーバイザーの例は次のうちどれですか? (3つ選んでください。)
A. Oracle VirtualBox
B. Oracle Solaris ゾーン
C. Microsoft Hyper-V
D. VMware ESXi

E. Microsoft Virtual PC
Answer: A,B,E (メーッセージを残す)

最新問題**: 21**
展示を参照してください。



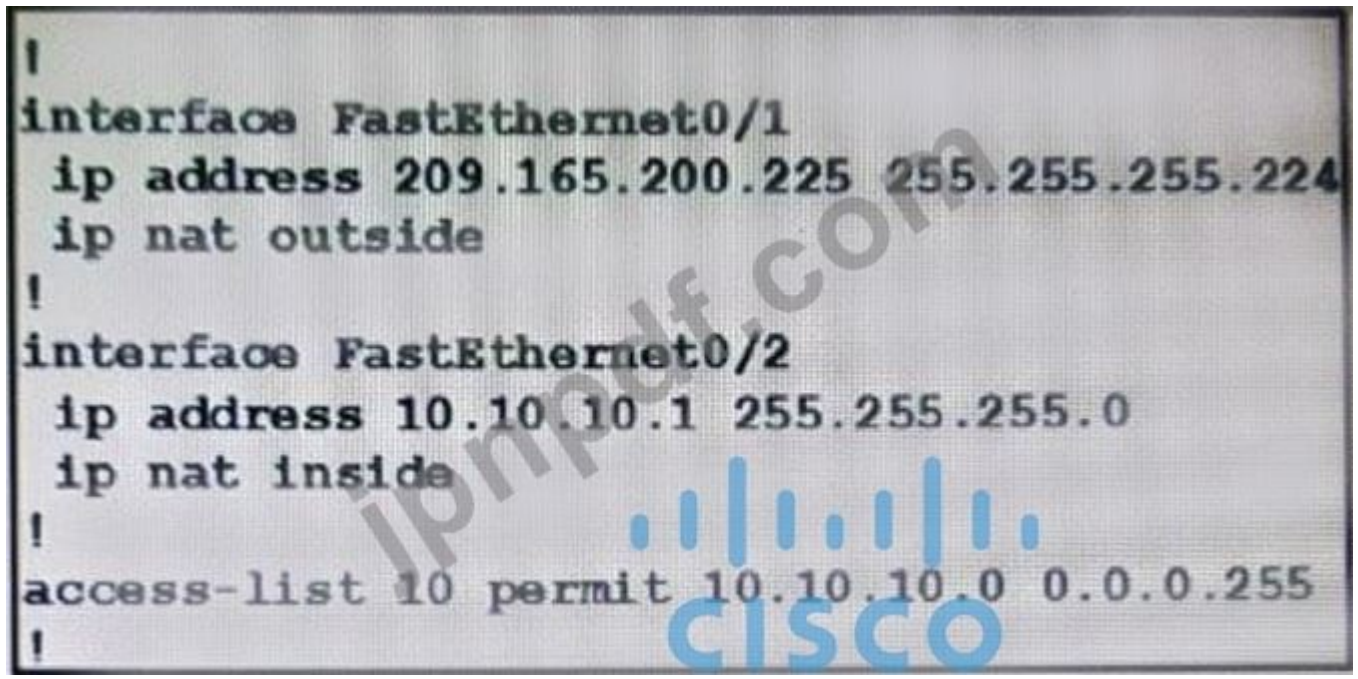
SW1 と SW2 の間の接続は動作していません。問題を解決する 2 つのアクションはどれですか? 2つ選んでください。）
A. SW2 でスイッチポート モード アクセスを構成する
B. SW1 で switchport nonegotiate を構成する
C. SW2 でスイッチポート モード トランクを構成します。
D. SW2 でスイッチポート モードをダイナミックに設定します。
E. SW2 で switchport nonegotiate を構成する
Answer: C,D (メーッセージを残す)

最新問題**: 22**
展示を参照してください。

エンジニアは、ルーターから直接接続されたサブネット 209.165.200.0/24 へ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。エンジニアは、アクセス コントロール リスト EGRESS をルーターの GigabitEthernet0/0 インターフェイスのアウトバウンド方向に適用します。ただし、ルーターは 209.165.200.0/24 サブネット上のホストに ping を実行できます。この動作について正しい説明はどれですか?

A. アクセス制御リストがインターフェイスに適用された後、アクセス制御リストを有効にするには、そのインターフェイスをシャットダウンし、非シャットダウンにする必要があります。
B. 送信元 IP アドレスからのトラフィックをブロックできるのは、標準のアクセス コントロール リストのみです。
C. ルーター インターフェイスへのアウトバウンドに適用されるアクセス制御リストは、ルーターから送信されるトラフィックには影響しません。
D. ルーターからのトラフィックをブロックするには、アクセス制御リストに明示的な拒否を含める必要があります。
Answer: C (メーッセージを残す)

最新問題: **23**

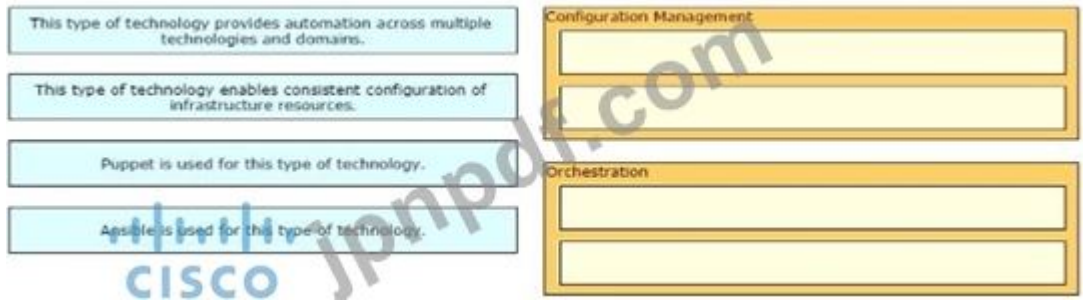


展示を参照してください。FastEthernet0/2 に接続されているホストがインターネットにアクセスできるようにするコマンドはどれですか?
A. ip nat inside source list 10 インターフェイス FastEthernet0/1 オーバーロード
B. ip nat inside source list 10 インターフェイス FastEthernet0/2 過負荷
C. ip nat outside source list 10 インターフェイス FastEthernet0/2 過負荷
D. ip nat outside source static 209.165.200.225 10.10.10.0 オーバーロード
Answer: A (メーッセージを残す)
説明
コマンド ip nat inside source list 10 interface FastEthernet0/1 overload は、Fa0/1 インターフェイスに割り当てられたアドレスをオーバーロードするように NAT を構成します。

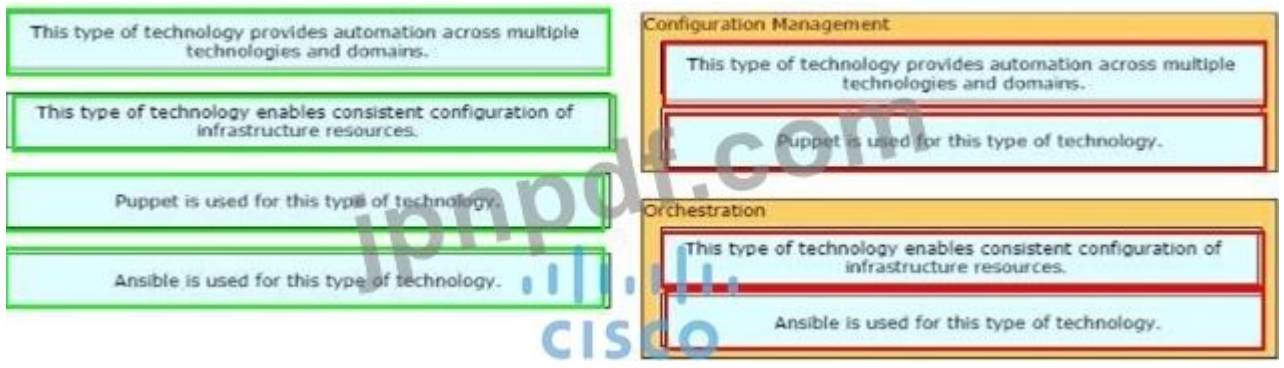
最新問題: **24**
RESTCONF を使用してネットワーク デバイスに構成を書き込む場合、TLS について正しい記述はどれですか?
A. プロキシ Web サーバーとして機能する NGINX を使用して提供されます。
B. Cisco デバイスではサポートされていません。
C. HTTP および HTTPS リクエストに使用されます。
D. 認証に証明書が必要でした。
Answer: (解答を表示する)

最新問題: **25**

左の特性を右のテクノロジー タイプにドラッグ アンド ドロップします。

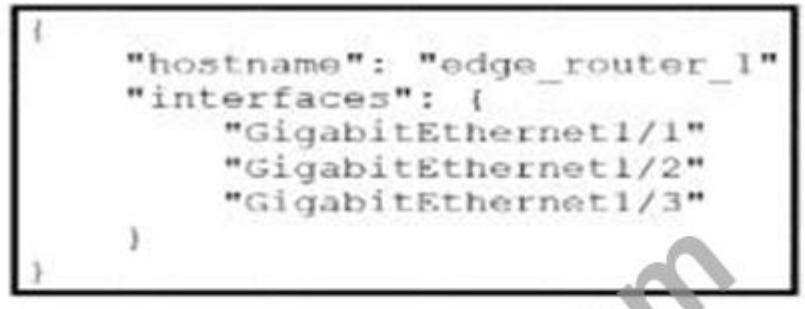


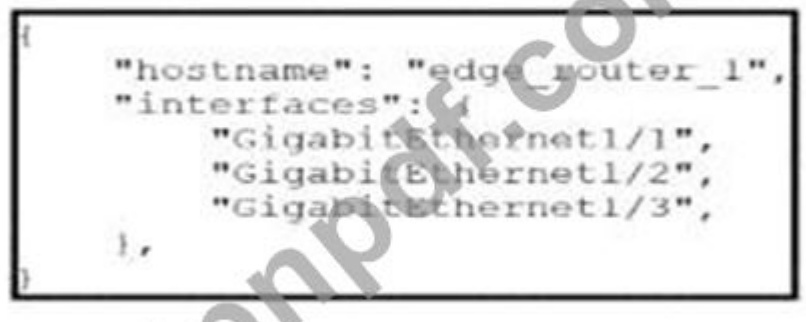
Answer:



最新問題: **26**

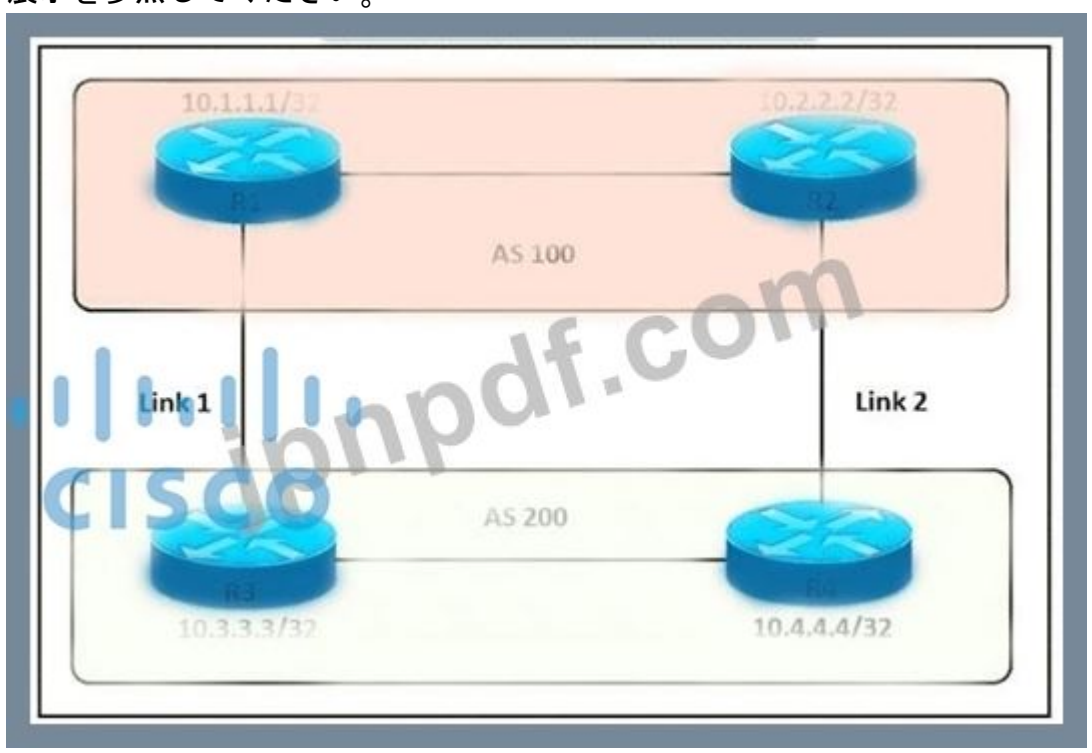
有効な JSON ファイルを表示する展示はどれですか?



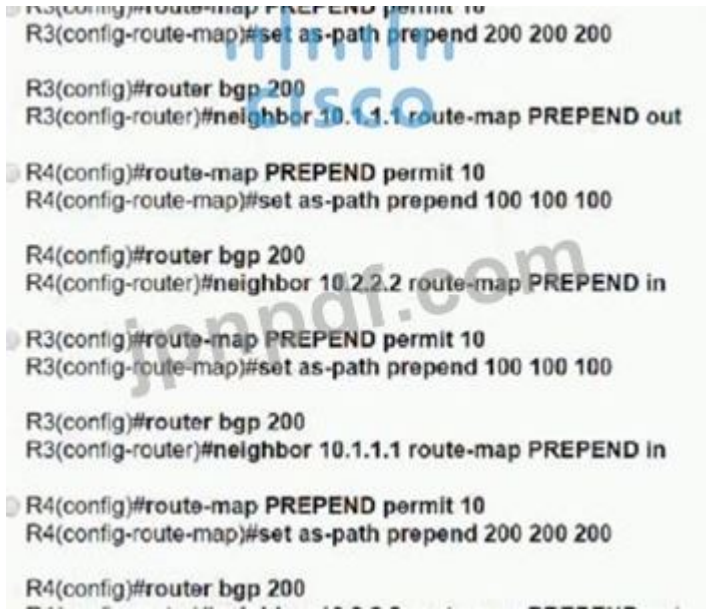


A. オプション B
B. オプション A
C. オプション D
D. オプション C
Answer: C (メーッセージを残す**)**

最新問題**: 27**
展示を参照してください。



エンジニアは、AS 200 を出るすべてのトラフィックがリンク 2 をエントリ ポイントとして選択するようにする必要があります。すべての BGP ネイバー関係が形成され、どのルーターでも属性が変更されていないと仮定すると、どの構成でタスクが達成されますか?

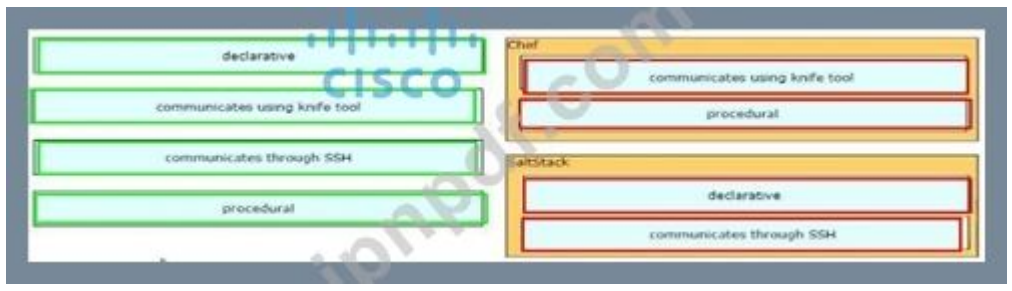


A. オプション A
B. オプション B
C. オプション C
D. オプション D
Answer: A (メーッセージを残す**)**
説明
R3 は、複数の AS 100 を使用して BGP アップデートを R1 にアドバタイズするため、R3 は、R3 を経由して AS 200 に到達するパスが R2 よりも遠いと考えているため、R3 はトラフィックを AS 200 に転送するために R2 を選択します。

最新問題**: 28**
NETCONF で一般的に使用されているデータ モデリング言語はどれですか?
A. HTML
B. XML
C. ヤン
D. レスト
Answer: C (メーッセージを残す**)**
Cisco IOS XE は、Yet Another Next Generation（YANG）データ モデリング言語をサポートしています。YANG をネットワーク構成プロトコル (NETCONF) と共に使用して、自動化されたプログラム可能なネットワーク操作の望ましいソリューションを提供できます。NETCONF(RFC6241) は、クライアント アプリケーションがデバイスから情報を要求したり、デバイスの構成を変更したりするために使用する XML ベースのプロトコルです。YANG は主に、NETCONF 操作で使用される設定および状態データをモデル化するために使用されます。
参考 :https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-5/configuration_guide/prog/b_165_prog_9500_cg/data_models.pdf
注: NETCONF も XML を使用しますが、XML はデータ モデリング言語ではありません。

最新問題**: 29**
特性を左側から右側に記述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。

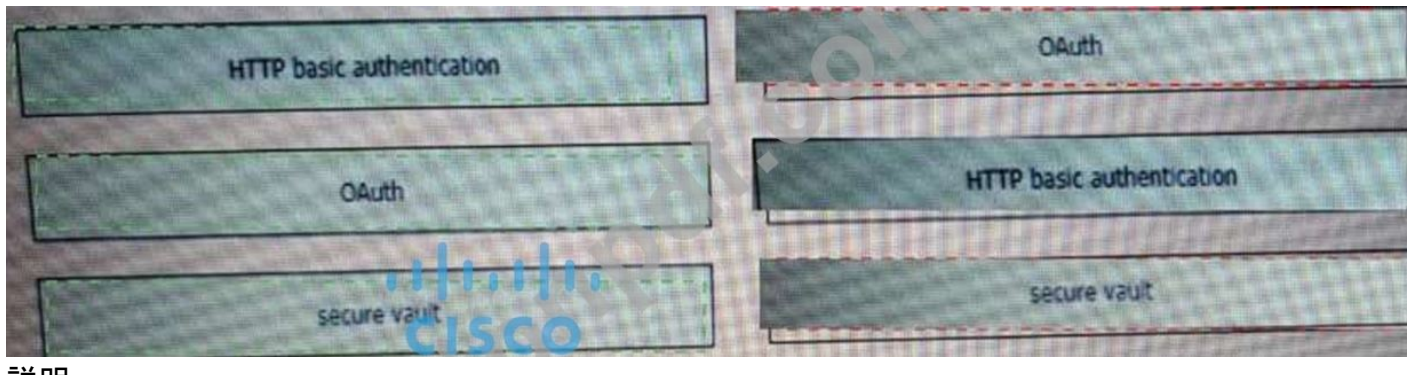
Answer:



最新問題**: 30**

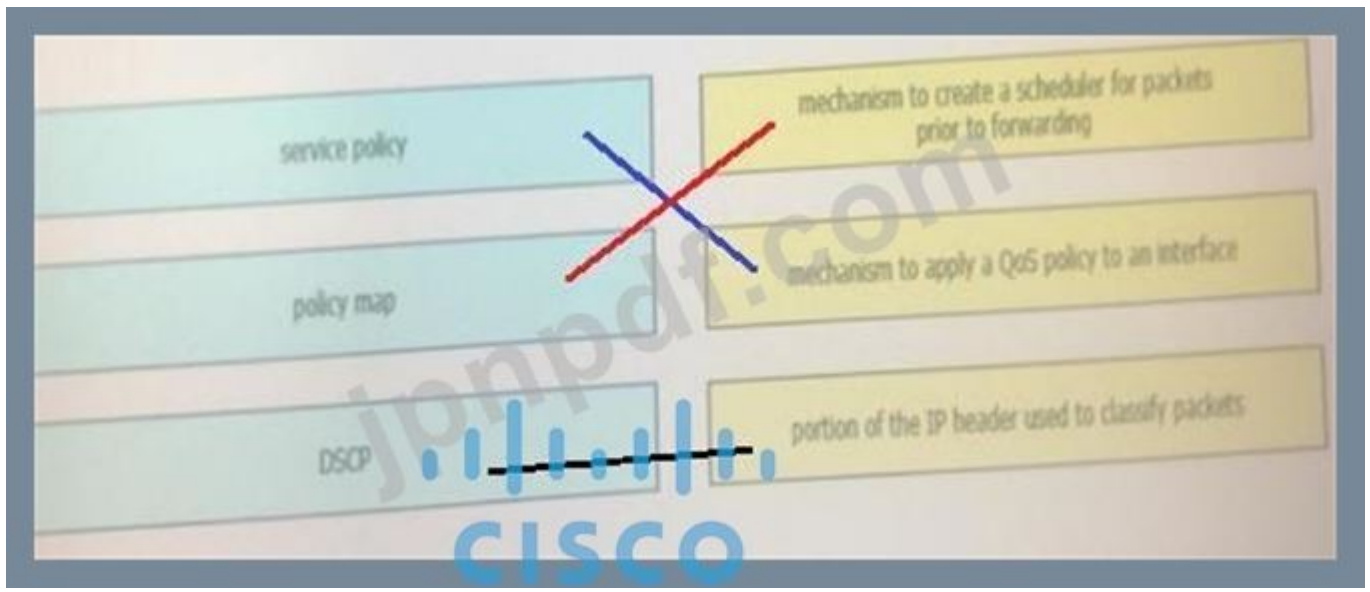
Qos メカニズムを左から右の正しい説明にドラッグ アンド ドロップします。

Answer:



説明

図を含む画像 自動生成された説明



最新問題: **31**
Python でエラー処理に使用されるステートメントはどれですか?
A. トライ/キャッチ
B. 試行/除外
C. ブロック/レスキュー
D. キャッチ/リリース
Answer: B (メーッセージを残す**)**

「try」と「except」という単語は Python のキーワードであり、例外をキャッチするために使用されます。例えば：
試す：
印刷 1/0
ZeroDivisionError を除く:
print "エラー! ゼロで割ることはできません!!!"

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **32**
ネットワーク監視システムは SNMP ポーリングを使用してルーター インターフェイスの統計を記録します エンジニアが新しいインターフェイスをインストールしてルーターをリロードするまで、SNMP クエリは期待どおりに機能します このアクションの後、ルーターのすべての SNMP クエリが失敗します この問題の原因は何ですか?
A. SNMP コミュニティが正しく構成されていません
B. SNMP サーバー トラップは、インターフェイス インデックスに対して無効になっています。
C. リンク状態のSNMPサーバートラップは無効です。
D. 再起動後に SNMP インターフェイス インデックスが変更されました。

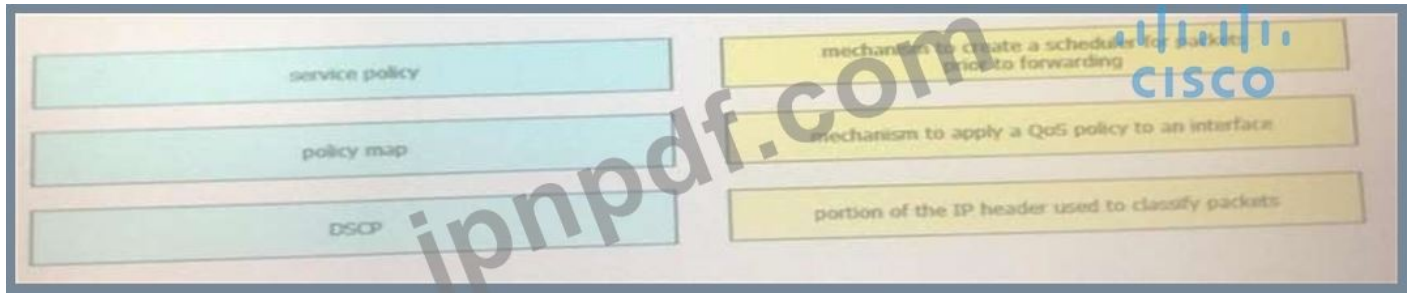
Answer: (解答を表示する)

最新問題**: 33**
ある顧客は、都市全体に 20 の店舗を持っています。各店舗には、中央の WLC によって管理される単一の Cisco アクセス ポイントがあります。顧客は、各店舗のユーザーの分析を収集したいと考えています。これらの要件をサポートする手法はどれですか?
A. プレゼンス
B. ハイパーロケーション
C. 到来角
D. 三辺測量
Answer: (解答を表示する)

最新問題**: 34**
サウスバウンド プロトコルを介してシスコ以外のデバイスを管理できるようにするために、Cisco DNA Center が使用する方法はどれですか?
A. SDK を使用してデバイス パックを作成します。
B. Cisco 以外のデバイスで使用可能な API を CSV 形式でインポートします。
C. 各ベンダーから利用可能な API を詳述する MIB を取得します。
D. API 呼び出しを使用してデバイスに問い合わせ、返されたデータを登録します。
Answer: D (メーッセージを残す)

最新問題**: 35**
Cisco SD-Access アーキテクチャでレイヤ 2 およびレイヤ 3 論理ネットワークを提供するために使用されるテクノロジーはどれですか?
A. アンダーレイ ネットワーク
B. VPN ルーティング/転送
C. 簡単な仮想ネットワーク
D. オーバーレイ ネットワーク
Answer: D (メーッセージを残す)
説明
An *overlay* network is created on top of the underlay network through virtualization (virtual networks). The data plane traffic and control plane signaling are contained within each virtualized network, maintaining isolation among the networks and an independence from the underlay
オーバーレイ ネットワークは、任意の物理アンダーレイ トポロジ上に構築されたデバイスを仮想的に接続するために使用される論理トポロジを作成します。
オーバーレイ ネットワークは、仮想化 (仮想ネットワーク) によってアンダーレイ ネットワークの上に作成されます。データ プレーン トラフィックとコントロール プレーン シグナリングは、各仮想化ネットワーク内に含まれ、ネットワーク間の分離とアンダーレイ ネットワークからの独立性を維持します。
SD-Access では、LISP によって提供されるサービスを介して、オーバーレイ全体でレイヤ 2 およびレイヤ 3 接続を拡張できます。
参照: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

最新問題**: 36**
Qos メカニズムを左から右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**: 37**

展示を参照してください。ルータ r R1 のどのコマンド セットで、プライベート ホスト PC1、PC2、および PC3 をパブリック スペースのアドレスに決定論的に変換できますか?

- RouterR1(config)#int f0/0
  RouterR1(config-if)#ip nat inside
  RouterR1(config-if)#exit
  RouterR1(config)#int f0/1
  RouterR1(config-if)#ip nat outside
  RouterR1(config-if)#exit
  RouterR1(config)#ip nat inside source static 10.10.10.101 155.1.1.101
  RouterR1(config)#ip nat inside source static 10.10.10.102 155.1.1.102
  RouterR1(config)#ip nat inside source static 10.10.10.103 155.1.1.103

- RouterR1(config)#int f0/0
  RouterR1(config-if)#ip nat inside
  RouterR1(config-if)#exit
  RouterR1(config)#int f0/1
  RouterR1(config-if)#ip nat outside
  RouterR1(config-if)#exit
  RouterR1(config)#access-list 1 10.10.10.0 0.0.0.255
  RouterR1(config)ip nat inside source list 1 interface f0/1 overload

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

最新問題**: 38**
LISP ネットワーク アーキテクチャとプロトコルが使用する 2 つの名前空間はどれですか? (2つ選んでください。)
A. TLOC
B. RLOC
C. DNS
D. VTEP
E. EID
Answer: (解答を表示する**)**
Locator ID Separation Protocol (LISP) は、ネットワーク アーキテクチャおよびプロトコルです。
単一の IP アドレスの代わりに 2 つの名前空間の使用を実装します。
+ エンド ホストに割り当てられたエンドポイント識別子 (EID)。
+ ルーティング ロケーター (RLOC) - を構成するデバイス (主にルーター) に割り当てられます。
グローバル ルーティング システム。
参照：
ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html

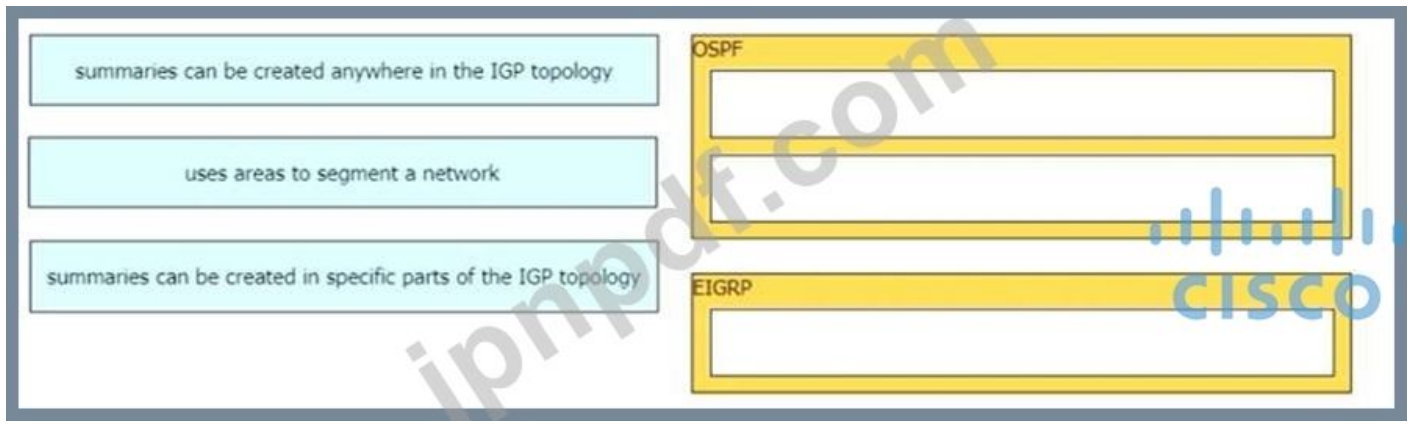
最新問題: **39**

REST API の認証方法を左から右の説明にドラッグ アンド ドロップします。

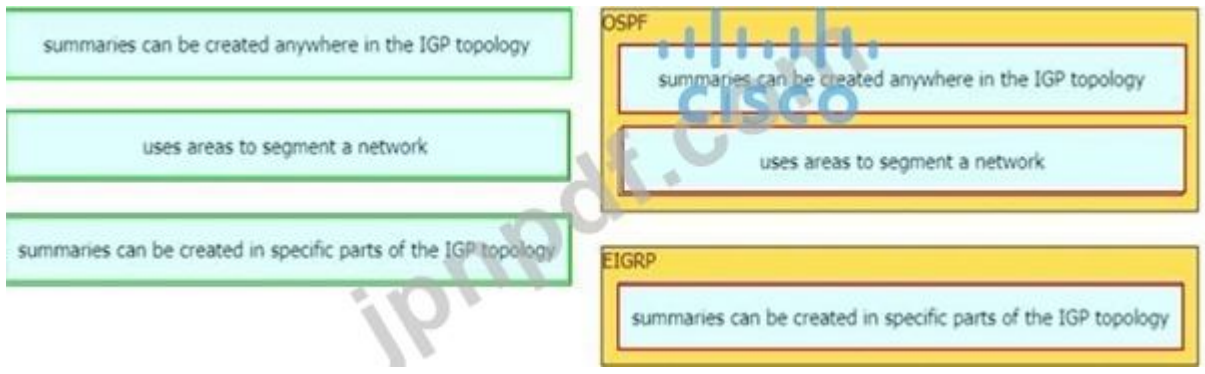
Answer:

最新問題: **40**

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**: 41**

仮想コンポーネントを左側から右側の説明にドラッグ アンド ドロップします。

Answer:

説明

+ ゲスト OS などの仮想マシンの設定を含む構成ファイル: VMX

+ ハイパーバイザーへのパケットの送信を担当する仮想マシンのコンポーネント: vNIC

+ 仮想マシン構成ファイルと仮想ディスクを含む zip ファイル: OVA

+ 仮想マシンのディスク ドライブを含むファイル: VMDK

VMX ファイルは、仮想マシンの構成を保持するだけです。

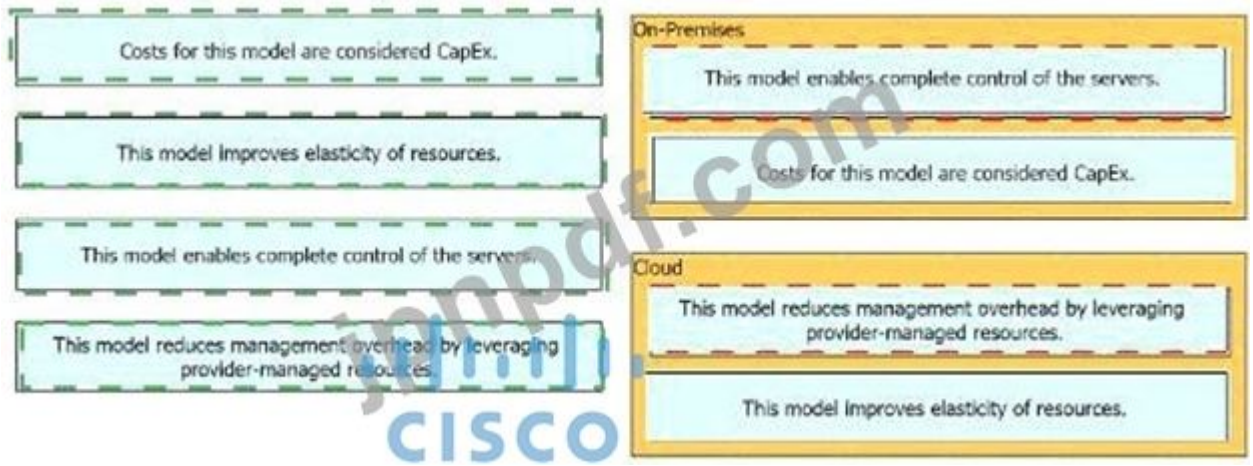
VMDK (Virtual Machine Disk の略) は、VMware Workstation や VirtualBox などの仮想マシンで使用される仮想ハード ディスク ドライブのコンテナーを記述するファイル形式です。

OVA ファイルは、仮想マシンの圧縮された 「インストール可能な」バージョンを含む Open Virtualization Appliance です。OVA ファイルを開くと、VM が抽出され、コンピューターにインストールされている仮想化ソフトウェアにインポートされます。

最新問題**: 42**

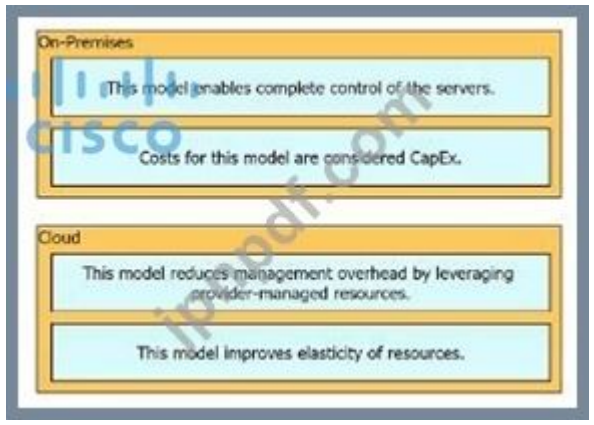
左側の特性を右側のインフラストラクチャ デプロイ モデルにドラッグ アンド ドロップします。

Answer:



説明

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



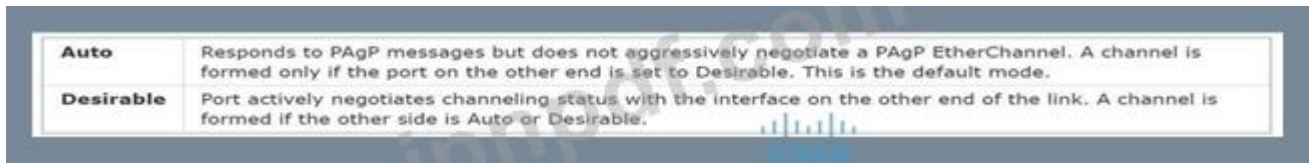
最新問題: **43**

左の特性を右の配置モデルにドラッグ アンド ドロップします。

Answer:

最新問題: **44**
OVF とは何ですか?
A. 仮想マシンまたは仮想アプライアンスを記述するために使用されるファイルのパッケージ
B. IMG に似た、仮想マシンの構築に使用される OVA ファイルを含むパッケージ
C. P2V 移行の 3 番目のステップ
D. 仮想マシンのベース オペレーティング システムのインストールに使用される ISO の代替形式
Answer: (解答を表示する**)**

最新問題: **45**
イーサチャネルの形成を妨げる PAgP モードの組み合わせはどれですか?
A. オート/オート
B. 望ましい/望ましい
C. 自動/望ましい
D. 望ましい
Answer: A (メーッセージを残す**)**
次の 2 つの PAgP モードがあります。



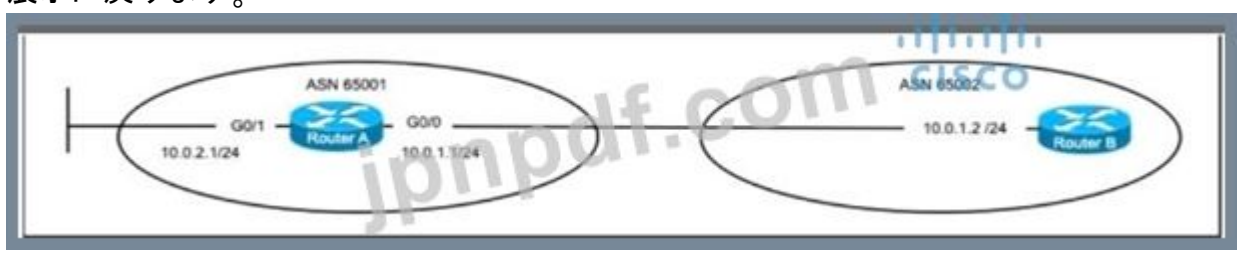
Auto	Responds to PAgP messages but does not aggressively negotiate a PAgP EtherChannel. A channel is formed only if the port on the other end is set to Desirable. This is the default mode.
Desirable	Port actively negotiates channeling status with the interface on the other end of the link. A channel is formed if the other side is Auto or Desirable.

次の表に、PAgP に対して EtherChannel が形成されるかどうかを示します。

PAgP	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	**No**

最新問題: **46**

展示に戻ります。



展示を参照してください。エンジニアは、ルーター B のルーター B に eBGP ネイバーシップを構成する必要があります。ルーター A の GO/1 に接続されているネットワークは、ルーター B にアドバタイズされる必要があります。

どの構成を適用する必要がありますか?

A)

```
router bgp 65001
neighbor 10.0.1.2 remote-as 65002
redistribute static
```

B)

```
router bgp 65002
neighbor 10.0.1.2 remote-as 65002
network 10.0.2.0 255.255.255.0
```

ハ）

```
router bgp 65001
neighbor 10.0.1.2 remote-as 65002
network 10.0.2.0 255.255.255.0
```

D)

```
router bgp 65001
neighbor 10.0.1.2 remote-as 65002
network 10.0.1.0 255.255.255.0
```

A. オプション A

B. オプション C

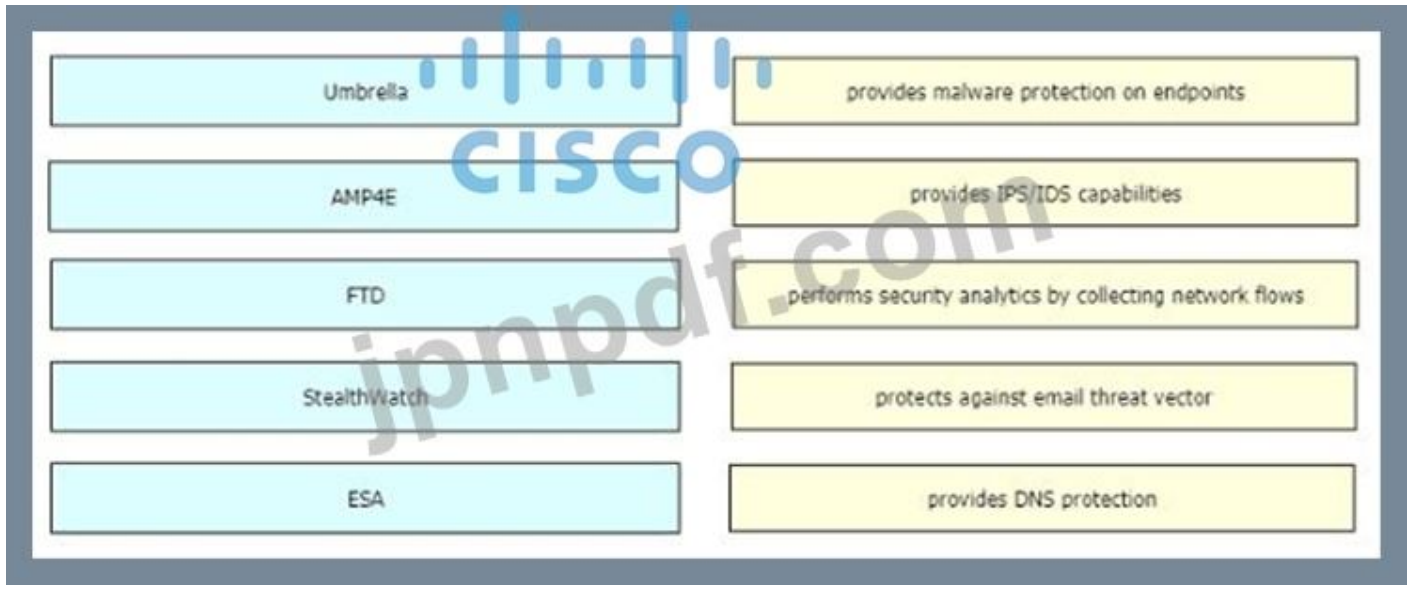
C. オプション B

D. オプション D

Answer: B (メーッセージを残す)

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

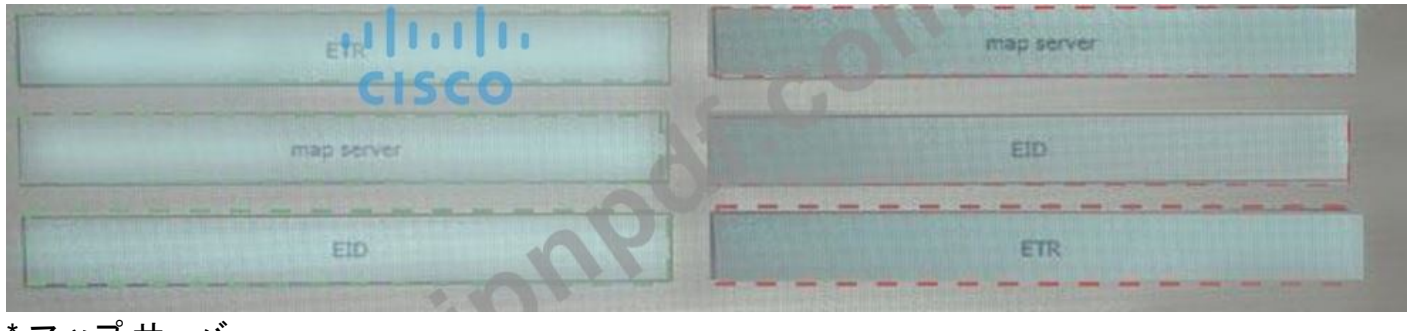
最新問題: **47**
脅威防御ソリューションを左側から右側の説明にドラッグ アンド ドロップします。



Answer:

最新問題: **48**
左側の LIPS コンポーネント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:



* マップ サーバー
* EID
*ETR

最新問題**: 49**
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: D (メーッセージを残す)
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 に基づいています。
(VXLAN)。VXLAN カプセル化は UDP ベースです。つまり、任意の IP ベースで転送できます。
ネットワーク（レガシーまたはサード パーティ）を作成し、SD-Access ファブリックのオーバーレイ ネットワークを作成します。それでも
LISP は SD-Access ファブリックのコントロール プレーンであり、LISP データ カプセル化を使用しません。
データプレーン; 代わりに、VXLAN カプセル化を使用します。
MAC-in-IP カプセル化を実行するために元のイーサネット ヘッダーを使用しますが、LISP はそうではありません。VXLAN の使用
SD-Access ファブリックがレイヤ 2 およびレイヤ 3 仮想トポロジ（オーバーレイ）をサポートできるようにします。
組み込みのネットワーク セグメンテーション (VRF) を備えた任意の IP ベースのネットワーク上で動作する機能
インスタンス/VN) および組み込みのグループベースのポリシー。

最新問題**: 50**
NTP を実装するときに使用できるセキュリティ機能はどれですか? (2つ選択)
A. 対称サーバーのパスワード
B. ドックオフセット認証
C. ブロードキャスト アソシエーション モード

D. 暗号化された認証メカニズム
E. アクセス リスト ベースの制限スキーム
Answer: D,E (メーッセージを残す**)**
マシンに保存されている時間は重要なリソースであり、NTP のセキュリティ機能を使用して、偶発的または悪意による不正確な時間の設定を回避することを強くお勧めします。利用可能な 2 つのセキュリティ機能は、アクセス リスト ベースの制限方式と暗号化された認証メカニズムです。
参照：
https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html

最新問題**: 51**
RSPAN セッション構成について正しい説明はどれですか?
A. RSPAN リージョン用に構成されたフィッター mutt
B. 着信トラフィックのみを監視できます
C. 一度に 1 つのセッションのみを構成できます
D. RSPAN 宛先として特別な VLAN タイプを使用する必要があります。
Answer: B (メーッセージを残す**)**

最新問題**: 52**
NTP が認証に使用する暗号化ハッシュ アルゴリズムはどれですか?
A. SSL
B. MD5
C. AES128
D. AES256
Answer: (解答を表示する**)**
NTP 認証の設定例を以下に示します。
Router1(config)#ntp authentication-key 2 md5 itexamanswers Router1(config)#ntp authenticate Router1(config)#ntp trusted-key 2

最新問題**: 53**
Protocol Independent Multicast はどのように機能しますか?
A. スパース モードでは、近隣の隣接関係を確立し、5 秒間隔で hello メッセージを送信します。
B. マルチキャスト ルーティング テーブルを使用して、マルチキャスト転送機能を実行します。
C. ユニキャスト経路情報を使用してマルチキャスト転送機能を実行します。
D. ブロードキャスト経路情報を使用して、マルチキャスト転送機能を実行します。
Answer: (解答を表示する**)**
PIM はマルチキャスト ルーティング プロトコルと呼ばれますが、実際には、完全に独立したマルチキャスト ルーティング テーブルを構築するのではなく、ユニキャスト ルーティング テーブルを使用してリバース パス フォワーディング (RPF) チェック機能を実行します。他のルーティング プロトコルとは異なり、PIM はルーター間でルーティング アップデートを送受信しません。

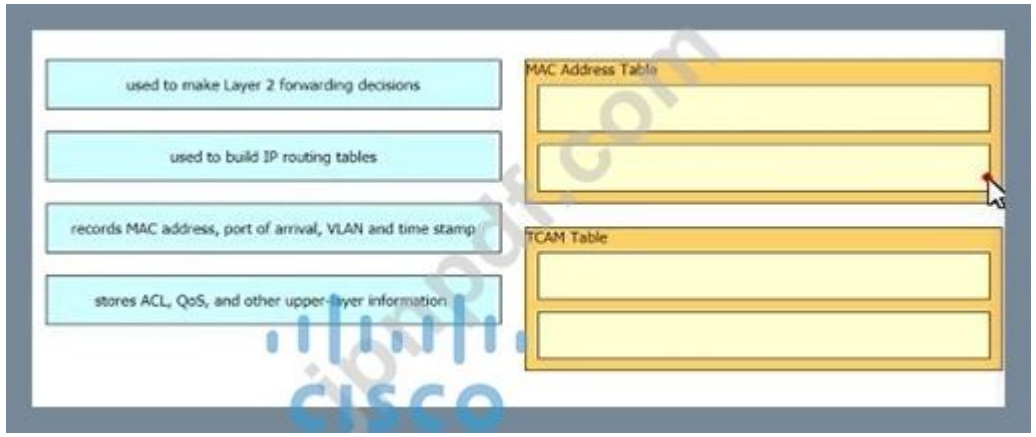
最新問題**: 54**
展示を参照してください。

```
        'Accept': 'application/yang-data+json',
        'Content-Type': 'application/yang-data+json'
    },
    data = json.dumps({
        'Cisco-IOS-XE-native:GigabitEthernet': {
            'ip': {
                'address': {
                    'primary': {
                        'address': '10.10.10.1',
                        'mask': '255.255.255.0'
                    }
                }
            }
        }
    }),
    verify = False)

# Print the HTTP response code
print('Response Code: ' + str(response.status_code))
```

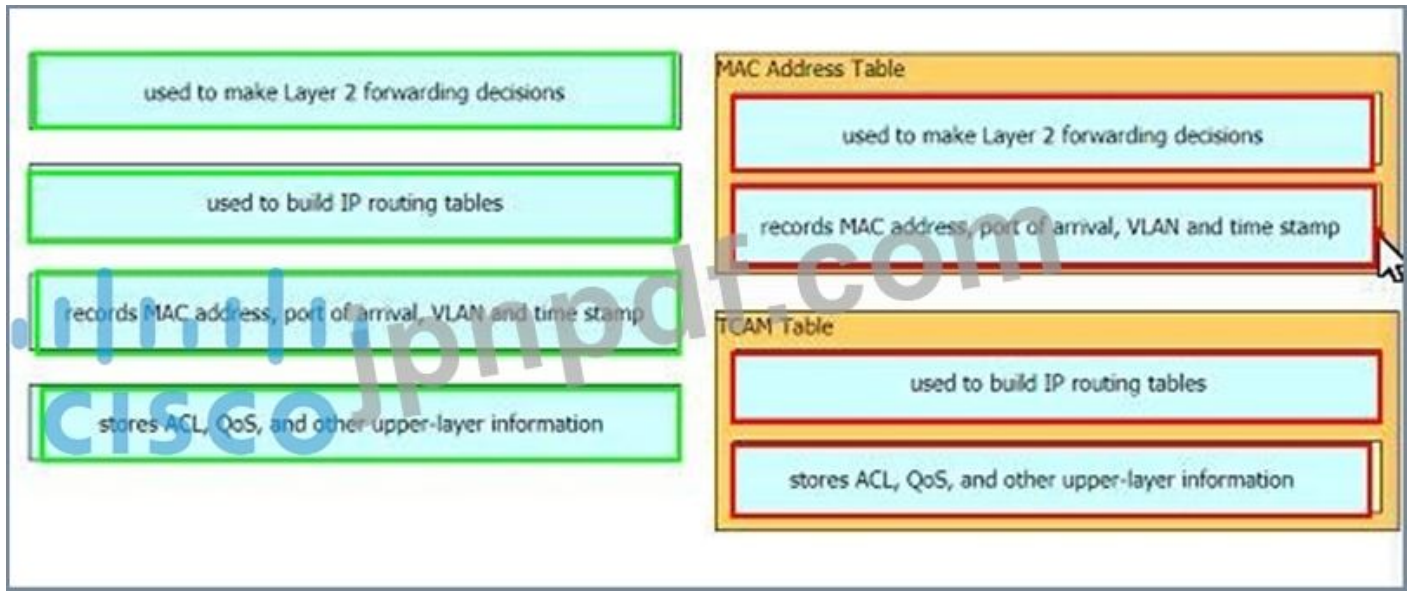
Cisco IOS-XE ルータでコードを実行すると、応答コードは 204 になります。
スクリプトの結果は何ですか？

A. 構成はクリアテキストでデバイスに正常に送信されます。
B. IP アドレス 10.10.10.1/24 で別のインターフェイスが既に構成されているため、構成は失敗します。
C. ターゲット デバイスにインターフェイス GigabitEthernet2 がないため、構成は失敗します。
D. インターフェイス GigabitEthernet2 は、IP アドレス 10.10.10.1/24 で構成されています。
Answer: D (メーッセージを残す**)**

最新問題**: 55**
左側の特性を右側のテーブル タイプにドラッグ アンド ドロップします。

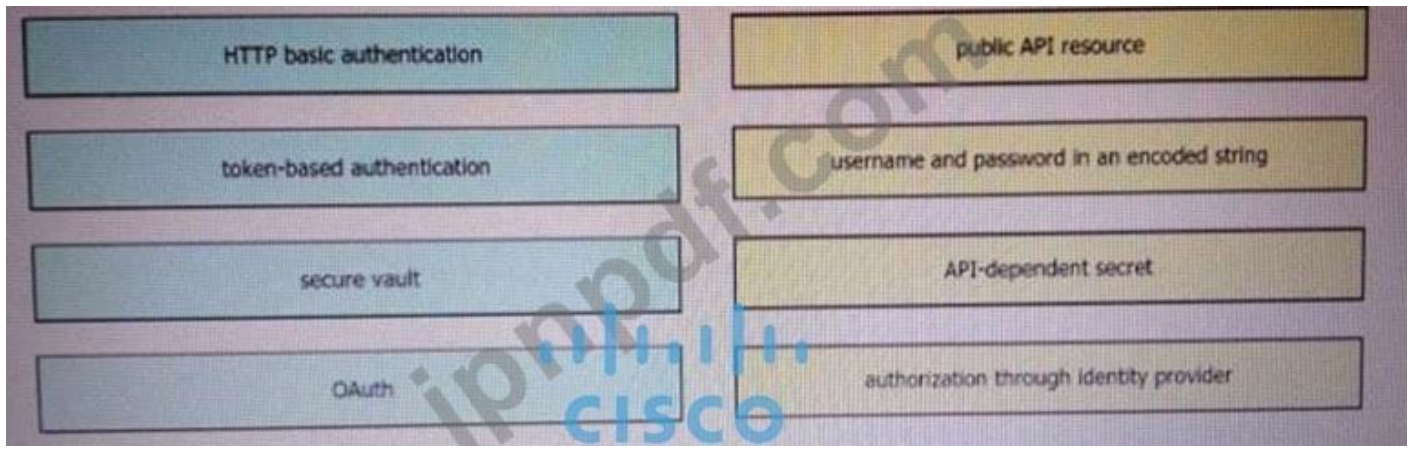


Answer:

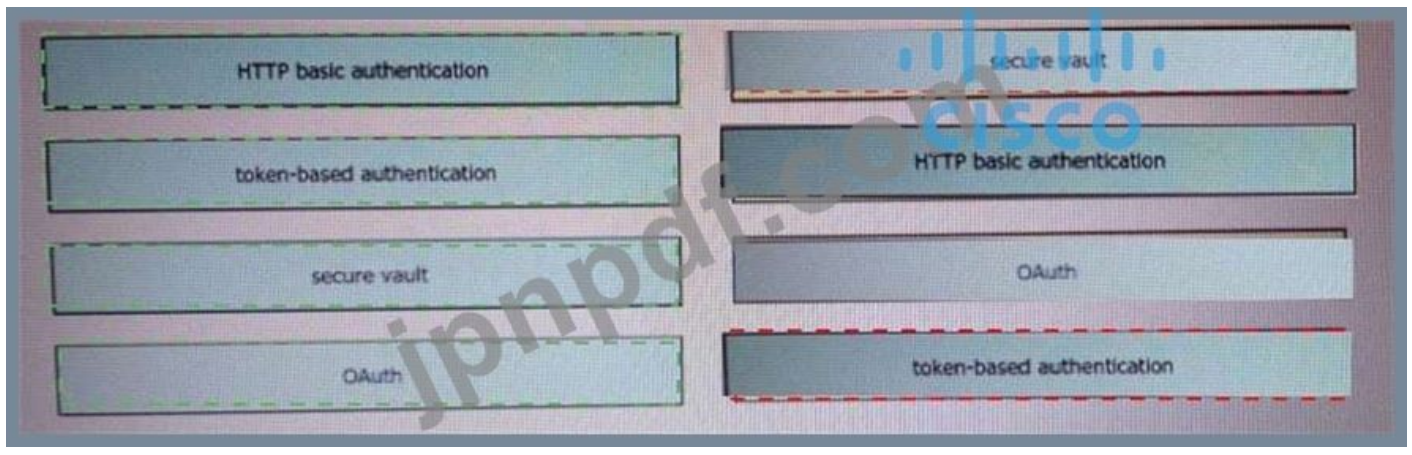


最新問題: 56

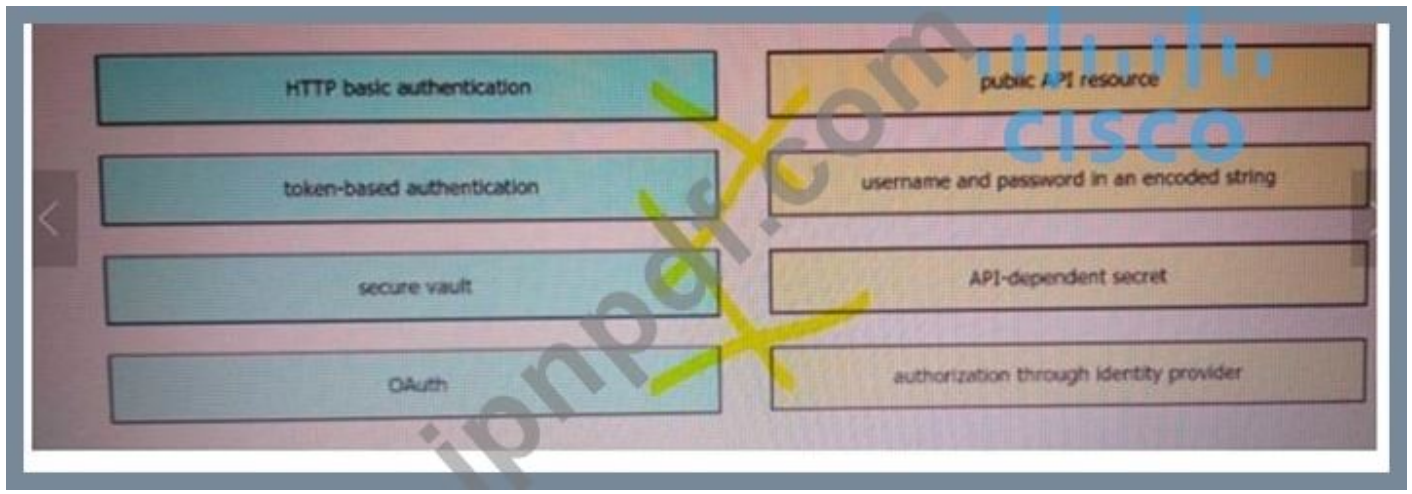
REST API の認証方法を左から右の説明にドラッグ アンド ドロップします。



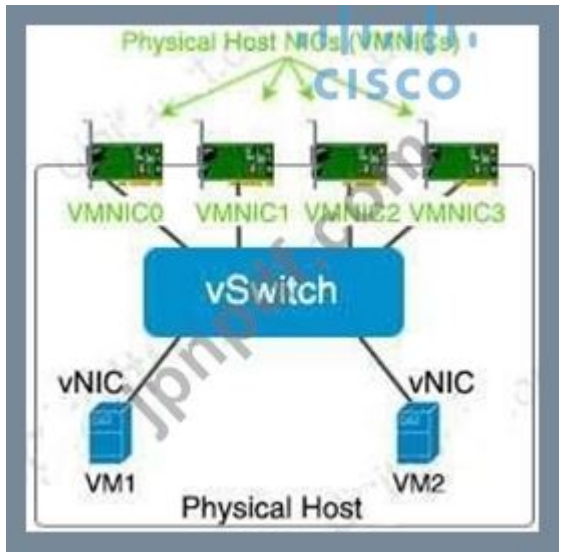
Answer:



説明

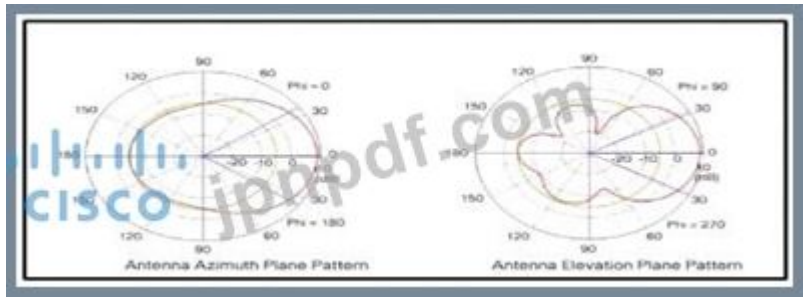


最新問題: **57**
仮想マシン環境でブロードキャスト放射が発生する理由を 2 つ挙げてください。2つ選んでください。）
A. ブロードキャスト パケットを処理するには、vSwitch がサーバーの CPU に割り込む必要があります。
B. 仮想マシン環境では、レイヤー 2 ドメインが大きくなる可能性があります。
C. 仮想マシンは主にブロードキャスト モードで通信します。
D. vSwitch とネットワーク スイッチ間の通信はブロードキャスト ベースです。
E. vSwitch とネットワーク スイッチ間の通信はマルチキャスト ベースです。
Answer: B,C (メーッセージを残す**)**
説明
ブロードキャスト放射は、コンピューター ネットワーク上のブロードキャストおよびマルチキャスト 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 ドメイン内で見られるブロードキャスト 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。そのため、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 -> VLAN を使用してブロードキャスト放射を減らす必要があります。
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への (VLAN を拡張するための) トランクの使用です。
ハイパーバイザーでの仮想化の構造に関する注意:
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 が外界へのレイヤー 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、物理スイッチに出向かなくてもレイヤー 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 から入るフレームは、VMNIC の外には出ません。
別の VMNIC カードからの物理ホスト。

最新問題: **58**
展示を参照してください。



放射パターンはどのタイプのアンテナを示していますか?
A. 双極子
B. 八木
C. パッチ
D. 無指向性
Answer: (解答を表示する**)**

最新問題: **59**
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参加し、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 グループにあり、異なる IP アドレスを持っていますが、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. イントラ VLAN
D. コントローラ内
Answer: D (メーッセージを残す**)**

モビリティ、またはローミングは、関連付けを維持するワイヤレス LAN クライアントの機能です。
あるアクセス ポイントから別のアクセス ポイントへシームレスに安全かつ最小限の遅延で
可能。一般的なクライアント ローミングの 3 つのタイプは次のとおりです。
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 クライアント ローミングをサポートします。
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。このローミングは透過的です
セッションが維持されるとクライアントに送信され、クライアントは同じものを使用し続けます
DHCP によって割り当てられた、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。
コントローラー間ローミング: 複数のコントローラー展開でクライアント ローミングをサポート
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、
同じサブネット。このローミングはクライアントに対しても透過的です。これは、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、クライアントは引き続き
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が割り当てた IP アドレス。
サブネット間ローミング: 複数のコントローラの展開でクライアントのローミングをサポート
異なる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
サブネット。セッションが維持されるため、このローミングはクライアントに対して透過的です。
コントローラ間のトンネルにより、クライアントは同じコントローラを引き続き使用できます。
セッションがアクティブである限り、DHCP によって割り当てられた、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。
参照：
4/構成/ガイド/統合/b_cg74_CONSOLIDATED/b_cg74_CONSOLID
あ
TED_chapter_01100.html
上記の 3 種類のクライアント ローミングでは、Inter-Subnet Roaming のみが
コントローラは異なるサブネットにあります。

最新問題: **60**
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確認する 2 つのコマンドはどれですか?

A. スパニング ツリー mst vlan 10,20 プライオリティ ルート

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 mst 1 プライオリティ 4096

D. スパニング ツリー mst 1 プライオリティ 1

E. スパニング ツリー mstp vlan 10,20 ルート プライマリ

Answer: B,C (メーッセージを残す)

最新問題: **61**

```
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。エンジニアが Switch1 と Switch2 の間に EtherChannel を構成していて、switch2 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、この問題を解決するアクションはどれですか?

A. Switch2 のメンバー ポートを少なく構成します。
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構成します。
C. 両方のスイッチで同じ EtherChannel プロトコルを構成します。
D. Switch1 でさらにメンバー ポートを構成します。
Answer: C (メーッセージを残す)
説明
この場合、Switch2 でネゴシエーション プロトコルなしで 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 操作用に構成されていない場合、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、そのループの発生を防止しようとします。

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **62**
特性を左側から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

クラウド6,2,5 : オンプレミス4,3,1

最新問題: **63**

SD-WAN コントローラーと SD-WAN エンドポイント間のコントロール プレーン トラフィックを暗号化するために使用されるプロトコルはどれですか?

A. DTLS

B. IPsec

C. PGP

D. HTTPS

Answer: (解答を表示する**)**

DTLS プロトコルは、vSmart (コントローラー) と他の SD-WAN エンドポイント間のコントロール プレーン トラフィックを暗号化するために使用されます。

最新問題: **64**

ある企業は、キャンパス インフラストラクチャにインテントベース ネットワーキングを実装することを計画しています。従来のキャンパス デザインからプログラマー ファブリック デザイナーに移行するのはどのデザイン ファシリティですか?

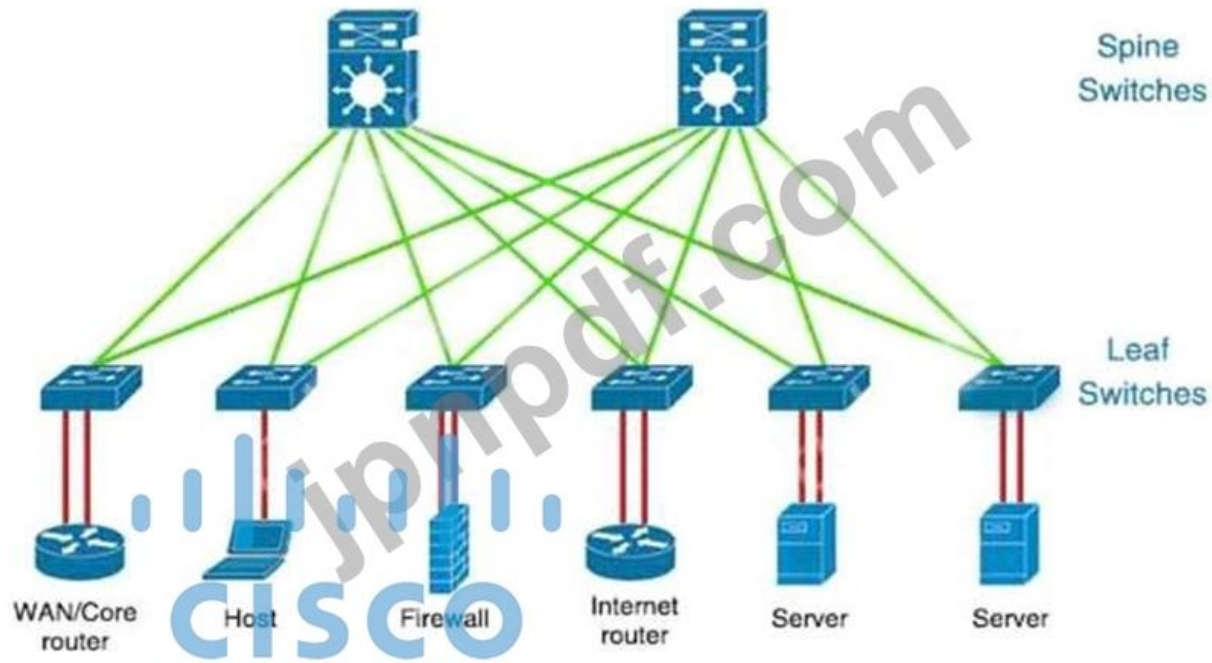
A. レイヤー 2 アクセス

B. 三段

C. 2段

D. ルーテッド アクセス

Answer: C (メーッセージを残す)
説明
Intent-based Networking (IBN) は、ハードウェア中心の手動ネットワークをコントローラー主導のネットワークに変換します。これは、ビジネスの意図を取り込み、それを自動化してネットワーク全体に一貫して適用できるポリシーに変換します。ネットワークの目標は、ネットワーク パフォーマンスを継続的に監視および調整して、望ましいビジネス成果を保証することです。IBN はソフトウェア定義ネットワーキング (SDN) に基づいています。SDN は通常、スパイン リーフ アーキテクチャを使用します。これは通常、スパイン (アグリゲーション レイヤーなど) とリーフ (アクセス レイヤーなど) の 2 つのレイヤーとして展開されます。

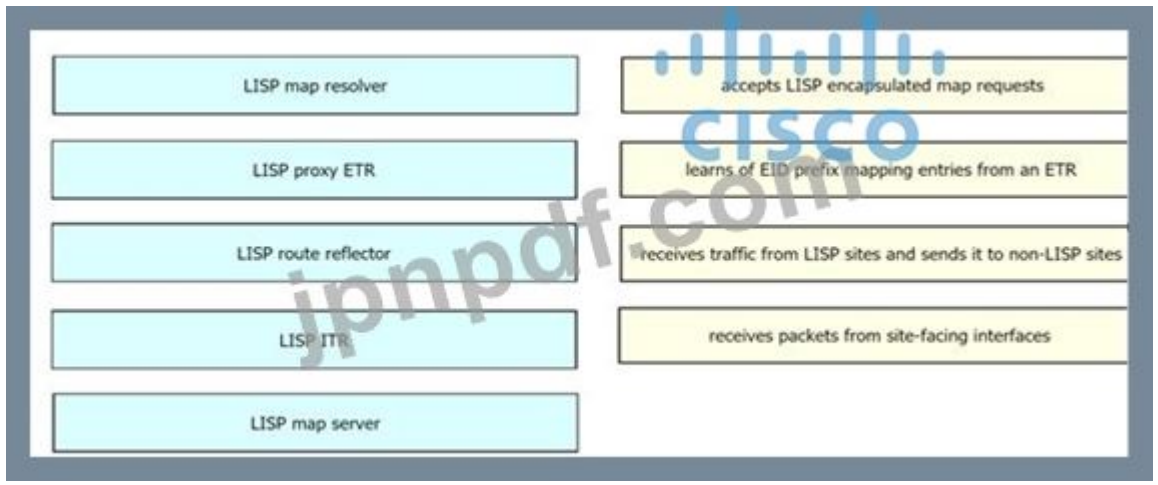


最新問題: **65**
VXLAN がレイヤー 2 およびレイヤー 3 トラフィックのセグメンテーションを提供するために使用するテクノロジーはどれですか?
A. VRF
B. VNI
C. VLAN
D. ブリッジ ドメイン
Answer: (解答を表示する)

最新問題: **66**
エンジニアは、パケット間の遅延変動に敏感な新しいアプリケーションの展開に関心を持っています。ルータをジッタ測定の宛先に設定するコマンドはどれですか?
A. Router(config)# ip sla Responder tcp-echo 172.29.139.134 5000
B. Router(config)# ip sla Responder tcp-connect 172.29.139.134 5000
C. Router(config)# ip sla Responder udp-connect 172.29.139.134 5000
D. Router(config)# ip sla Responder udp-echo 172.29.139.134 5000
Answer: D (メーッセージを残す)

最新問題: **67**

LISP コンポーネントを左側から右側の機能にドラッグ 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 カプセル化されたマップ要求を受け入れます: LISP マップ リゾルバー
+ ETR からの EID プレフィックス マッピング エントリの学習: 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: LISP プロキシ ETR
+ サイトに面した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 Egress Tunnel Router (ETR) の RLOC の宛先 IP アドレスを持つ追加のヘッダーを使用して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 カプセル化パケットを受信し、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ので、「map-server」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 LISP 以外のサイトにトラフィックを送信する必要がある場合に使用されますが、パケット ソースとしてルーティング可能な EID を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ます。PETR は ETR と同じように機能しますが、非 LISP サイトの宛先にトラフィックを送信する EID に対して機能します。

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、定期的に Map-Register メッセージを構成済みのすべてのマップ サーバーに送信します。

Map Resolver (MR): 通常は ITR からの LISP Encapsulated Map Request 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**
ワイヤレス クライアントが 2 つの異なるワイヤレス コントローラ間をローミングすると、ネットワーク接続が一定期間停止します。この問題の原因となる構成の問題はどれですか?
A. モビリティ グループ内のすべてのコントローラが同じ仮想インターフェイス IP アドレスを使用しています。
B. モビリティ グループ内のすべてのコントローラが同じモビリティ グループ名を使用しています。
C. モビリティ グループ内のすべてのコントローラが同じ仮想インターフェイス IP アドレスを使用しているわけではありません。
D. モビリティ グループ内のすべてのコントローラが同じモビリティ グループ名を使用しているわけではありません。
Answer: D (メーッセージを残す**)**

最新問題: **69**
無線、アンテナ ケーブル、およびアンテナを通過した後の信号の放射電力を測定するために使用される計算は何ですか?
A. EIRP
B. mW
C. dBm
D. dBi
Answer: A (メーッセージを残す**)**
送信機の電力レベル、ケーブルの長さ、およびアンテナ ゲインの完全な組み合わせがわかれば、アンテナから放射される実際の電力レベルを把握できます。これは、実効等方性放射電力 (EIRP) として知られており、dBm で測定されます。
EIRP は、ほとんどの国の政府機関によって規制されているため、非常に重要なパラメーターです。このような場合、システムは最大許容 EIRP を超える信号を放射できません。システムの EIRP を求めるには、送信機の電力レベルをアンテナ ゲインに加算し、ケーブル損失を差し引くだけです。
送信機が 10 dBm (10 mW) の電力レベルに設定されているとします。損失が 5 dB のケーブルは、送信機をゲインが 8 dBi のアンテナに接続します。システムの結果の EIRP は、10 dBm - 5 dB + 8 dBi、つまり 13 dBm です。
EIRP は、デシベル ミリワット (dBm)、等方性アンテナに対する dB (dBi)、およびデシベル (dB) の値で構成されていることに気付くかもしれません。単位が異なっているように見えますが、それらはすべて dB の 「ドメイン」にあるため、安全に組み合わせることができます。

最新問題: **70**
エンジニアは、最初に AAA サーバをチェックしてからローカル ユーザ名をチェックする EXEC 許可リストを設定する必要があります。両方の方法が失敗した場合、ユーザーは拒否されます。どの構成を適用する必要がありますか?
A. aaa 承認 exec デフォルト グループ 半径 ローカル
B. aaa 承認 exec デフォルト ローカル グループ 半径 なし
C. aaa 承認 exec デフォルト ローカル グループ tacacs+
D. aaa 承認 exec デフォルト グループ 半径 ローカル なし
Answer: A (メーッセージを残す**)**

最新問題: **71**
デフォルトで、HSRP グループ 15 が使用する仮想 MAC アドレスはどれですか?
A. 05:5e:ac:07:0c:0f
B. c0:42:34:03:73:0f
C. 00:00:0c:07:ac:0f

D. 05:af:1c:0f:ac:15
Answer: C (メーッセージを残す**)**
説明
インターフェイス Ethernet0/0.100
カプセル化 dot1Q 100
IP アドレス 10.0.111.1 255.255.255.0
スタンバイ 15 IP 10.0.111.254
!
cisco(config-subif)#do s stand
Ethernet0/0.100 - グループ 15
状態は話す
仮想 IP アドレスは 10.0.111.254 です
アクティブな仮想 MAC アドレスが不明です
ローカル仮想 MAC アドレスは 0000.0c07.ac0f (v1 デフォルト)
ハロータイム3秒、ホールドタイム10秒
次の hello は 1.200 秒で送信されます
プリエンプション無効
アクティブなルーターが不明です
スタンバイ ルータが不明です

最新問題**: 72**
この EEM アプレット イベントは何を達成しますか?
 Event snmp oid 1.3.6.1.3.7.1.5.1.2.4.2.9 get-type next entry-op g
entry-val 75 ポーリング間隔 5"
A. 5 回のポーリング サイクルで値が 75% を超えた場合にメールを発行します。
B. SNMP 変数を読み取り、値が 75% を超えるとアクション GO をトリガーします。
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**)**
EEM は、イベントを監視し、監視対象のイベントが発生したり、しきい値に達したときに、情報提供または修正措置を講じる機能を提供します。EEM ポリシーは、イベントと、そのイベントが発生したとき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、アプレットまたはスクリプトの 2 種類があります。アプレットは、CLI 構成内で定義される単純な形式のポリシーです。
Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)オブジェクト識別子の値をサンプリングして実行される Embedded Event Manager (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 {exact | 次の} entry-op 演算子 entry-val エントリ値 [exit-comb {または | and}] [exit-op operator] [exit-val exit-value] [exit-time exit-time-value] poll-interval poll-int-value
+ 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 get 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 の内容をエントリ値と比較します。一致した場合、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: 現在のオブジェクト ID の内容を比較して、SNMP イベントを発生させるかどうかを決定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。一致した場合、イベントがトリガーされ、イベント監視が再度有効になります。
+ poll-interval: 連続するポーリング間の時間間隔を指定します (秒単位)。

最新問題**: 73**
ルーターが 100 kbps を受け入れる SSH の量を制限する構成はどれですか?
A)

B)

ハ)

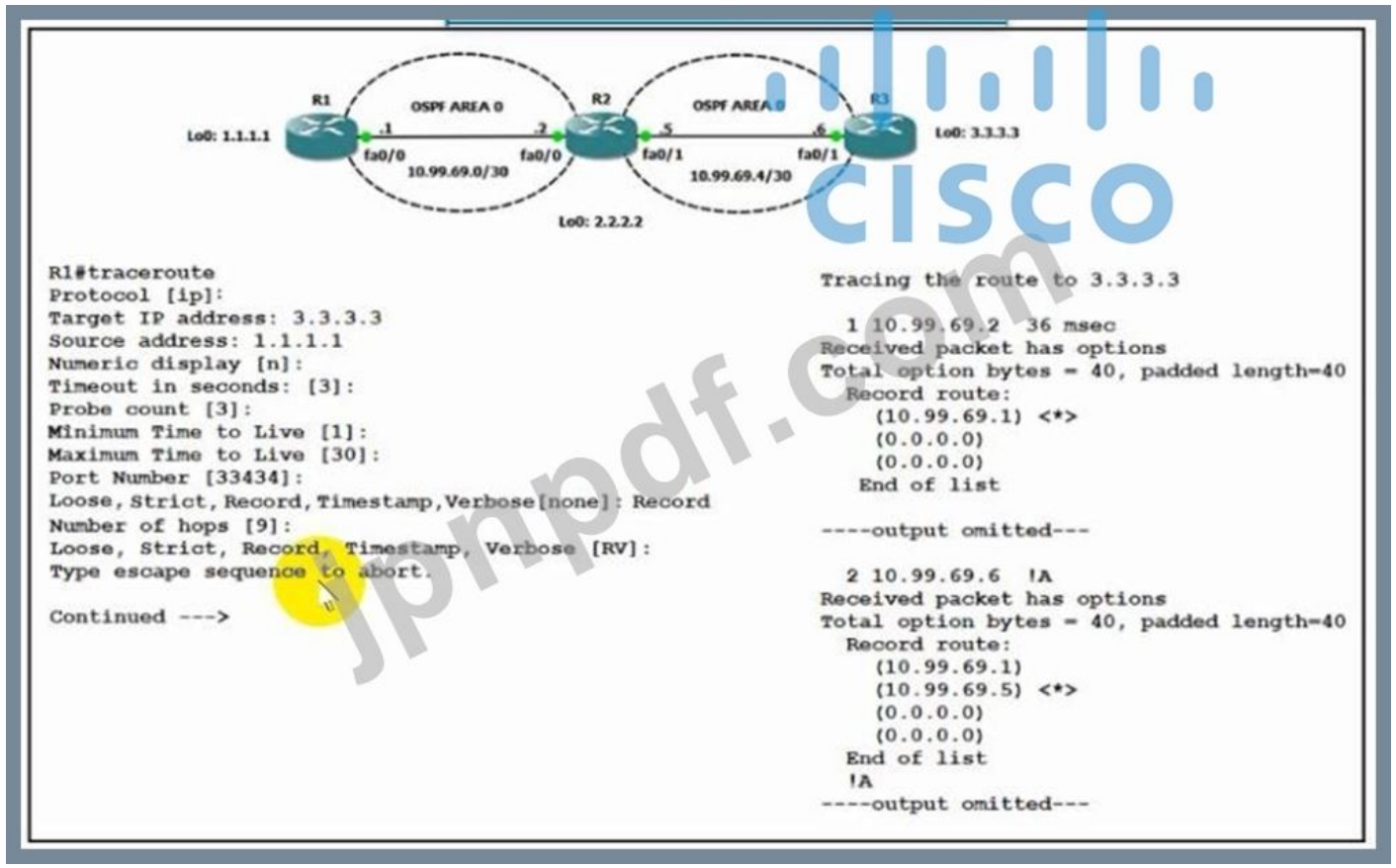
D)

A. オプション A

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

最新問題**: 74**
顧客はいくつかの小さな支店を持っており、CAPWAP を使用してローカル管理を行う WI-FI ソリューションを導入したいと考えています。
この要件を満たす展開モデルはどれですか?
A. 自律型
B. モビリティエクスプレス
C. SD-Access ワイヤレス
D. ローカルモード
Answer: B (メーッセージを残す**)**
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、専用の WLC に投資したくない小規模から中規模の、またはマルチサイト 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 個の AP をサポートできます。Mobility Express WLC はまた、CAPWAP を使用して他の AP と通信します。
注: ローカル モードは、AP が動作する最も一般的なモードです。これはデフォルト モードでもあります。ローカル モードでは、LAP は関連するコントローラへの CAPWAP (または LWAPP) トンネルを維持します。

最新問題**: 75**
展示を参照してください。

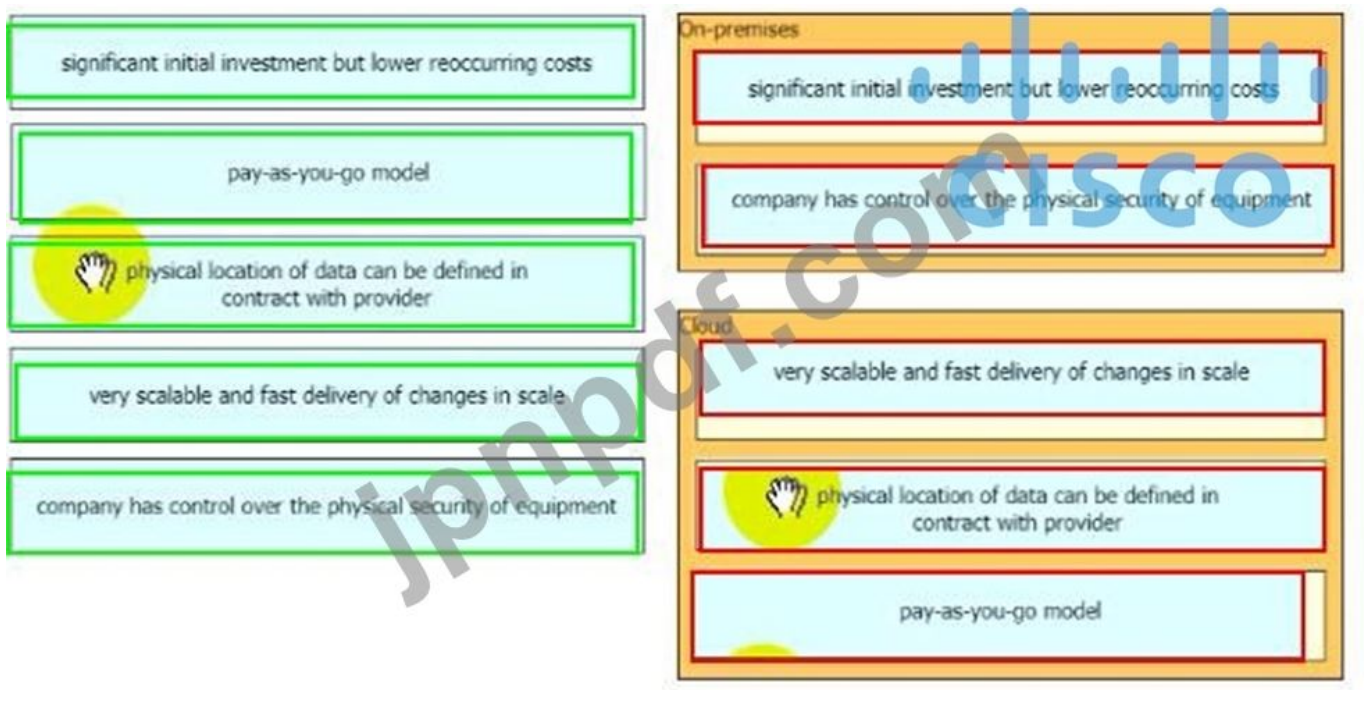


R1 から R3 への traceroute が失敗します。失敗の原因は何ですか？

A. R3 の fa0/1 に Inbound が適用された ACL がトラフィックをドロップしています。
B. R3 のループバックはシャットダウン状態です。
C. R2 の loopback0 にインバウンドに適用された ACL がトラフィックをドロップしています。
D. 接続経路の OSPF への再分配は設定されていません。
Answer: A (メーッセージを残す)

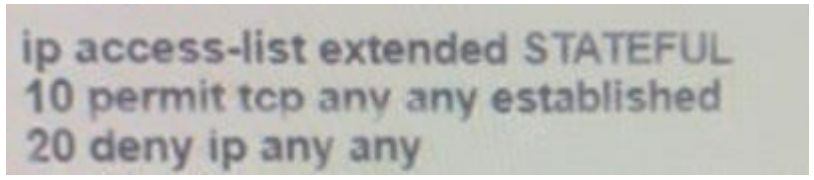
最新問題**: 76**
特性を左側から右側の適切なインフラストラクチャ展開タイプにドラッグ アンド ドロップします。

Answer:



有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361**30%OFF問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **77**
このアクセス制御リストを適用した結果は?



A. URG ビットが設定された TCP トラフィックが許可されます
B. SYN ビットが設定された TCP トラフィックが許可されます
C. ACK ビットが設定された TCP トラフィックが許可されます
D. DF ビットが設定された TCP トラフィックが許可されます
Answer: C (メーッセージを残す**)**
説明
確立されたキーワードは、ACK および/または RST 制御ビットが設定された TCP セグメントに一致する TCP アクセス リスト エントリにのみ適用されます（送信元ポートと宛先ポートに関係なく）。これは、TCP 接続が一方向のみですでに確立されていることを前提としています。. 以下の例を見てみましょう。

社内のホストに外部サーバーへの telnet を許可したいだけで、その逆は許可したくない場合は、次のように 確立された」アクセス リストを使用できます。tcp any any eq telnet ! インターフェイス S0/0 ip access-group 100 in ip access-group 101 out

最新問題: **78**
Cisco SD-Access ソリューションで、拡張ノードが単一のエッジ ノードに接続するために使用するプロトコルはどれですか?
A. VXLAN
B. CTS
C. 802 1Q
D. IS-IS
Answer: A (メーッセージを残す**)**

最新問題: **79**
展示を参照してください。

```
import json
from requests import get

Headers = { "Content-Type" : "application/yang-data+json",
            "Accept" : "application/yang-data+json" }

Devices = open("devices.txt", "r")

for Device in Devices.readlines():
  Hostname, IP, Login, Pass = Device.strip().split(",")
  URL = f"https://{IP}/restconf/data/Cisco-IOS-XE-native:native"
  Creds = (Login, Pass)
  Response = get(URL, auth = Creds, headers = Headers, verify = False)
```

各デバイス構成が JSON 形式のファイルにデバイス名で保存されるようにするには、スクリプトをどのように完成させる必要がありますか?

A)

Insert after the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
  OutFile.write(Response)
```

B)

Insert after the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
  OutFile.write(json.dumps(Response.text))
```

ハ)

Append to the body of the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
  OutFile.write(Response.text)
```

D)

Insert immediately before the for loop:

```
with open(f"{Hostname}.json", "w") as OutFile:
  OutFile.write(json.load(Devices))
```

A. オプション

B. オプション

C. オプション

D. オプション

Answer: C (メーッセージを残す**)**

最新問題: **80**
管理者は、認証のためにルーターのユーザー名とパスワードのデータベースを使用して、ルーター X への Telnet アクセス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)

```
RouterX(config)# line aux 0
RouterX(config-line)# password cisco
RouterX(config-line)# login
```

B)

```
RouterX(config)# aaa new-model
RouterX(config)# aaa authentication login auth-list local
```

ハ）

```
RouterX(config)# line vty 0 4
RouterX(config-line)# login local
RouterX(config-line)# end
```

D)

```
RouterX(config)# line vty 0 4
RouterX(config-line)# login
RouterX(config-line)# end
```

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: D (メーッセージを残す)

最新問題: **81**
AMP4E がブロックできる 2 つの脅威はどれですか? 2つ選んでください。）
A. SQL インジェクション
B. メール フィッシング
C. Microsoft Word マクロ攻撃
D. ランサムウェア
E. DDoS
Answer: B,D (メーッセージを残す)

最新問題: **82**
Cisco EAP-FAST に関する事実とは?
A. RADIUS サーバー証明書は必要ありません。
B. クライアント証明書が必要です。
C. IETF 規格です。
D. 透過モードで動作します。
Answer: (解答を表示する)
説明
EAP-FAST is also designed for simplicity of deployment since it does not require a certificate on the wireless LAN client or on the RADIUS infrastructure yet incorporates a built-in provisioning mechanism.
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-fixed/72788-CSSC-Deployment-Guide.h

最新問題: **83**
展示を参照してください。

```
flow monitor FLOW-MONITOR-1
 record netflow ipv6 original-input
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!
```

ルーターの Flexible NetFlow 構成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. 完全な NetFlow に必要な量と比較すると、CPU とメモリの使用率が低下します。
B. コレクターへの NetFlow 更新は、50% 少ない頻度で送信されます。
C. サンプリング データの解像度は上がりますが、ルーターのパフォーマンスがさらに必要になります。
D. IPv4 パケットは毎秒検査のためにコレクタに転送されます。
Answer: A (メーッセージを残す**)**

最新問題: **84**
Cisco SD アクセス ファブリックの推奨 MTU サイズはどれくらいですか?
A. 4464
B. 1500
C. 17914
D. 9100
Answer: (解答を表示する**)**

最新問題: **85**
展示を参照してください。エンジニアは、show process cpu sorted コマンドの出力をファイルに追加するスクリプトを作成する必要があります。
A. アクション 4.0 publish-event "show process cpu sorted | append flash:high-cpu-file"
B. アクション 4.0 syslog コマンド 「show process cpu sorted | append flash:high-cpu-file」
C. アクション 4.0 cli コマンド 「show process cpu sorted | append flash:high-cpu-file」
D. アクション 4.0 ens-event "show process cpu sorted | append flash:high-cpu-file"
Answer: C (メーッセージを残す**)**

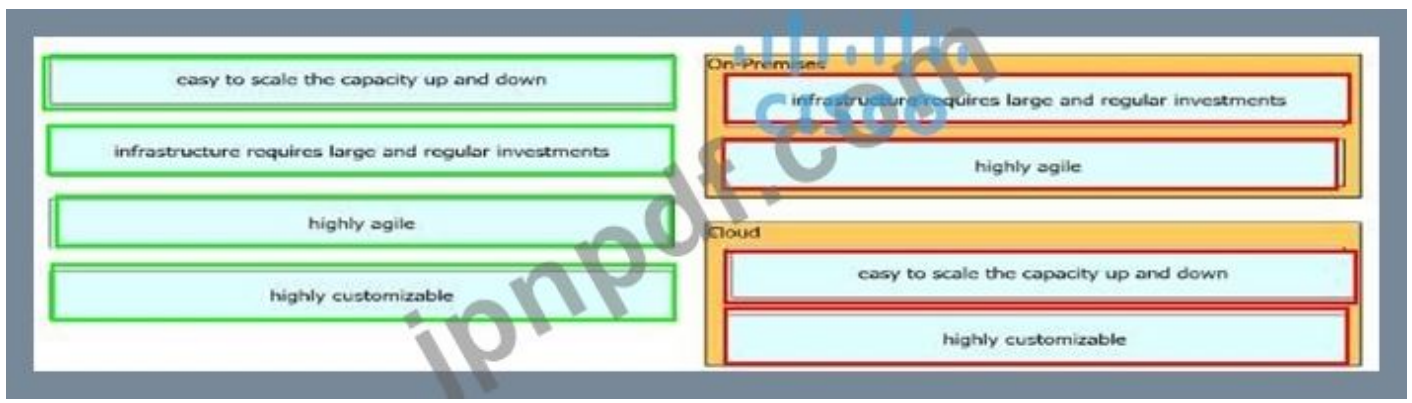
最新問題: **86**
複数の PIM-SM ドメインを相互接続するために MSDP をどのように使用しますか?
A. MSDP メッセージは、ドメイン内のアクティブなソースをアドバタイズするために使用されます
B. SDP は、ランデブー ポイントがドメイン外のアクティブなソースを動的に検出できるようにします。
C. MSDP は、ドメイン間操作のために BGP またはマルチプロトコル BGP に依存します。
D. MSDP SA 要求メッセージは、特定のグループのアクティブ ソースのリストを要求するために使用されます。
Answer: (解答を表示する**)**

最新問題: **87**
展示を参照してください。

PE3 で新しい VRF を作成しました。デバッグを有効にしました
ip bgp vpnv4 ユニキャストは PE1 で更新され、デバッグでルートを確認できますが、BGP VPNv4 テーブルでは確認できません。正しい2つのステートメントはどれですか? (2つ選んでください)
A. PE1 の VRF にルート ターゲット インポート 999:999 を設定すると、ルートが受け入れられます。
B. PE1 と PE3 の間で VPNv4 が構成されていない
C. address-family ipv4 vrf が PE3 で構成されていません
D. 自動経路フィルタリングにより、PE1 は経路を拒否します。
E. PE3 の VRF にルート ターゲット インポート 999:999 を設定すると、ルートが受け入れられます。
Answer: (解答を表示する**)**
要件は、ルータがこの情報をメモリに保持する必要がないように、PE ルータへの入口で MP-iBGP アップデートをフィルタリングできることです。
自動ルート フィルタリング機能は、このフィルタリング要件を満たします。この機能は、すべての PE ルーターでデフォルトで利用可能であり、有効にするために追加の構成は必要ありません。その機能は、PE の設定済み VRF のいずれとも一致しないルート ターゲット拡張コミュニティを含む VPN-IPv4 ルートを自動的にフィルタリングすることです。これにより、不要な VPN-IPv4 ルートがサイレントに効果的に破棄されるため、PE がメモリに格納する必要がある情報の量が削減されます -> 回答「自動ルート フィルタリングにより、PE1 はルートを拒否します」が正解です。
参照：
PE1 がルートをドロップした理由は、PE1 に「route-target import 999:999」コマンドがないためです (そのため、デバッグで「DENIED due to: extended community not supported」が表示されます)。このコマンドを入力して、このルートを受け入れる -> 「PE1 の VRF にルート ターゲット インポート 999:999 を設定すると、ルートが受け入れられる」という回答が正解です。

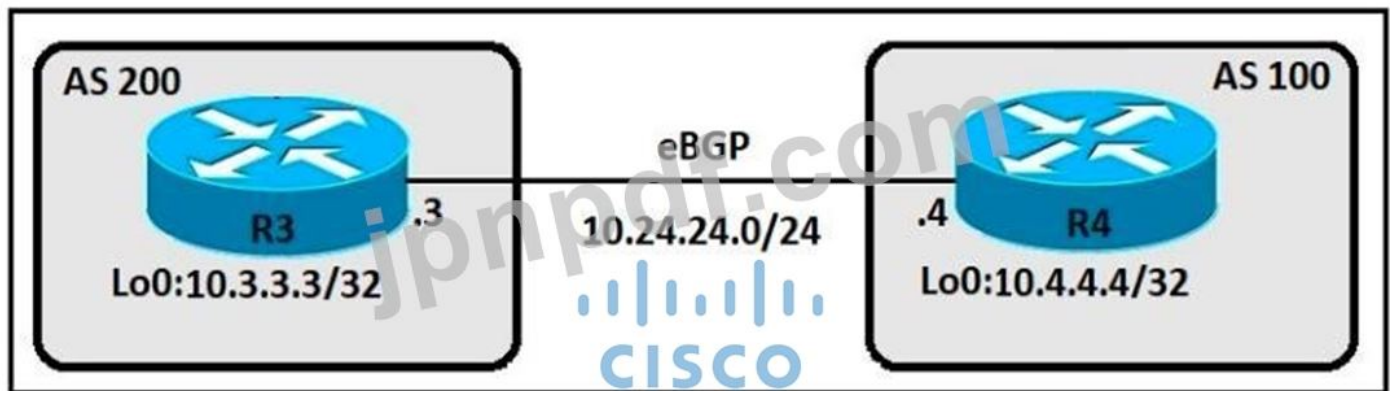
最新問題: **88**
特性を左側から、右側に記述されているインフラストラクチャ展開モデルにドラッグ アンド ドロップします。

Answer:



最新問題**: 89**

展示を参照してください。



エンジニアは、ルーター R3 とルーター R4 の間に eBGP ピアリングを確立する必要があります。両方のルーターは、ループバック インターフェイスを BGP ルーター ID として使用する必要があります。このタスクを実行する構成セットはどれですか?

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

最新問題**: 90**
展示を参照してください。

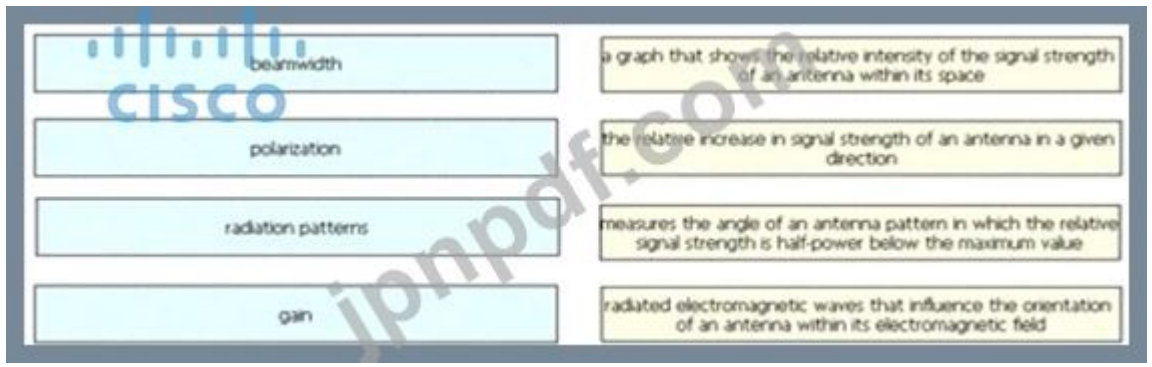
展示でコードを実行した後。NETCONF サーバーが NETCONF クライアントに返すデータの量を、インターフェイスの構成のみに減らす手順はどれですか?
A. JSON フィルターを文字列として作成し、それを get_config() メソッドに引数として渡します。
B. txml ライブラリを使用して、インターフェイスの構成のために NETCONF サーバーから返されたデータを解析します。
C. XML フィルタを文字列として作成し、get_config() メソッドに引数として渡します。
D. JSON ライブラリを使用して、インターフェイスの構成のために NETCONF サーバーから返されたデータを解析します。
Answer: C (メーッセージを残す**)**

最新問題**: 91**
タイプ 1 ハイパーバイザー上の仮想マシンの IP と MAC の割り当て要件を説明しているのはどれですか?
A. 各仮想マシンには一意の IP アドレスが必要ですが、MAC アドレスは物理サーバーと共有されます。
B. 各仮想マシンには一意の MAC アドレスが必要ですが、IP アドレスは物理サーバーと共有されます。
C. 仮想マシンは一意の IP または一意の MAC を必要としません。これらは、物理サーバーの IP アドレスと MAC アドレスを共有します。
D. 各仮想マシンには、他のノードに到達できるようにするための一意の IP アドレスと MAC アドレスが必要です。
Answer: D (メーッセージを残す**)**

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**36130%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **92**

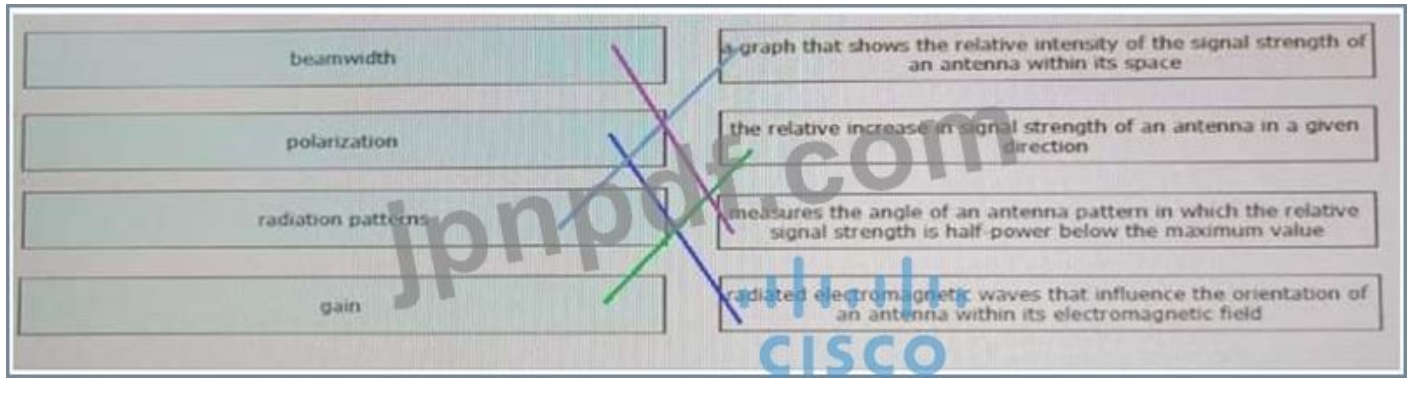
左側のワイヤレス要素を右側の定義にドラッグ アンド ドロップします。



Answer:

説明

チャート、折れ線グラフ 説明自動生成

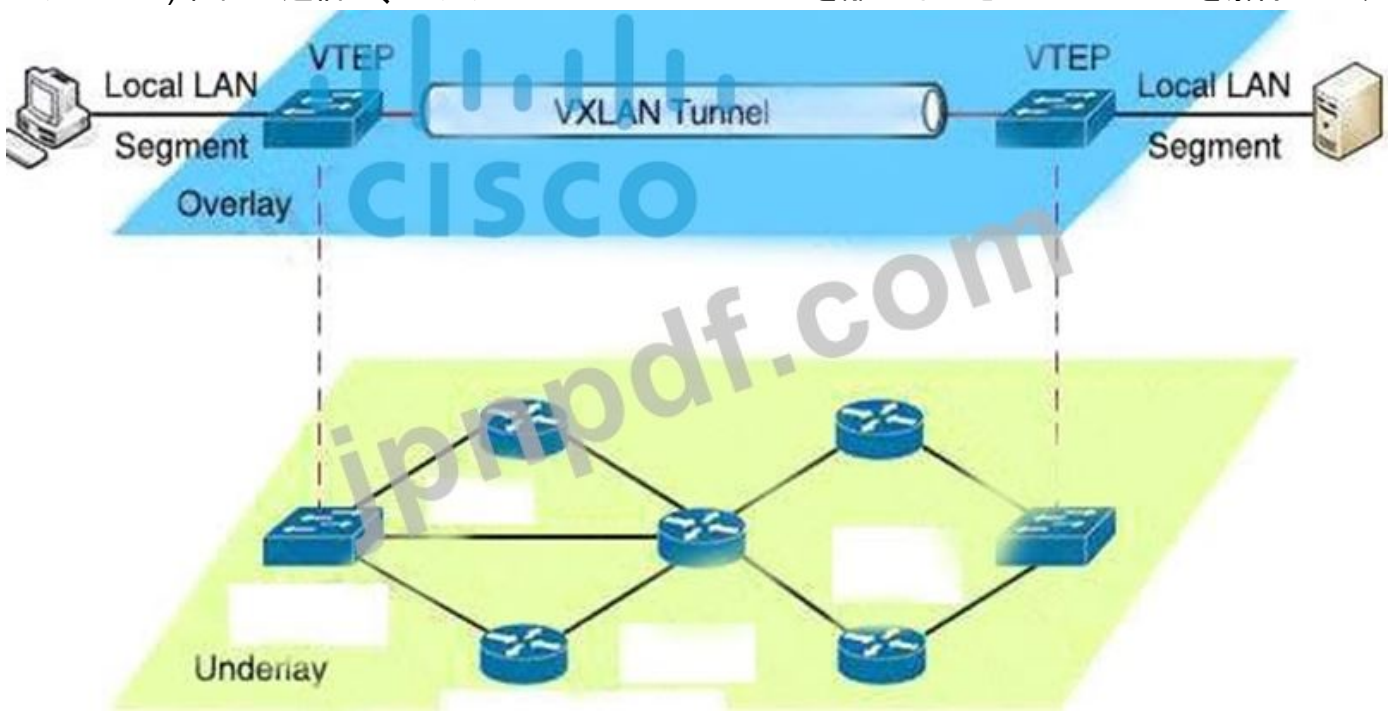


最新問題: **93**

VXLAN の VTEP の機能はどれですか?

A. IPv6 から IPv4 VXLAN へのトンネリング トラフィック

B. ローカル VXLAN イーサネット セグメントで暗号化通信を許可する
C. 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
D. IPv4 から IPv6 VXLAN へのトンネリング トラフィック
Answer: C (メーッセージを残す**)**
説明
VTEP はオーバーレイ ネットワークとアンダーレイ ネットワークの間を接続し、フレームを VXLAN パケットにカプセル化して IP ネットワーク (アンダーレイ) 経由で送信し、パケットが VXLAN トンネルを離れるときにカプセル化を解除します。
VTEP はオーバーレイ ネットワークとアンダーレイ ネットワークの間を接続し、フレームを VXLAN パケットにカプセル化して IP ネットワーク (アンダーレイ) 経由で送信し、パケットが VXLAN トンネルを離れるときにカプセル化を解除します。



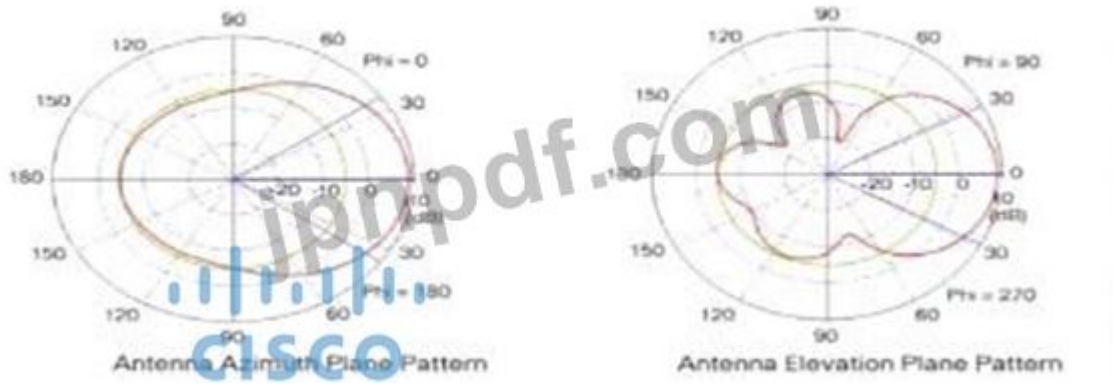
最新問題**: 94**
展示を参照してください。

これらのコマンドは、スイッチの構成に追加されました。この構成に追加された場合、どのコマンドがエラーのフラグを立てますか?
A. セッション 1 ソース vlan 10 を監視します。
B. セッション 1 ソース インターフェイス ポート チャネル 7、ポート チャネル 8 を監視します。
C. セッション 1 のソース インターフェイス ポート チャネル 6 を監視します。

D. セッション 1 のソース インターフェイス FatEtheret0/1 x を監視します。
Answer: A (メーッセージを残す**)**

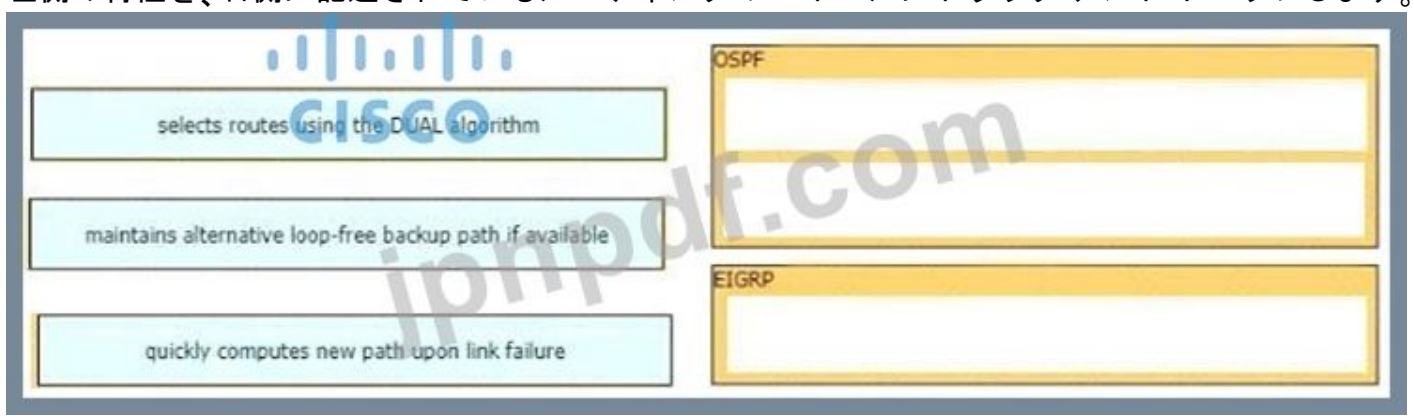
最新問題**: 95**
Cisco SD-Access アーキテクチャでレイヤ 2 およびレイヤ 3 論理ネットワークを提供するために使用されるテクノロジーはどれですか?
A. 簡単な仮想ネットワーク
B. オーバーレイ ネットワーク
C. アンダーレイ ネットワーク
D. VPN ルーティング/転送
Answer: B (メーッセージを残す**)**

最新問題**: 96**
展示を参照してください。

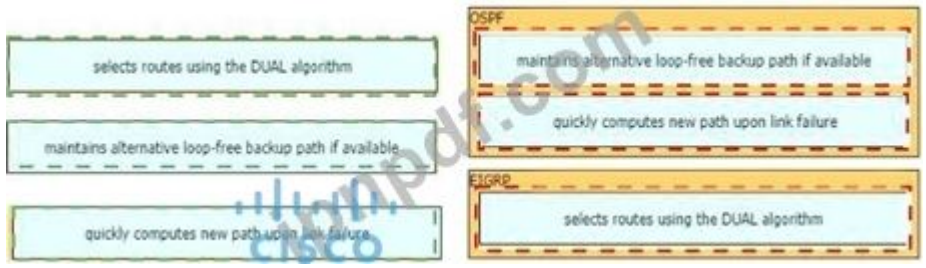


放射パターンはどのタイプのアンテナを示していますか?
A. 八木
B. 双極子
C. パッチ
D. 無指向性
Answer: C (メーッセージを残す**)**

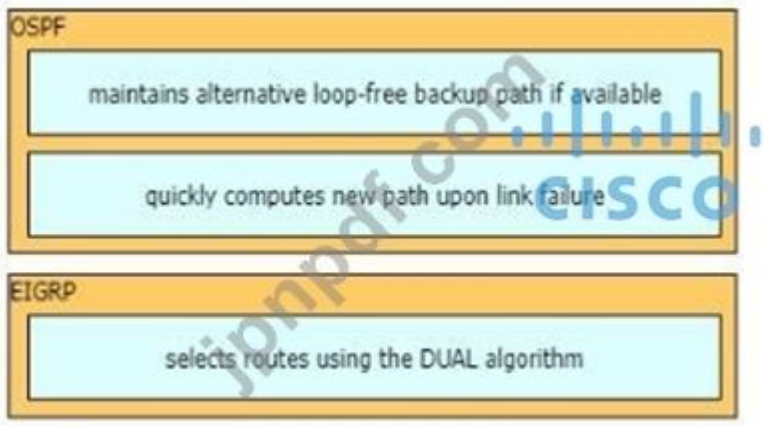
最新問題**: 97**
左側の特性を、右側に記述されているルーティング プロトコルにドラッグ アンド ドロップします。



Answer:

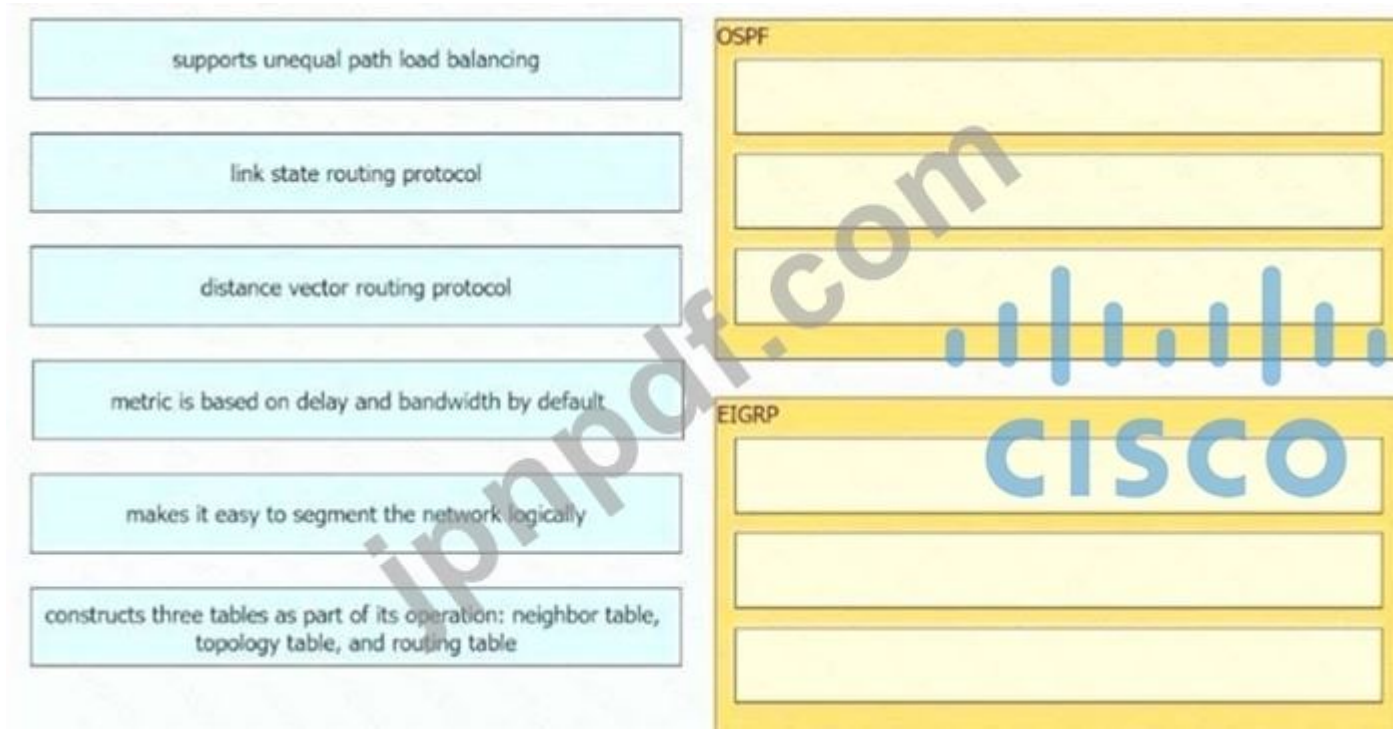


説明

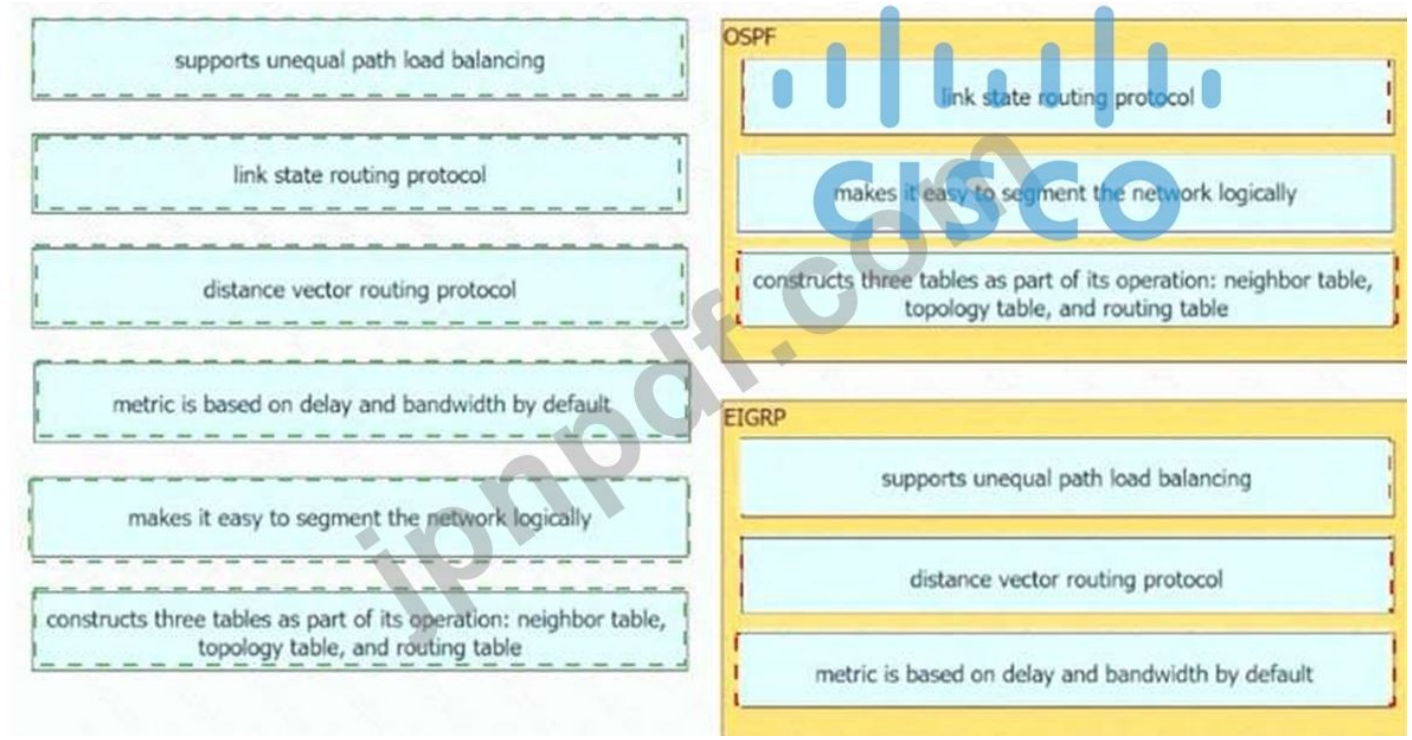


最新問題**: 98**

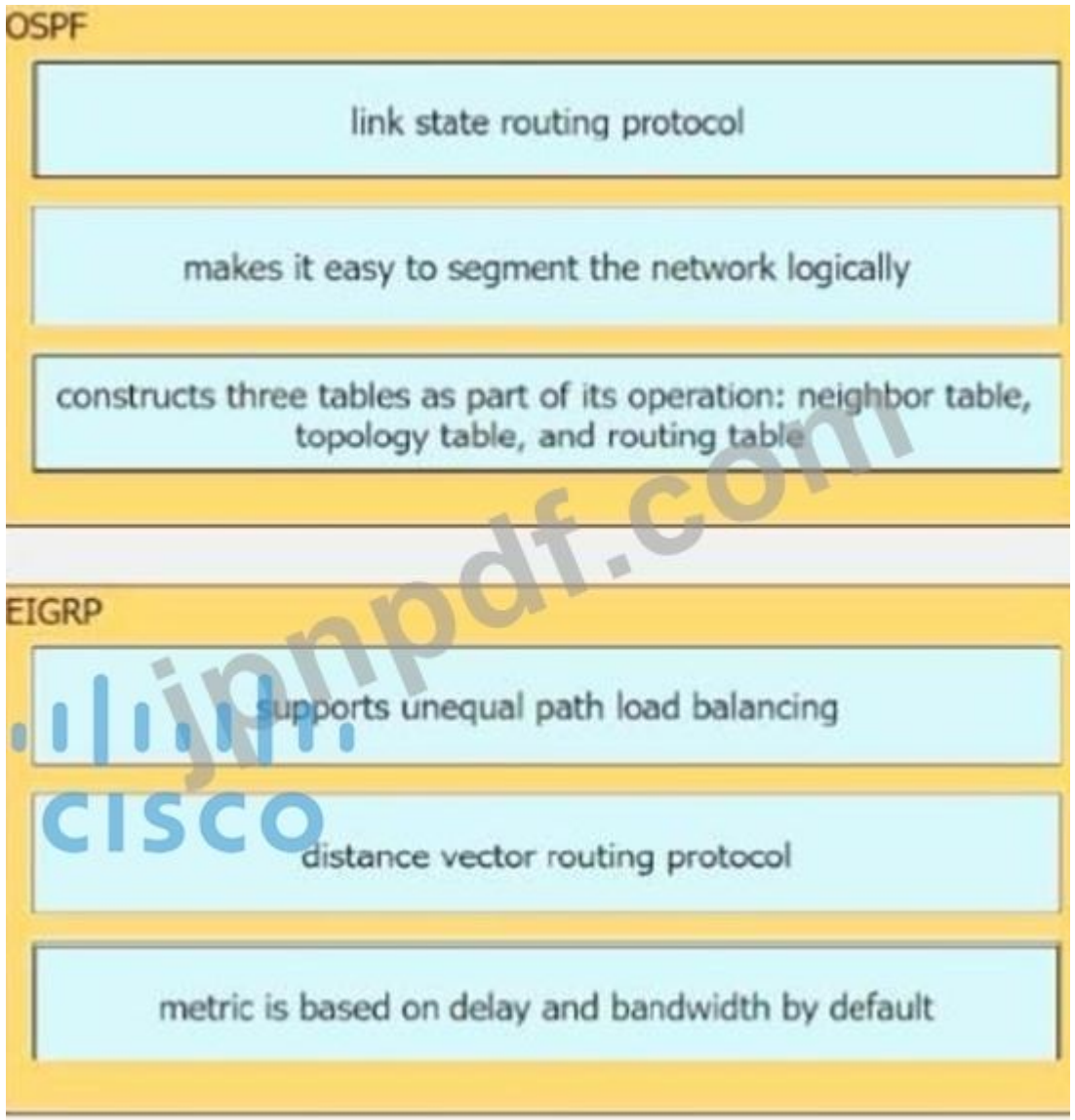
左側の特性を、右側に記述されているルーティング プロトコルにドラッグ アンド ドロップします。



Answer:

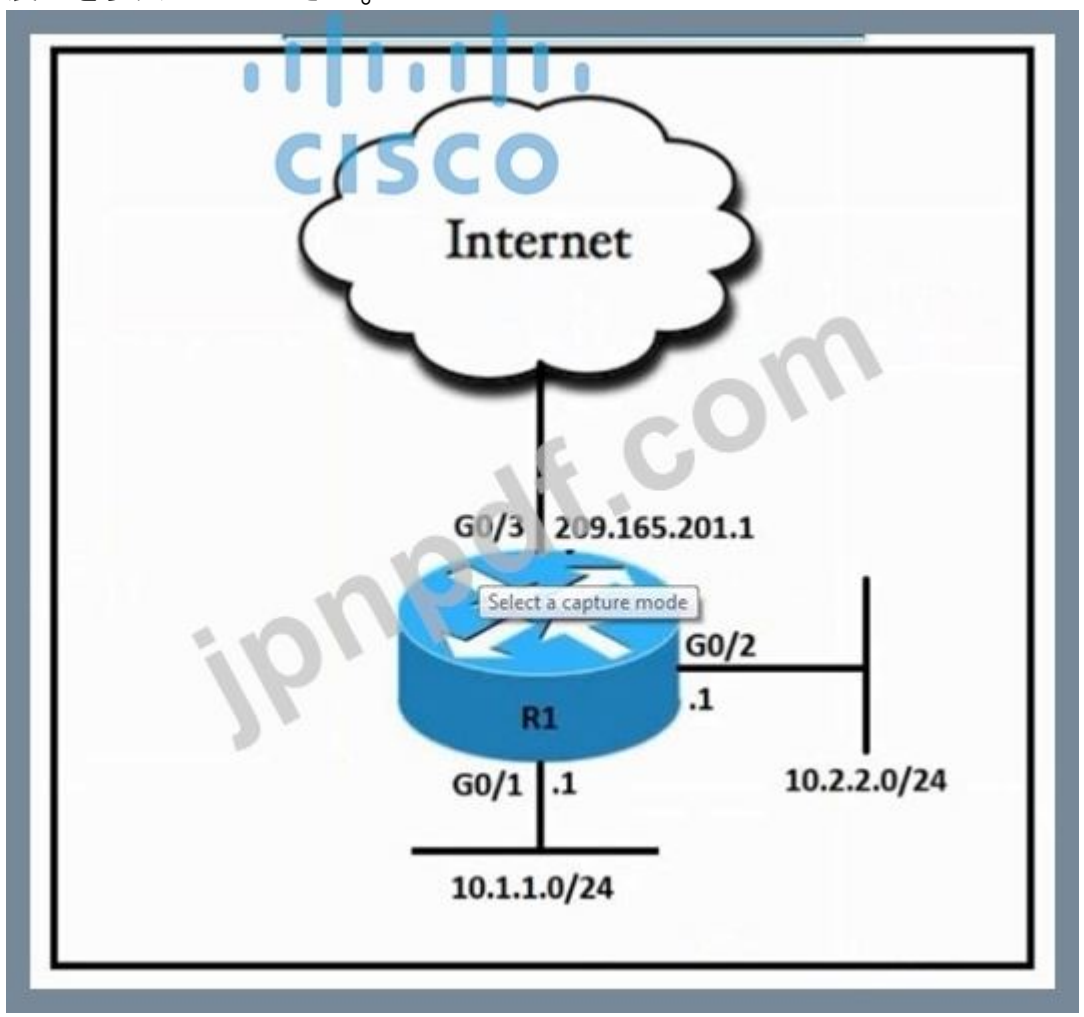

supports unequal path load balancing
link state routing protocol
distance vector routing protocol
metric is based on delay and bandwidth by default
makes it easy to segment the network logically
constructs three tables as part of its operation: neighbor table, topology table, and routing table
OSPF
link state routing protocol
makes it easy to segment the network logically
constructs three tables as part of its operation: neighbor table, topology table, and routing table
EIGRP
supports unequal path load balancing
distance vector routing protocol
metric is based on delay and bandwidth by default

説明


OSPF
link state routing protocol
makes it easy to segment the network logically
constructs three tables as part of its operation: neighbor table, topology table, and routing table
EIGRP
supports unequal path load balancing
distance vector routing protocol
metric is based on delay and bandwidth by default

最新問題: **99**

展示を参照してください。



エンジニアは、10.2.2.0/24 サブネット内のすべてのユーザーがインターネットにアクセスできるようにする必要があります。アドレス空間を節約するために、209.165.201.1 のパブリック インターフェイス アドレスをすべての外部通信に使用する必要があります。これらの要件を満たすコマンド セットはどれですか?

A)

B)

ハ)

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: D (メーッセージを残す**)**
コマンド -ip nat inside source list 10 interface G0/3 overload || G0/3 インターフェイスに割り当てられたアドレスにオーバーロードする NAT (PAT) を構成します。

最新問題: **100**
SD-WAN 展開では、vSmart コントローラのどのアクションが責任を負いますか?
A. vEdge ノードを SD-WAN ファブリックにオンボードします。
B. SD-WAN ファブリック内で実行されるデータ転送を制御するポリシーを配布します。
C. SD-WAN ファブリック内のノードの構成とステータスを処理、維持、収集します。
D. vEdge ルーターからテレメトリ データを収集する
Answer: B (メーッセージを残す**)**

最新問題: **101**

建物内で外部アンテナを使用するのはいつですか?

A. 5GHz使用時のみ

B. 2 4 GHz使用時のみ

C. Mobility Express利用時のみ

D. 必要なカバレッジを提供する場合

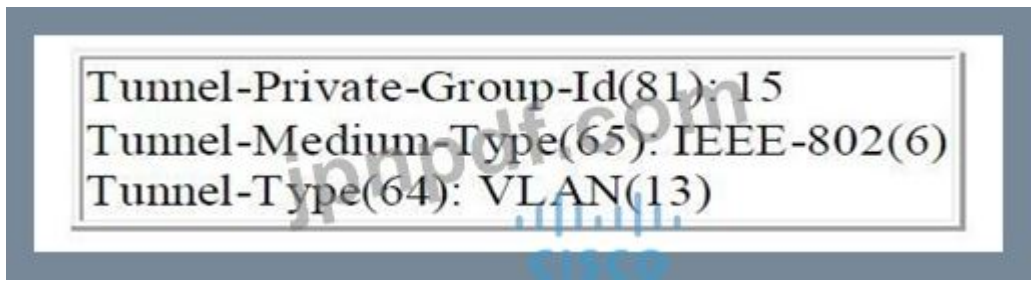
Answer: D (メーッセージを残す)

最新問題**: 102**

展示を参照してください。

```
(WLC) >show interface summary
Interface Name                Vlan Id
------------------------      -------
deadnet                       999
users1                        14
users2                        15
users3                        16

(WLC) >show wlan 1
WLAN Identifier . . . . . . . . . . . . . . . . 1
Network Name (SSID) . . . . . . . . . . . . . . wlan1
AAA Policy Override . . . . . . . . . . . . . . Enabled
Interface . . . . . . . . . . . . . . . . . . . deadnet
FlexConnect Local Switching . . . . . . . . . . Enabled
FlexConnect Central Association . . . . . . . . Disabled
flexconnect Central Dhcp Flag . . . . . . . . . Disabled
flexconnect nat-pat rlag . . . . . . . . . . . . Disabled
flexconnect DNS Override Flag . . . . . . . . . Disabled
flexconnect PPPoE pass-through . . . . . . . . . Disabled
flexconnect local-switching IP-source-guar . .Disabled
FlexConnect Vlan based Central Switching . .  Enabled
FlexConnect Local Authentication . . . . . .  Disabled
FlexConnect Learn IP Address . . . . . . . .  Enabled

(WLC) >show ap config general ------
AP Mode . . . . . . . . . . . . . . . . . . . . FlexConnect
FlexConnect Vlan mode : . . . . . . . . . . . . . Enabled
            Native ID : . . . . . . . . . . . . . . . . 1
            WLAN 1 : . . . . . . . . . . . . . . . . . . 10 (AP-Specific)
FlexConnect VLAN ACL Mappings
Vlan : . . . . . . . . . . . . . . . . . . . . . . 10
            Ingress ACL : . . . . . . . . . . . . . . . None
            Egress ACL : . . . . . . . . . . . . . . . . None
VLAN with least priority : . . . . . . . . . . . 13
FlexConnect Group . . . . . . . . . . . . . . . . flexgroup1
Group VLAN ACL Mappings
Vlan : . . . . . . . . . . . . . . . . . . . . . . 11
            Ingress ACL : . . . . . . . . . . . . . . . None
            Egress ACL : . . . . . . . . . . . . . . . . None
Vlan : . . . . . . . . . . . . . . . . . . . . . . 12
```

ワイヤレス クライアントは、現在スタンドアロン モードで動作している FlexAP1 に接続しています。AAA 認証プロセスは、次の AVP を返しています。



クライアントが経験する3つの行動はどれですか? (3つ選んでください。)

A. AP がスタンドアロン モードの場合、クライアントは VLAN 15 に配置されます。

B. AP がスタンドアロン モードの場合、クライアントは VLAN 10 に配置されます。

C. AP が接続モードに移行すると、クライアントは認証解除されます。

D. AP がスタンドアロン モードの場合、クライアントは VLAN 13 に配置されます。

E. AP が接続モードの場合、クライアントは VLAN 13 に配置されます。

F. AP が接続モードに移行すると、クライアントは関連付けられたままになります。

G. AP が接続モードの場合、クライアントは VLAN 15 に配置されます。

H. AP が接続モードの場合、クライアントは VLAN 10 に配置されます。

Answer: (解答を表示する**)**

説明

+ WLC show interface summary の出力から、WLC に 4 つの VLAN (99、14、15、16)があることがわかりました。+ show ap config general FlexAP1 の出力から、FlexConnect AP に 4 つの VLAN (10、11、12 および 13. また、FlexConnect AP の WLAN は VLAN 10 にマッピングされます（回線WLAN から

1: ..... 10 (AP 固有))。

の参照から：

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise FlexConnect VLAN 中央スイッチングの概要 WLAN 上のトラフィック フローFlexConnect AP が接続モードの場合にローカル スイッチング用に設定されたものは次のとおりです。

+ VLAN が AAA 属性の 1 つとして返され、その VLAN が FlexConnect AP データベースに存在しない場合、トラフィックは中央でスイッチングされ、VLAN が WLC に存在する場合、AAAserver から返されたこの VLAN/インターフェイスがクライアントに割り当てられます。(-> VLAN 15 が WLC に存在するため、クライアント inconnected モードにはこの VLAN が割り当てられます -> AP が接続モードの場合、クライアントは VLAN 15 に配置される」という回答が正しい) + VLAN が次のように返される場合AAA 属性の 1 つであり、その VLAN が F に存在しないlexConnect APdatabase では、トラフィックは中央で切り替えられます。その VLAN も WLC に存在しない場合、クライアントには、WLC の WLAN にマッピングされた VLAN/インターフェイスが割り当てられます。+ VLAN が AAA 属性の 1 つとして返され、その VLAN が FlexConnect AP データベースに存在する場合、トラフィックはローカルに切り替わります。+ VLAN が AAA サーバから返されない場合、クライアントにはその FlexConnect AP で WLAN にマッピングされた VLAN が割り当てられ、トラフィックはローカルにスイッチングされます。

FlexConnect AP がスタンドアロン モードの場合、ローカル スイッチング用に設定された WLAN のトラフィック フローは次のとおりです。

+ AAA サーバから返された VLAN が FlexConnect AP データベースに存在しない場合、クライアントはデフォルトの VLAN (つまり、FlexConnect AP 上の WLAN マップ VLAN)に配置されます (-> したがって、AP がスタンドアロンである間、モードでは、クライアントは VLAN 10 に配置されます' が正しい)。AP が接続し直すと、このクライアントは認証解除され (-> したがって、AP が接続モードに移行すると、クライアントは認証解除される」という回答が正しい)、トラフィックを集中的に切り替えます。

最新問題**: 103**

Cisco SD-WAN の単一の管理プレーンであるコントローラはどれですか?

A. vBond
B. vEdge
C. vSmart
D. vManage
Answer: (解答を表示する**)**
Cisco SD-WAN ソリューションの主要コンポーネントは、vManage ネットワークで構成されています。
管理システム (管理プレーン)、vSmart コントローラー (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)。
+ vManage - この集中型ネットワーク管理システムは、GUI インターフェイスを提供し、
アンダーレイとオーバーレイのすべての Cisco SD-WAN デバイスとリンクを監視、設定、および維持します。
通信網。
+ 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集中管理を担当します
SD-WAN ネットワークのプレーン。各 vEdge ルータへの安全な接続を確立し、
Overlay Management Protocol (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。また、vEdge ルータ間の安全なデータ プレーン接続を調整します。
暗号鍵情報を配布することにより、非常にスケーラブルで IKE を使用しないアーキテクチャが可能になります。
+ vBond オーケストレータ - このソフトウェア ベースのコンポーネントは、
vEdge デバイスとオーケストレーション vSmart および vEdge 接続。においても重要な役割を担っています。
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有効にします。
+ 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ます。
物理サイトまたはクラウドに配置され、サイト間の安全なデータ プレーン接続を提供します
1 つ以上の WAN トランスポートを介して。トラフィックの転送、セキュリティ、暗号化、
Quality of Service (QoS)、Border Gateway Protocol (BGP) や Open などのルーティング プロトコル
Shortest Path First (OSPF) など。
参照：
2018年10月.pdf

最新問題**: 104**
PIM スパース モードでの RP の役割は何ですか?
A. RP は、要求されたマルチキャスト グループの送信元で PIM Join メッセージに応答します。
B. RP はコントロール プレーン ノードとしてのみ機能し、マルチキャスト パケットを受信または転送しません。
C. RP は、PIM-SM 共有マルチキャスト配布ツリーのルートであるマルチキャストルーターです。
D. RP は、受信者によって要求されたすべてのマルチキャスト ストリームのデフォルトのエージング タイムアウトを維持します。
Answer: C (メーッセージを残す**)**

最新問題**: 105**
総当たり攻撃から REST API を保護し、影響を最小限に抑えるために使用されるアルゴリズムはどれですか?
A. SHA-512 および SHA-384
B. MD5 アルゴリズム–128および SHA-384
C. SHA-1、SHA-256、SHA-512

D. PBKDF2、BCrypt、SCrypt
Answer: (解答を表示する**)**
REST API を保護するためのベスト プラクティスの 1 つは、パスワード ハッシュを使用することです。パスワードは
システムが危険にさらされた場合でも、システムを保護する (または被害を最小限に抑える) ために常にハッシュ化されます。
いくつかのハッキングの試みで。本当に証明できるそのようなハッシュアルゴリズムはたくさんあります
PBKDF2、bcrypt、scrypt アルゴリズムなどのパスワード セキュリティに有効です。
REST API を保護するその他の方法は次のとおりです。常に HTTPS を使用する、URL で情報を公開しない
(ユーザー名、パスワード、セッション トークン、および API キーは URL に表示されません)、
リクエストにタイムスタンプを追加、OAuth を使用、入力パラメーターの検証。

最新問題**: 106**
展示を参照してください。

エンジニアは、アクセス ポートからトランクへの SW1 と SW2 の間のポット チャネルを再構成し、すぐに SW1 のログでこのエラーに気付きます。
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
```

ハ)

```
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 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**)**

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **107**
ワイヤレス LAN コントローラを検出するために入力している AP が使用する 2 つの方法はどれですか? (2つ選んでください。)
A. ローカルサブネットでのブロードキャスト
B. Cisco Discovery Protocol ネイバー
C. DNS ルックアップ cisco-DNA-PRIMARY.localdomain
D. 他の AP のクエリ
E. DHCP オプション 43
Answer: (解答を表示する)

最新問題: **108**
Cisco SD-WAN 導入における集中管理ポリシーとは何ですか?
A. クラウド内のノード認証を管理する一連のルール
B. ユーザー アクセス ポリシーを定義する順序付きステートメントのリスト
C. ルーティングの実行方法を定義する一連のステートメント
D. クラウド内のすべてのノードで有効なサービスのリスト
Answer: (解答を表示する)

最新問題: **109**
仮想マシン環境でブロードキャスト放射が発生する理由を 2 つ挙げてください。(2つ選んでください。)
A. ブロードキャスト パケットを処理するには、vSwitch がサーバーの 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 モードで通信します。
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: (解答を表示する)
説明
ブロードキャスト放射は、コンピューター ネットワーク上のブロードキャストおよびマルチキャスト 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 ドメイン内で見られるブロードキャスト 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。そのため、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 -> VLAN を使用してブロードキャスト放射を減らす必要があります。
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への (VLAN を拡張するための) トランクの使用です。

ハイパーバイザーでの仮想化の構造に関する注意:
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 が外界へのレイヤー 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、物理スイッチに出向かなくてもレイヤー 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 から入るフレームは、VMNIC の外には出ません。
別の VMNIC カードからの物理ホスト。

最新問題: 110
クライアントと AP の間で交換される DHCP メッセージを、右側の交換される順序にドラッグ アンド ドロップします。

Answer:

最新問題: **111**

Cisco DNA Center で設計ワークフローが使用されるのはいつですか?

A. 既存のインフラストラクチャを持たないグリーンフィールド展開

B. グリーンフィールドまたはブラウンフィールドの展開で、既存のデータを一掃する

C. ブラウンフィールド展開で、ネットワーク内の既存のデバイスの構成を変更するため

D. ブラウンフィールド展開で、新しいネットワーク デバイスをプロビジョニングしてオンボードするため

Answer: A (メーッセージを残す**)**

説明

設計エリアでは、ネットワーク全体のデバイスに適用できる物理トポロジ、ネットワーク設定、デバイス タイプ プロファイルなど、ネットワークの構造とフレームワークを作成します。

既存のインフラストラクチャがまだない場合は、設計ワークフローを使用します。既存のインフラストラクチャがある場合は、検出機能を使用します。

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-c

最新問題: **112**

展示を参照してください。

```
access-list 1 permit 172.16.1.0 0.0.0.255
ip nat inside source list 1 interface gigabitethernet0/0 overload
```

このデバイスの NAT 構成の内部インターフェイスと外部インターフェイスは正しく識別されています。この構成の効果は何ですか?

A. ダイナミック NAT

B. 静的 NAT

C. NAT64
D. パット
Answer: D (メーッセージを残す)

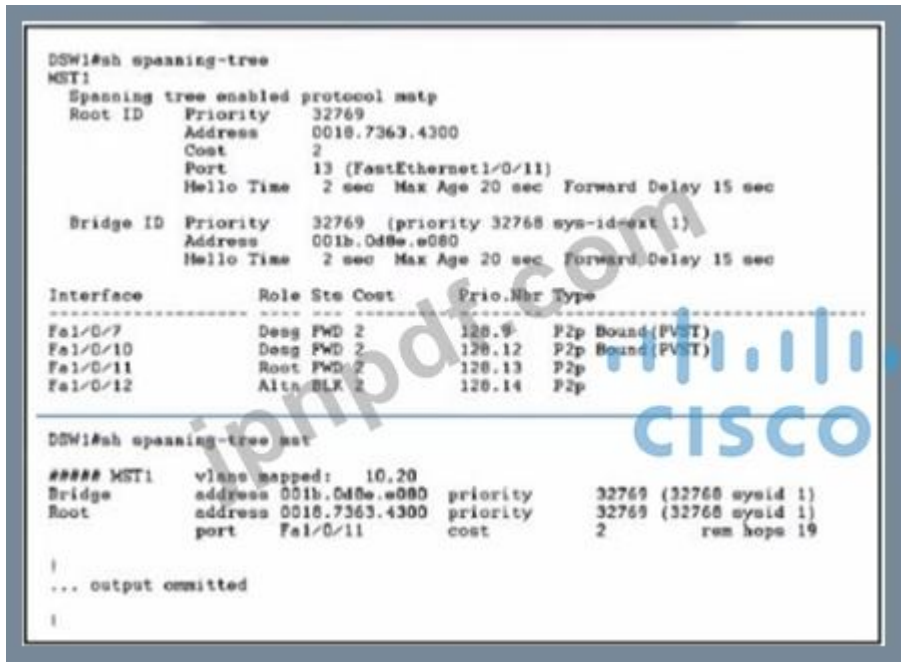
最新問題: **113**
VXLAN について正しい記述はどれですか?
A. VXLAN は TCP 35 トランスポート プロトコルを物理的なデータ センター ネットワーク上で使用します。
B. VXLAN は、レイヤー 2 セグメント ID フィールドを 24 ビットに拡張します。これにより、同じネットワーク上で最大 4094 の一意のレイヤ 2 セグメントが可能になります。
C. VXLAN は、レイヤー 2 フレームを IP-UDP ヘッダーにカプセル化します。これにより、ルーター境界を越えたレイヤー 2 隣接関係が可能になります。
D. VXLAN は、ループ防止のためにスパニング ツリー プロトコルを使用します。
Answer: C (メーッセージを残す)
説明
802.1Q VLAN ID スペースは 12 ビットのみです。VXLAN ID スペースは 24 ビットです。この 2 倍のサイズにより、VXLAN ID スペースは 1600 万のレイヤー 2 セグメントをサポートできます -> 回答 「VXLAN はレイヤー 2 セグメント ID フィールドを 24 ビットに拡張し、同じネットワーク上で最大 4094 の一意のレイヤー 2 セグメントを許可します」は正しくありません.
VXLAN は、既存のレイヤ 3 インフラストラクチャ上でレイヤ 2 またはレイヤ 3 オーバーレイ ネットワークを拡張するために使用される MAC-in-UDP カプセル化方式です。

最新問題: **114**
展示を参照してください。


```
hostname R1
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
auto-cost reference-bandwidth 1000
!
hostname R2
router ospf 2
network 20.0.0.0 0.0.0.255 area 0
```

OSPF ネイバーシップを形成するために R2 に適用する必要があるコマンドはどれですか?
A. ネットワーク 20.1.1.2.0.0.0.0 エリア 0
B. ネットワーク 20.1.1.2 255.255.255 エリア 0
C. ネットワーク 20.1.1.2.0.0.255.255 エリア 0
D. ネットワーク 20.1.1.2 255.255.0.0。エリア0
Answer: (解答を表示する)

最新問題: **115**
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確認する 2 つのコマンドはどれですか?

A. スパニング ツリー mst 1 プライオリティ 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 プライオリティ ルート

E. スパニング ツリー mst 1 プライオリティ 4096

Answer: B,E (メーッセージを残す)

説明

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.

2 番目のコマンド出力 $how spanning-tree mst)から、MST1 に VLAN 10 と 10 が含まれていることがわかります。

20.したがって、DSW1 をこれらの VLAN のルート ブリッジにしたい場合は、MST 1 リージョンをルートに設定する必要があります。コマンド §panning-tree mst 1 root primary」でうまくいきます。実際、このコマンドはマクロを実行し、優先度を現在のルートよりも低く設定します。

また、これらの VLAN の現在のルート ブリッジの優先度が 32769 (デフォルト値 + sysid) であることも確認できるため、DSW1 の優先度を特定の低い値に設定できます。ただし、優先度は の倍数でなければならないことに注意してください。

4096。

最新問題: **116**

シスコ エクスプレス フォワーディングのロード バランシングについて正しい説明はどれですか? （選ぶ二）

A. 各ハッシュは、RIB 内の単一のエントリに直接マップされます

B. 送信元 IP アドレスのサブネット マスクを組み合わせて、宛先ごとにハッシュを作成します。

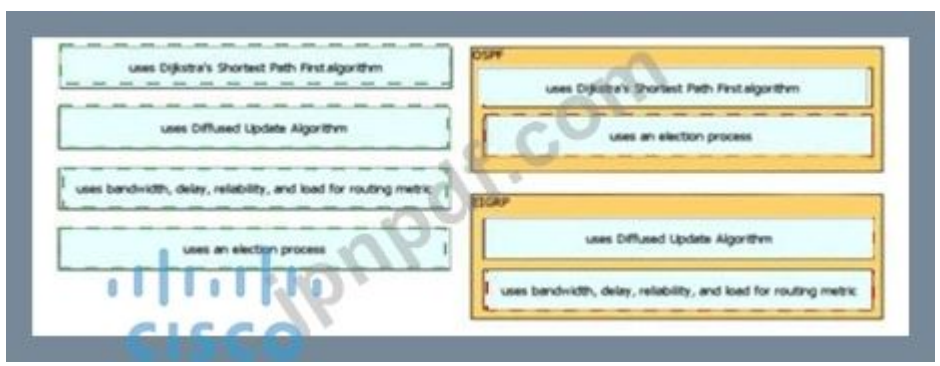
C. シスコ エクスプレス フォワーディングは、最大 2 つの宛先にロード バランシングできます。

D. ソース IP アドレスと宛先 IP アドレスを組み合わせて、それぞれのハッシュを作成します。

行き先
E. 各ハッシュは、隣接テーブル内の単一のエントリに直接マップされます
Answer: (解答を表示する**)**
Cisco IOS ソフトウェアは、基本的に CEF ロード バランシングの 2 つのモードをサポートしています。宛先ごとまたはパケットごとです。
送信先ごとの負荷分散では、送信元と送信先からハッシュが計算されます
IP アドレス (-> Answer '送信元 IP アドレスと宛先 IP アドレスを組み合わせて、ハッシュを作成します。
それぞれの宛先」が正しい)。このハッシュは、
隣接テーブル (-> 回答 各ハッシュは、隣接テーブルの単一のエントリに直接マップされます」
この送信元/宛先アドレスを持つすべてのパケットに同じパスが使用されている場合
ペア。パケットごとのロード バランシングが使用されている場合、パケットは使用可能な
パス。いずれの場合も、FIB および隣接テーブルの情報は、必要なすべての情報を提供します。
非負荷分散操作と同様に、情報を転送します。
使用されるパスの数は、ルーティング プロトコルが設定するエントリの数によって制限されます。
ルーティング テーブル。IOS のデフォルトは、ほとんどの IP ルーティング プロトコルで 4 エントリです。
1 つのエントリである BGP。設定できる最大数は 6 種類です
パス -> Answer 'シスコ エクスプレス フォワーディングは、最大 2 つのパスでロード バランシングできます。
宛先」が正しくありません。
参照：
09186a00800afeb7.html

最新問題**: 117**
左側の特性を、右側の適用対象のプロトコルにドラッグ アンド ドロップしますか?

Answer:



説明
図の説明が自動生成される

最新問題: **118**

展示を参照してください。

放射パターンはどのタイプのアンテナを表していますか?

A. 八木

B. 多方向

C. 方向パッチ

D. 無指向性

Answer: A (メーッセージを残す**)**

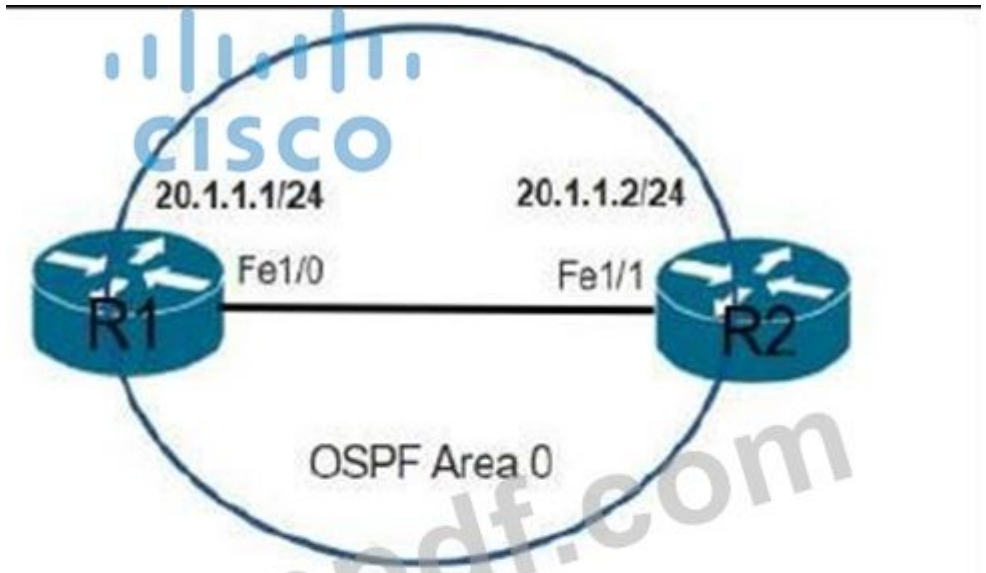
説明

八木アンテナは、単純なアンテナ (通常はダイポールまたはダイポールのようなアンテナ) を駆動し、長さと間隔が厳密に制御された一連の非駆動素子を使用してビームを成形することによって形成されます。

参照: https://www.cisco.com/c/en/us/products/collateral/wireless/aironetanennas-accessories/prod_white_paper0900aecd806a1a3e.htm

最新問題**: 119**

展示を参照してください。




```
hostname R1
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
auto-cost reference-bandwidth 1000
!
hostname R2
router ospf 2
network 20.0.0.0 0.0.0.255 area 0
```

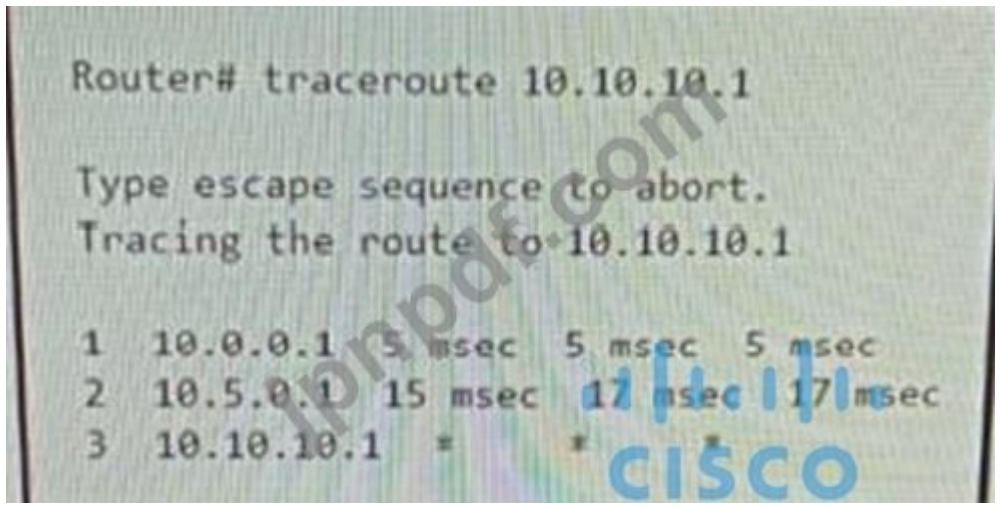
OSPF ネイバーシップを形成するために R2 に適用する必要があるコマンドはどれですか?

A. ネットワーク 20.1.1.2.0.0.0.0 エリア 0

B. ネットワーク 20.1.1.2 255.255.0.0。エリア0

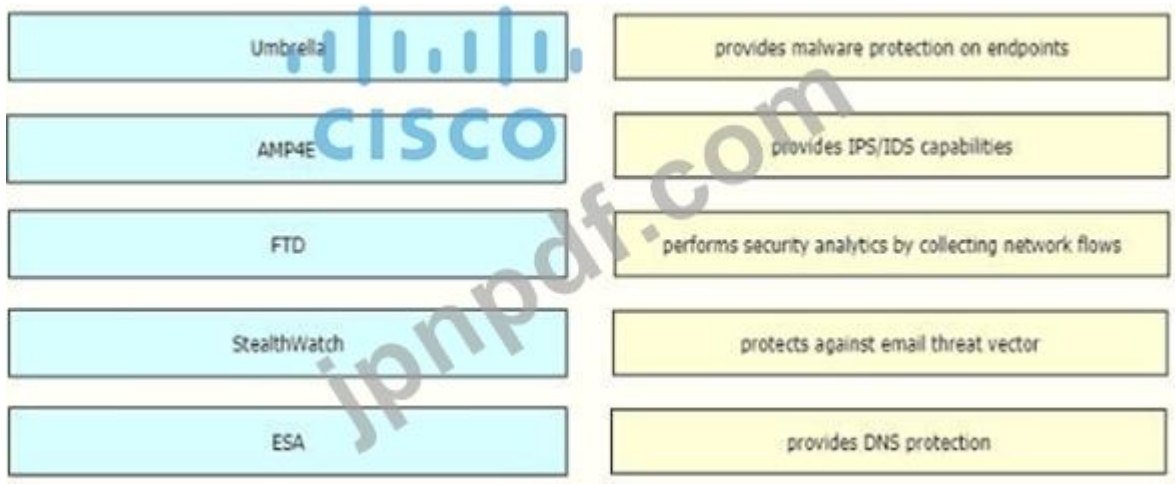
C. ネットワーク 20.1.1.2.0.0.255.255 エリア 0
D. ネットワーク 20.1.1.2 255.255.255 エリア 0
Answer: A (メーッセージを残す)
説明
R2 の network 20.0.0.0 0.0.0.255 area 0 コマンドは、R2 の Fa1/1 インターフェイスの IP アドレスをカバーしていなかったため、OSPF はこのインターフェイスで実行されませんでした。したがって、コマンド network 20.1.1.2 0.0.255.255 area 0 を使用して、このインターフェイスで OSPF をオンにする必要があります。
注: コマンド network 20.1.1.2 0.0.255.255 area 0 も使用できるため、この回答も正しいですが、回答 C がここでの最良の回答です。
R1 で network 0.0.0.0 255.255.255.255 area 0 コマンドを実行すると、すべてのアクティブで OSPF が実行されます。

最新問題**: 120**
展示を参照してください。



エンジニアが接続の問題のトラブルシューティングを行っており、traceout を実行しています。結果は何を確認しますか？
A. プロトコルに到達できません
B. 宛先ポートに到達できません
C. プローブがタイムアウトしました
D. 宛先サーバーがビジー状態であると報告しました
Answer: A (メーッセージを残す)

最新問題**: 121**
脅威防御ソリューションを左側から右側の説明にドラッグ アンド ドロップします。



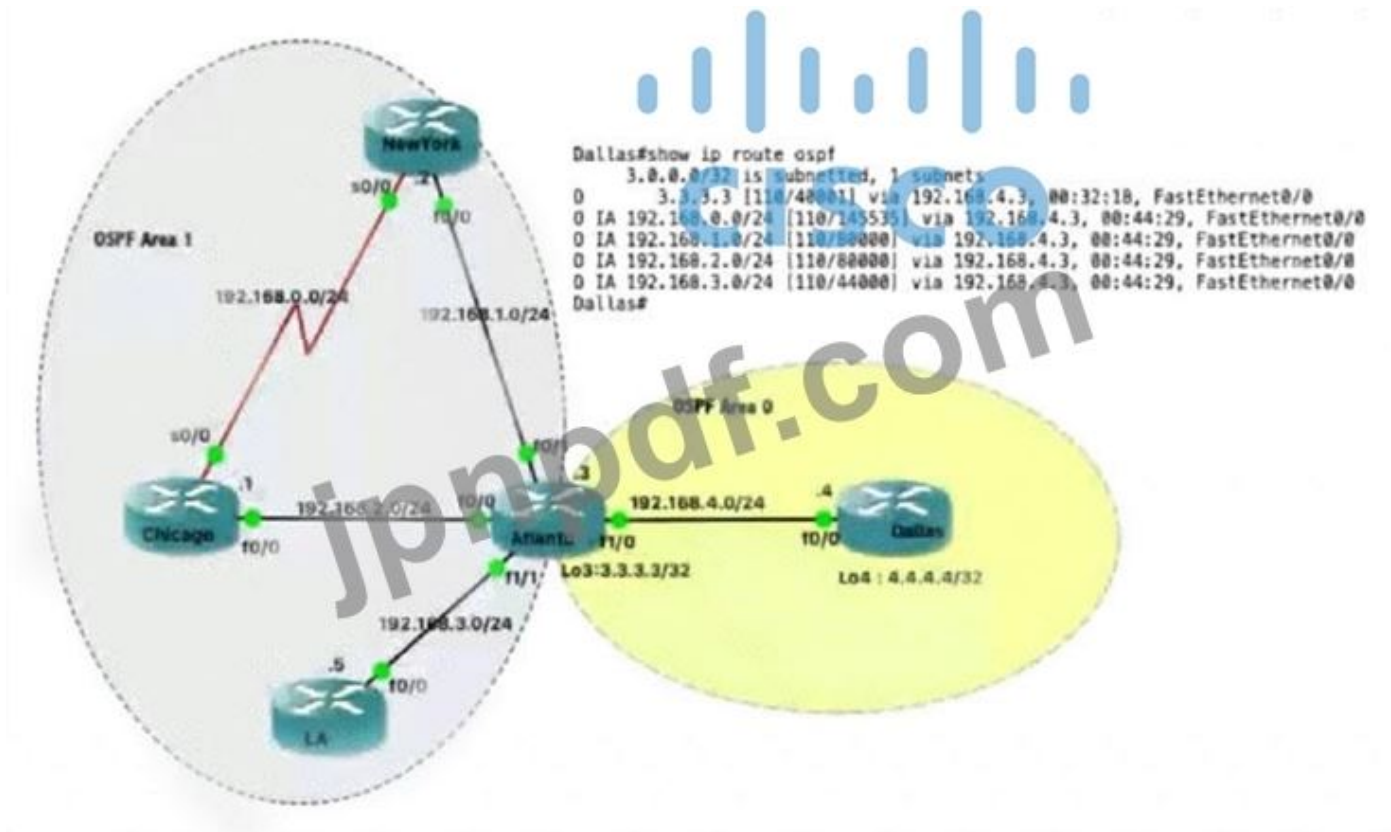
Answer:

説明

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **122**

展示を参照してください。

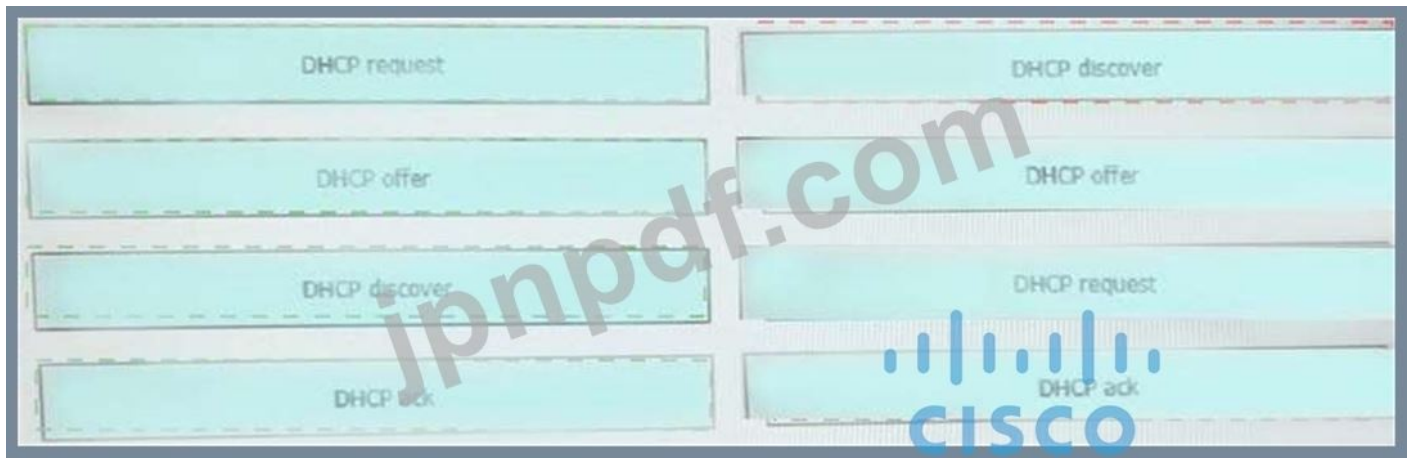


アトランタ ルーターに適用すると、バックボーン エリアへのタイプ 3 LSA フラッディングが減少し、ダラス ルーターのエリア間ルートが要約されるコマンドはどれですか?

A. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.252.0
B. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.248.0
C. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.252.0
D. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.248.0
Answer: C (メーッセージを残す)

最新問題: **123**
クライアントと AP の間で交換される DHCP メッセージを、右側の交換される順序にドラッグ アンド ドロップします。

Answer:



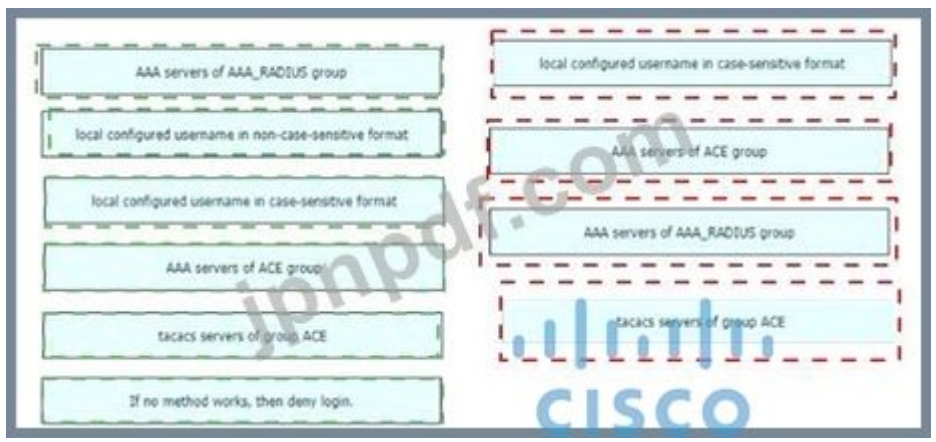
説明

DHCP クライアントと DHCP サーバーの間で送信されるメッセージは、DHCPDISCOVER、DHCPO FFER、DHCPREQUEST、および DHCPACKNOWLEDGEMENT の 4 つです。
このプロセスは、多くの場合、DORA (発見、提供、要求、承認) と略されます。

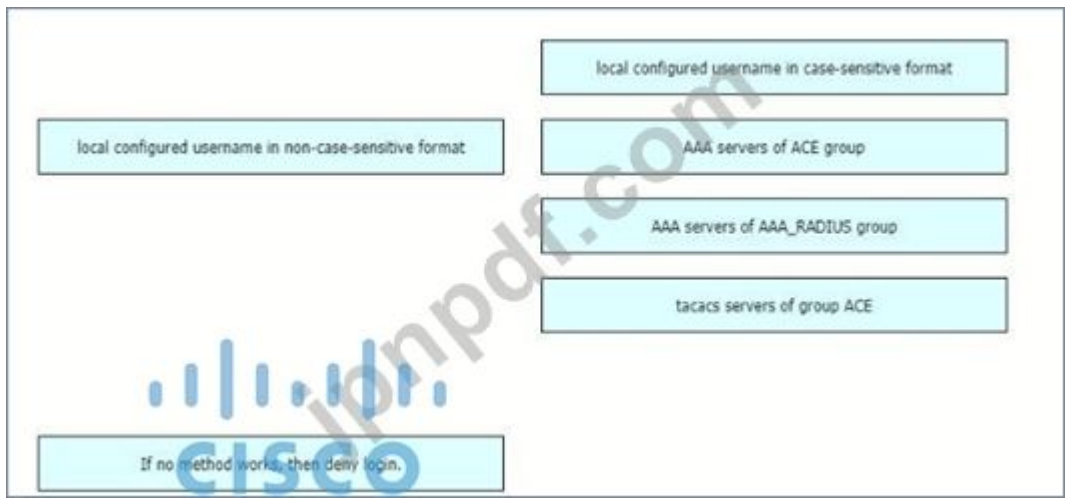
最新問題: **124**
エンジニアが以下の構成を作成します。認証方法を左から右の優先順にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。

```
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:



説明



最新問題: **125**

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 Core 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ようにする必要があります。

この要件を満たすコマンドはどれですか?

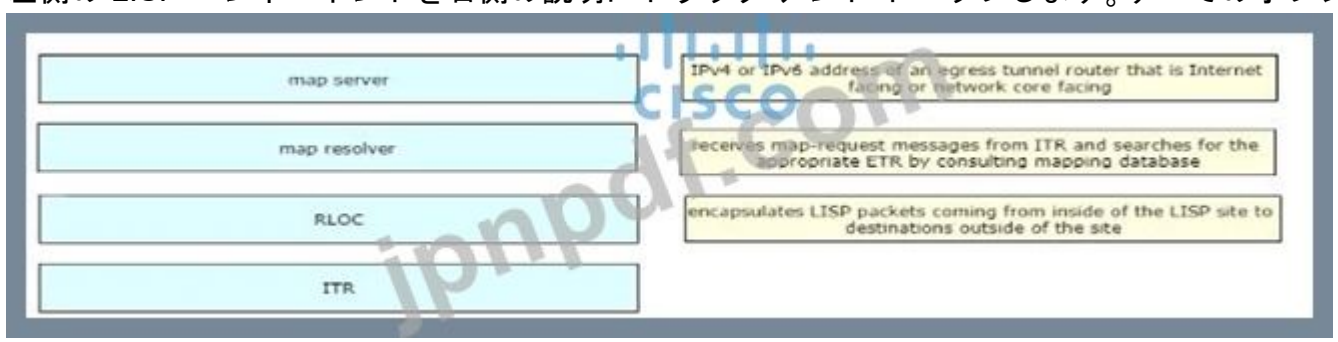
A. SwitchC(config)#vtp pruning vlan 110

B. SwitchC(config)#vtp プルーニング

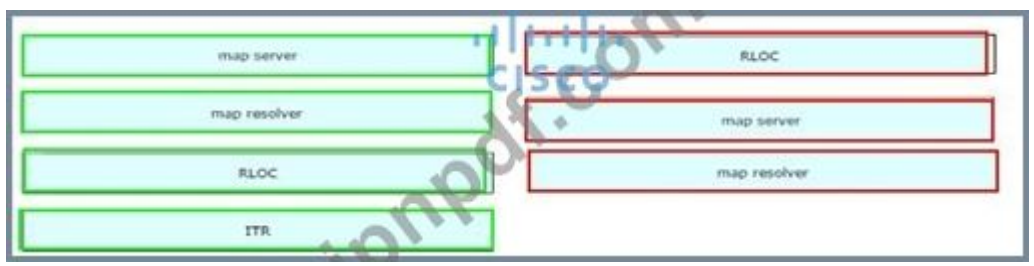
C. SwitchC(config)#interface port-channel 1

SwitchC(config-if)#switchport トランク許可 vlan 削除 110
D. SwitchC(config)#interface port-channel 1
SwitchC(config-if)#switchport trunk allowed vlan add 210,310
Answer: C (メーッセージを残す**)**

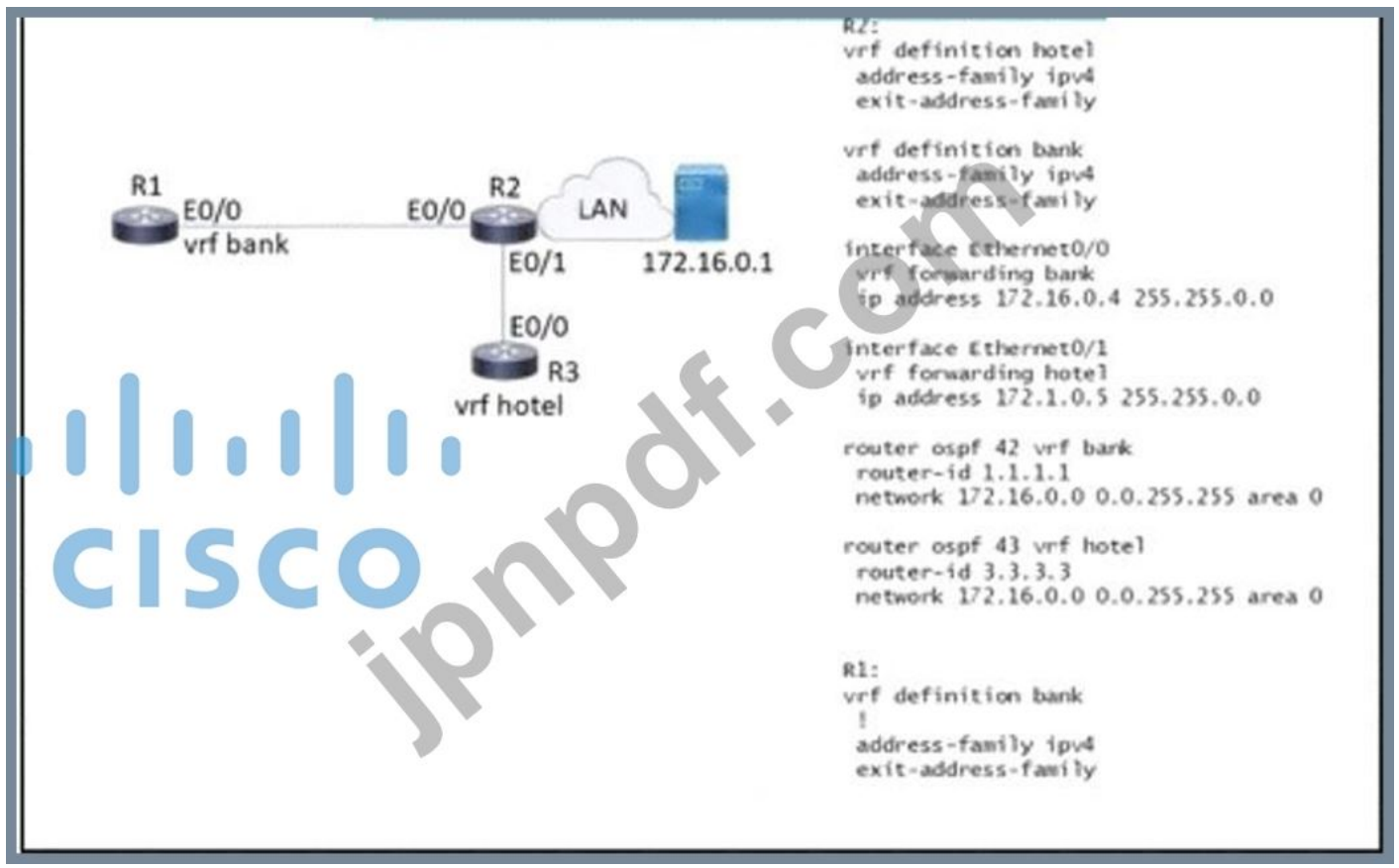
最新問題**: 126**
左側の LISP コンポーネントを右側の説明にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。



Answer:



最新問題**: 127**



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、R にどの構成を適用する必要がありますか?

A)

```
interface Ethernet0/0
 vrf forwarding hotel
 ip address 172.16.0.7 255.255.0.0

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

B)

```
interface Ethernet0/0
 ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf hotel
 network 172.16.0.0 255.255.0.0
```

C)

```
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf bank
 network 172.16.0.0 255.255.0.0
```

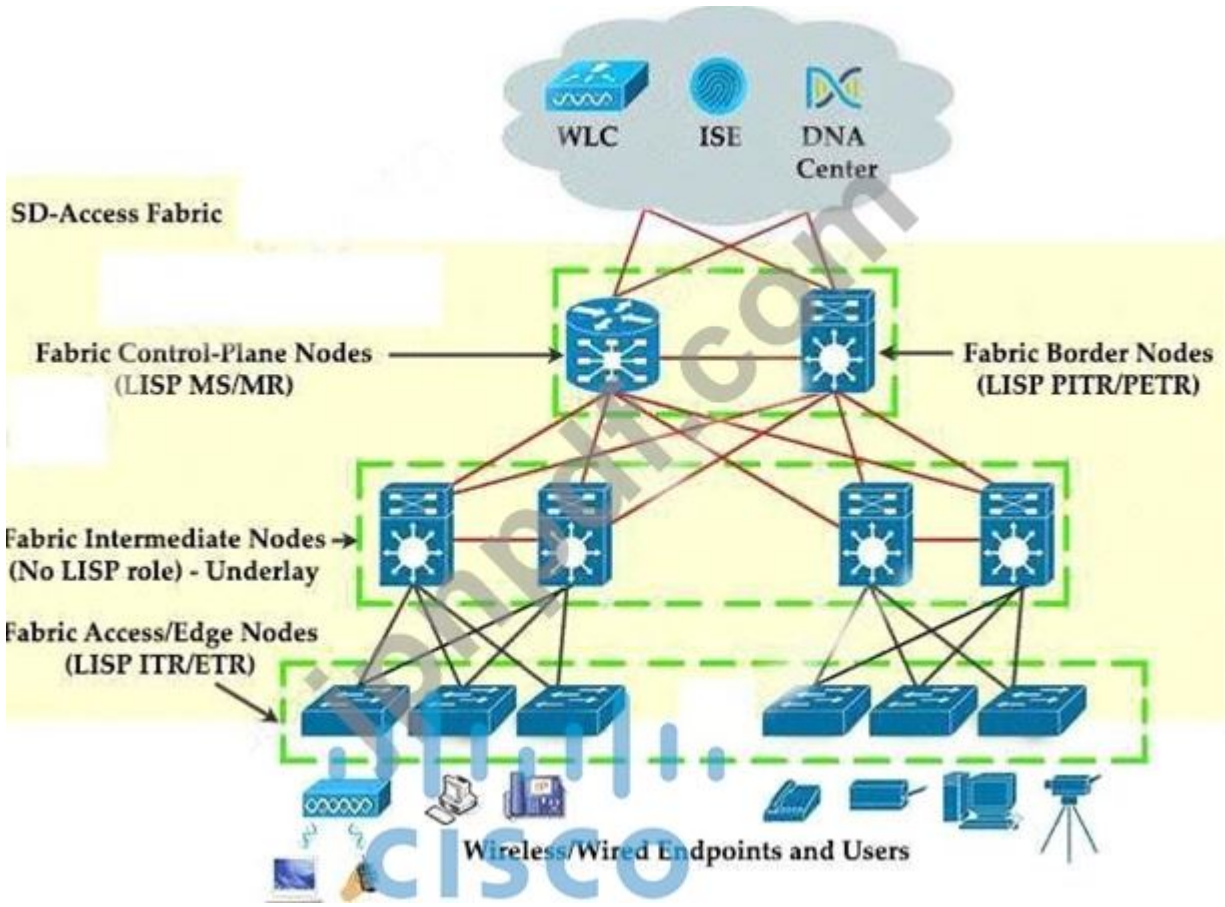
D)

```
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
```

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**: 128**
Cisco SD-Access ファブリックの 2 つのデバイス ロールは何ですか? （2つ選んでください。）
A. コア スイッチ

B. vBond コントローラー
C. エッジ ノード
D. アクセススイッチ
E. 境界ノード
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 ロールがあります。
+ 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 ボーダー ノード: このファブリック デバイス (コア レイヤー デバイスなど) は、外部のレイヤー 3 ネットワークを SDA ファブリックに接続します。
+ ファブリック エッジ ノード: このファブリック デバイス (アクセスまたはディストリビューション レイヤー 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 アクセス 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。



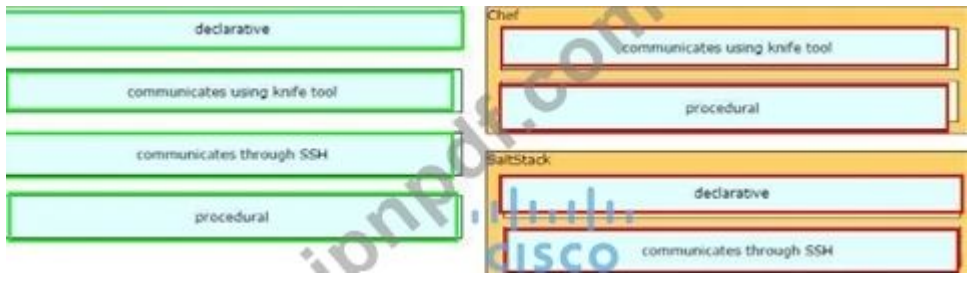
最新問題**: 129**
Cisco ルーターを NTP 権限のあるサーバーとして使用する場合、どの NTP モードを有効にする必要がありますか?
A. ブロードキャスト クライアント
B. ピア
C. サーバー
D. プライマリ

Answer: B (メーッセージを残す)

最新問題: **130**

特性を左側から右側に記述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: **131**

IP アドレス 10.10.10.1 のワークステーションから発信された http トラフィックを除くすべてのトラフィックを許可する、ルーターの WAN インターフェイスに適用されるアウトバウンド アクセス リストはどれですか?

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
```

ハ)

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

D)

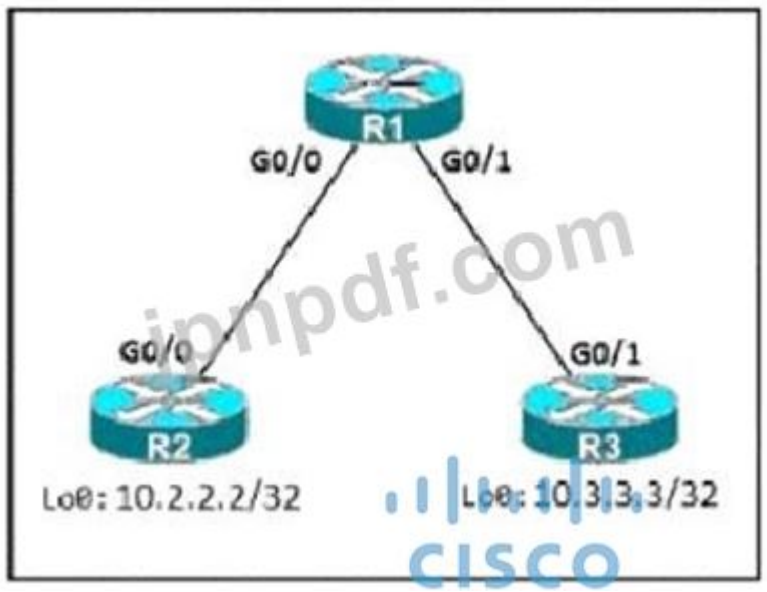
```
ip access-list extended 10
deny tcp host 10.10.10.1 any eq 80
permit ip any any
```

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

最新問題: **132**
cisco SD アクセス導入における cisco DNA センターの機能は何ですか?
A. すべての非ファブリック ノードとそれに対応するファブリック ノードの統合と自動化を提供します。
B. ファブリック ネットワーク デバイスの設計、管理、展開、プロビジョニング、および保証を担当します。
C. ファブリック内のルーティング決定を担当します。
D. ファブリックに関連するすべてのエンドポイント、ノード、および外部ネットワークに関する情報を保持します。
Answer: B (メーッセージを残す**)**

最新問題: **133**
TCAM と MAC アドレス テーブルの違いは何ですか?
A. MAC アドレス テーブルは CAM ACL に含まれ、QoS 情報は TCAM に格納されます。
B. MAC アドレス テーブルは部分一致をサポートします。TCAM には完全一致が必要です
C. ルータ プレフィックス ルックアップは CAM で行われます。MAC アドレス テーブルのルックアップは TCAM で行われます。
D. TCAM はレイヤ 2 転送の決定に使用されます CAM はルーティング テーブルの構築に使用されます
Answer: A (メーッセージを残す**)**
説明
https://community.cisco.com/t5/networking-documents/cam-content-addressable-memory-vs-tcam-ternary-conte

最新問題: **134**
展示を参照してください。



エンジニアは、週末の時間帯にルーター R3 のループバック インターフェイスからルーター R2 のループバック インターフェイスへの Telnet トラフィックを拒否する必要があります。ルーター R3 と R2 のループバック インターフェイス間の他のすべてのトラフィックは、常に許可する必要があります。このタスクを実行するコマンドはどれですか?
A)

```
R3(config)#time-range WEEKEND
R3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59

R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R3(config)#access-list 150 permit ip any any time-range WEEKEND

R3(config)#interface G0/1
R3(config-if)#ip access-group 150 out
```

B)

```
R1(config)#time-range WEEKEND
R1(config-time-range)#periodic Friday Sunday 00:00 to 00:00

R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R1(config)#access-list 150 permit ip any any

R1(config)#interface G0/1
R1(config-if)#ip access-group 150 in
```

A)

```
R1(config)#time-range WEEKEND
R1(config-time-range)#periodic weekend 00:00 to 23:59

R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R1(config)#access-list 150 permit ip any any

R1(config)#interface G0/1
R1(config-if)#ip access-group 150 in
```

D)

```
R3(config)#time-range WEEKEND
R3(config-time-range)#periodic weekend 00:00 to 23:59

R3(config)#access-list 150 permit tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R3(config)#access-list 150 permit ip any any time-range WEEKEND

R3(config)#interface G0/1
R3(config-if)#ip access-group 150 out
```

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

最新問題**: 135**
脅威防御ソリューションを左側から右側の説明にドラッグ アンド ドロップします。

Answer:

説明

最新問題: **136**

データモデリング言語はどのように使用されていますか」

A. データを簡単に構造化し、グループ化し、検証し、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 エレメントを表します。

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する。

D. スクリプト言語を人間が読めるようにするため
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.

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **137**
エンジニアがサンプル コードを実行すると、ターミナルからこの出力が返されます。この問題を修正するサンプル コードの変更はどれですか?

Sample Code

```
#!/usr/bin/env python

import json
import sys

test_json = """
{
   "type": "Cisco ASR 1001-X Router",
    "lastUpdateTime": 1552394222783,
    "macAddress": "00:c8:8b:80:bb:00",
    "serialNumber": "FXS1932Q1SE"
}
"""
print(json.load(test_json))
```

Output

```
$ python print_json.py
Traceback (most recent call last):
   File "question_3.py", line 15, in <module>
      Print(json.load(test_json))
   File
"/System/Library/Framework/Python.framework?Versions?2.7/lib/python2.7/json/_init_.py", line 286 in load
      return loads (fp.read(),
AttributeError: 'str' object has no attribute 'read'
```

A. JSON メソッドを load() から load() に変更します。
B. test_json 文字列内の null を二重引用符で囲みます
C. 単一の二重引用符のセットを使用し、test_json を 1 行に要約します。
D. test_json 文字列で明示的に read() メソッドを呼び出します
Answer: A (メーッセージを残す**)**

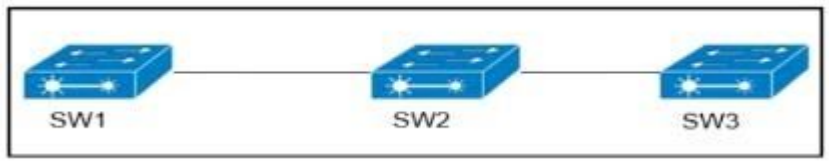
- `json.load()` method (without "**s**" in "load") used to **read JSON encoded data from a file** and convert it into a Python dictionary.
- `json.loads()` method, which is used to **parse valid JSON string** into Python dictionary.

最新問題: **138**
Cisco SD-WAN 環境での vsmart コントローラの役割は何ですか?
A. IT が認証と承認を実行します。
B. コントロール プレーンを管理します。
C. 集中型ネットワーク管理システムです。
D. データプレーンを管理します。
Answer: B (メーッセージを残す**)**
説明
コントロール プレーン (vSmart) は、ネットワーク トポロジを構築および維持し、トラフィック フローに関する決定を行います。vSmart コントローラは、WAN エッジ デバイス間でコントロール プレーン情報を配布し、コントロール プレーン ポリシーを実装し、データ プレーン ポリシーをネットワーク デバイスに配信して適用します。

最新問題: **139**
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に、[Clients] > [Detail] で設定された Mobility Role Anchor があ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. コントローラ内
B. レイヤー 3 インターコントローラー
C. 間接
D. レイヤー 2 インターコントローラー
Answer: (解答を表示する)

最新問題: **140**
出品物参照。



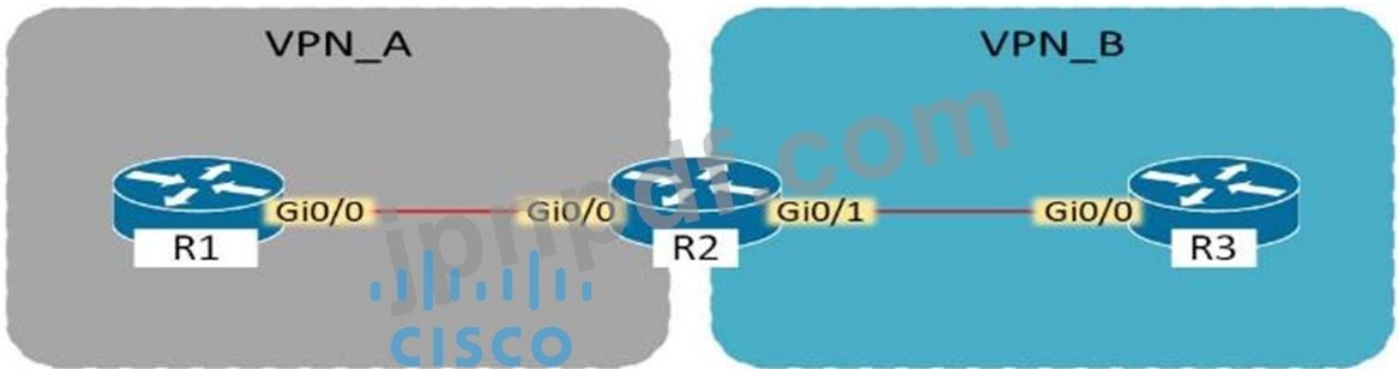
VLAN 50 と 60 は、すべてのスイッチ間のトランク リンク上に存在します SW3 のすべてのアクセス ポートは VLAN 50 用に設定され、SW1 は VTP サーバーです SW3 が VLAN 50 からのみフレームを受信することを保証するコマンドはどれですか?
A. SW1 (config)#vtp プルーニング
B. SW3(config)#vtp モード トランスペアレント
C. SW2(config)#vtp プルーニング
D. SW1 (config)#vtp モード トランスペアレント
Answer: A (メーッセージを残す**)**
SW3 には VLAN 60 がないため、この VLAN のトラフィック (SW2 から送信) を受信しないはずです。
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) でプルーニングを設定する必要があることにも注意してください。

最新問題**: 141**
IP アドレス 209 16b 201 2b を持つクライアントは、209 l6b.200.22b のポート 80 で Web サーバーにアクセスする必要があります。このトラフィックを許可します。エンジニアは、Web サーバーに接続するポートのインバウンド方向に適用されるアクセス制御リストにステートメントを追加する必要があります。どのステートメントがこのトラフィックを許可しますか?
A. tcp ホスト 209.165.200.225 を許可する lt 80 ホスト 209.165.201.25
B. tcp ホスト 209.165.200.225 ホスト 209.165.201.25 eq 80 を許可
C. tcp ホスト 209.165.201.25 ホスト 209.165.200.225 eq 80 を許可します。
D. tcp ホスト 209.165.200.225 eq 80 ホスト 209.165.201.25 を許可する
Answer: D (メーッセージを残す**)**

最新問題**: 142**
パケットが到着した順序でインターフェイスからパケットを送信する QoS キューイング方式はどれですか?
A. カスタム
B. 加重公平
C. FIFO
D. 優先度
Answer: C (メーッセージを残す**)**
説明


先入れ先出し (FIFO): FIFO には、トラフィックの優先順位やクラスの概念はありません。FIFO を使用すると、インターフェイスからのパケットの送信は、パケットが到着した順序で行われます。つまり、QoS はありません。

最新問題**: 143**
展示を参照してください。



R が CE ルーターであると仮定すると、R1 の Gi0/0 に割り当てられる VRF はどれですか?

A. VRF VPN_B

B. デフォルト VRF

C. 管理 VRF

D. VRF VPN_A

Answer: B (メーッセージを残す)

R1 の Gi0/0 の設定には特別なことはありません。R2 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の VRF は、シスコのグローバル ルーティング テーブルの概念に似ています。
IOS

最新問題: **144**

エンジニアは、WLAN でローカル Web 認証を構成しています。エンジニアは、Web ポリシーのレイヤ 3 セキュリティ オプションの下にある [認証] ラジオ ボタンを選択します。WLAN の Web 認証を提供するデバイスはどれですか?

A. ISE サーバー

B. ローカル WLC

C. RADIUS サーバー

D. アンカー WLC

Answer: B (メーッセージを残す)

次のステップは、内部 Web 認証用に WLC を設定することです。内部 Web 認証は、WLC のデフォルトの Web 認証タイプです。」上記のリンクの手順 4 では、この質問で説明されているようにセキュリティを構成します。したがって、この設定は内部 Web 認証用であると推測できます。
この段落は、リンク https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/69340-web-auth-config.html#c5 から引用したものです。

最新問題: **145**

展示を参照してください。

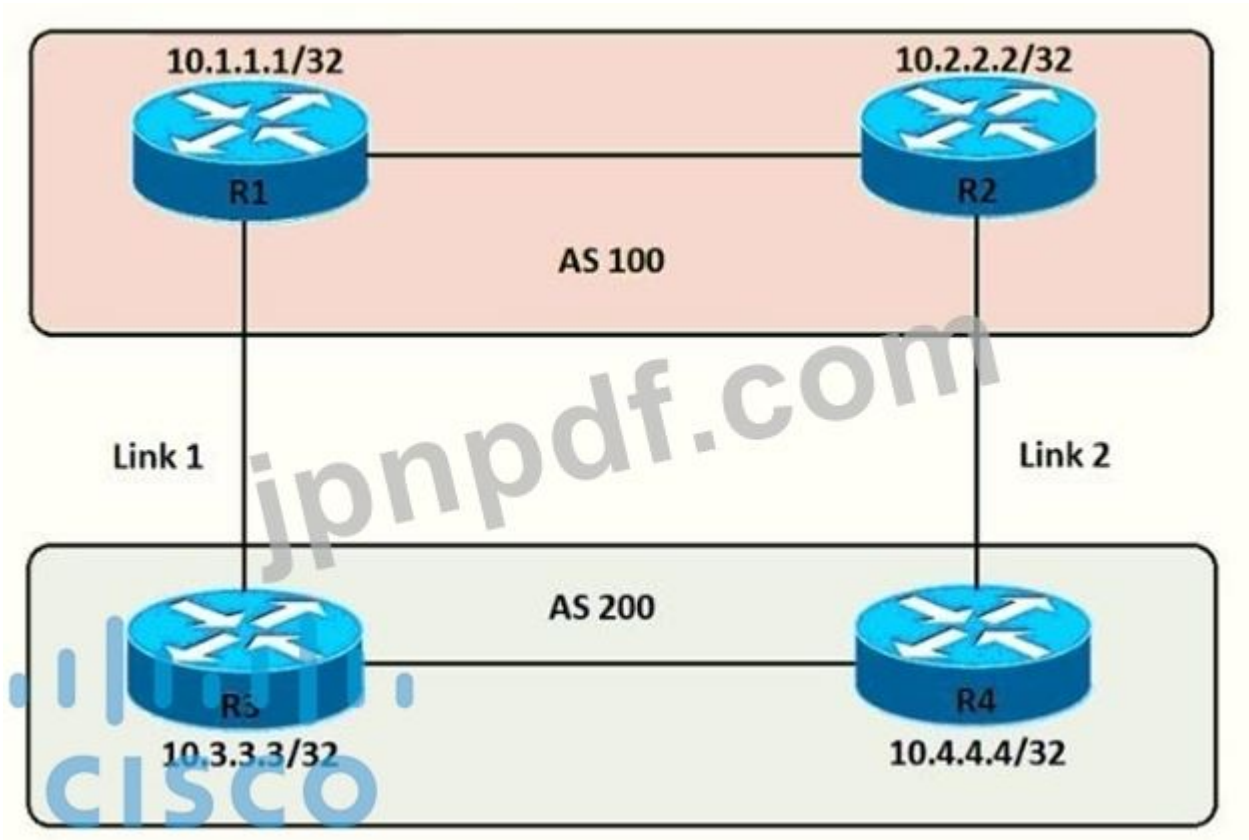
```
*Jun19 11:12: BGP(4):10.1.1.2 rcvd UPDATE w/ attr:nexthop 10.1.1.2, origin ?,
localpref 100,metric 0,extended community RT:999:999
*Jun19 11:12: BGP(4):10.1.1.2 rcvd 999:999:192.168.1.99/32,label 29–DENIED due to:
extended community not supported
```

PE3 で新しい VRF を作成しました。デバッグを有効にしました
ip bgp vpnv4 ユニキャストは PE1 で更新され、デバッグでルートを確認できますが、BGP VPNv4 テーブルでは確認できません。正しい2つのステートメントはどれですか? (2つ選んでください)

A. PE1 の VRF にルート ターゲット インポート 999:999 を設定すると、ルートが受け入れられます。
B. PE1 と PE3 の間で VPNv4 が構成されていない
C. address-family ipv4 vrf が PE3 で構成されていません
D. 自動経路フィルタリングにより、PE1 は経路を拒否します。
E. PE3 の VRF にルート ターゲット インポート 999:999 を設定すると、ルートが受け入れられます。
Answer: (解答を表示する**)**
説明
一部の PE ルーターは不要なルーティング情報を受信する可能性があるため、基本的な要件は、ルーターがこの情報をメモリに保持する必要がないように、PE ルーターへの入口で MP-iBGP 更新をフィルタリングできることです。
自動ルート フィルタリング機能は、このフィルタリング要件を満たします。この機能は、すべての PE ルーターでデフォルトで利用可能であり、有効にするために追加の構成は必要ありません。その機能は、PE の設定済み VRF のいずれとも一致しないルート ターゲット拡張コミュニティを含む VPN-IPv4 ルートを自動的にフィルタリングすることです。これにより、不要な VPN-IPv4 ルートがサイレントに効果的に破棄されるため、PE がメモリに格納する必要がある情報の量が削減されます -> 回答 「自動ルート フィルタリングにより、PE1 はルートを拒否します」が正解です。

最新問題: **146**
グラフィカル ユーザー インターフェイス、テキスト、アプリケーション、電子メール 説明が自動的に生成されます 別紙を参照してください。スクリプトを実行すると、展示に出力が表示されます。スクリプトの最初の行は何ですか?
A. ncclient マネージャーのインポート
B. ncclient インポート マネージャーから
C. ncclient インポートから *
D. インポート マネージャー
Answer: C (メーッセージを残す**)**

最新問題: **147**
展示を参照してください。

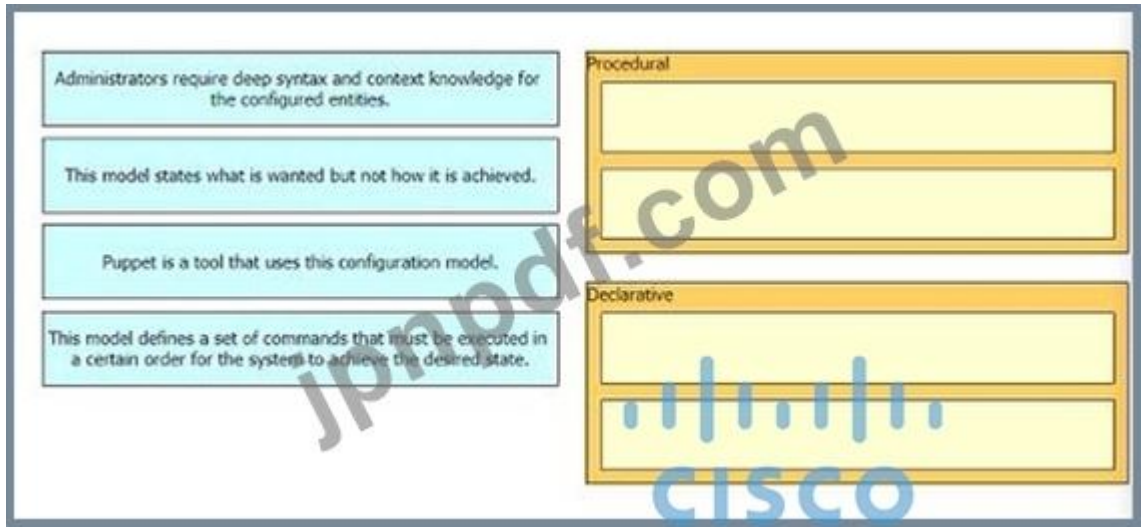


エンジニアは、AS 200 を出るすべてのトラフィックがリンク 2 をエントリ ポイントとして選択するようにする必要があります。すべての BGP ネイバー関係が形成され、どのルーターでも属性が変更されていないと仮定すると、どの構成でタスクが達成されますか?

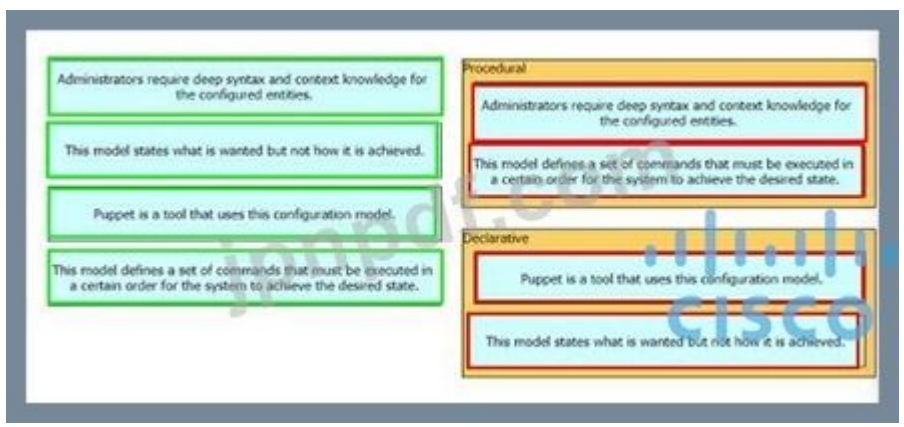
A. オプション A
B. オプション B
C. オプション C
D. オプション D
Answer: (解答を表示する)

説明
R3 は、複数の AS 100 を使用して BGP アップデートを R1 にアドバタイズするため、R3 は、R3 を経由して AS 200 に到達するパスが R2 よりも遠いと考えているため、R3 はトラフィックを AS 200 に転送するために R2 を選択します。

最新問題: **148**
10 個の特性を右側の構成モデルにドラッグ アンド ドロップします。



Answer:

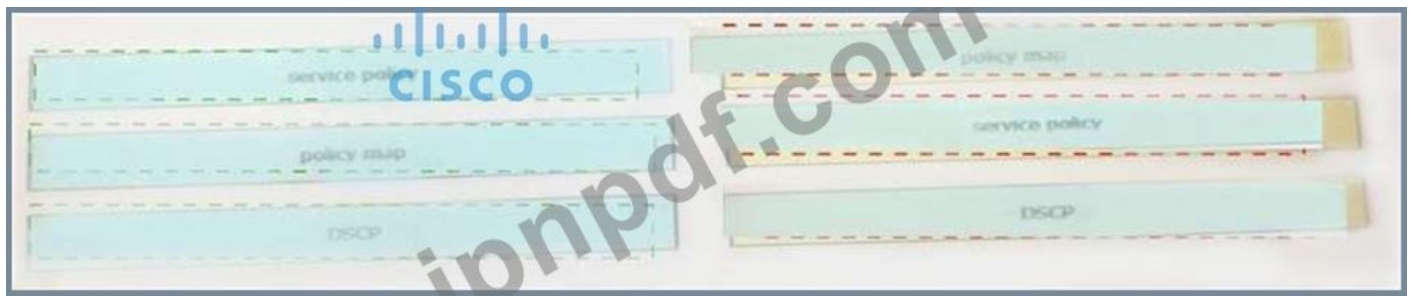


最新問題: **149**
仮想コンポーネントを左側から右側の欺瞞にドラッグ アンド ドロップします。

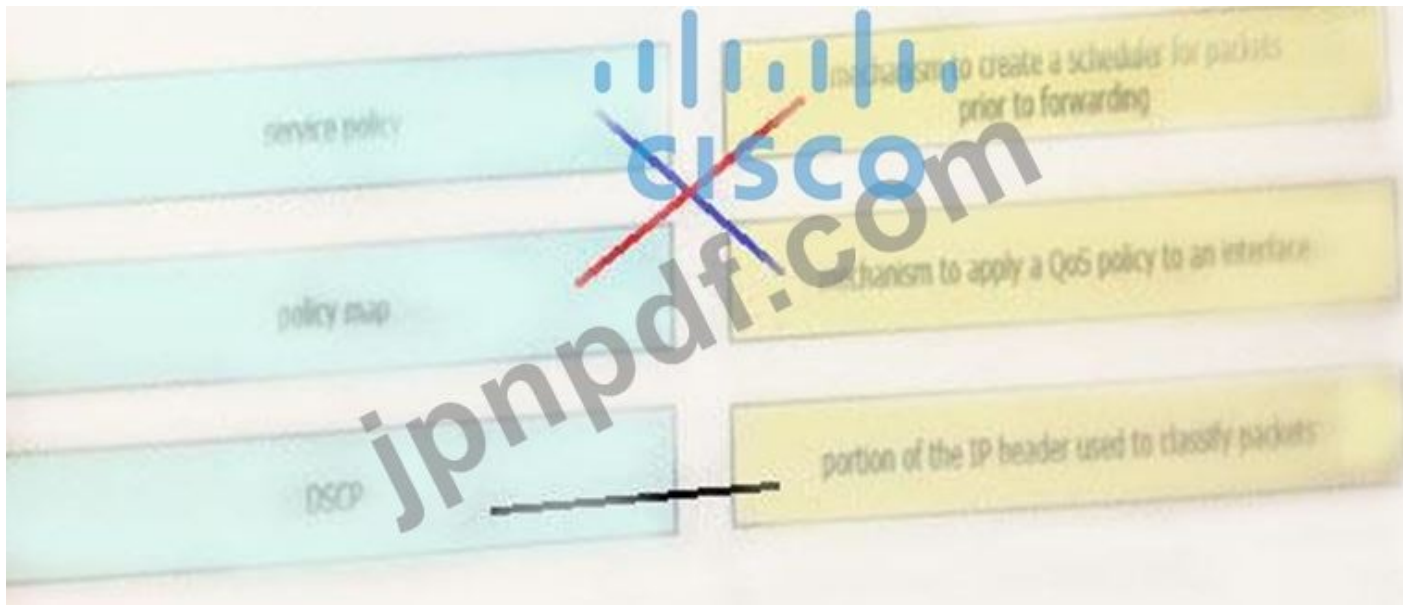
Answer:

最新問題: **150**
Qos メカニズムを左から右の正しい説明にドラッグ アンド ドロップします。

Answer:



説明



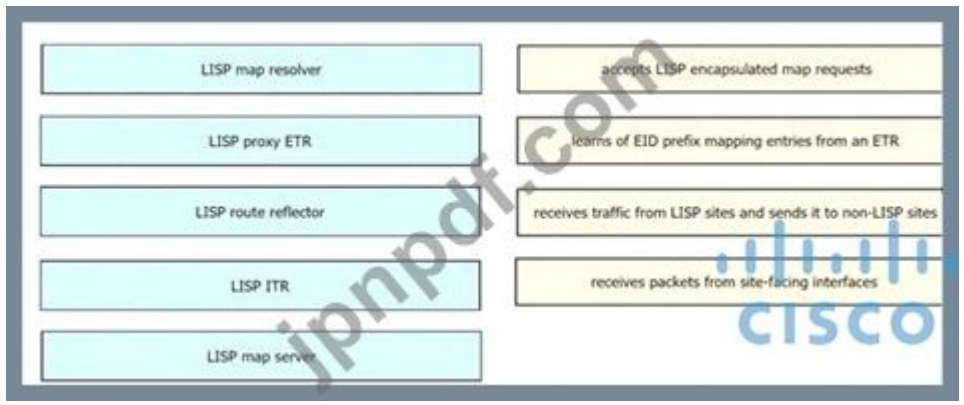
最新問題: **151**
展示を参照してください。

SW2 と SW3 の間にポート チャネルが設定されます。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?

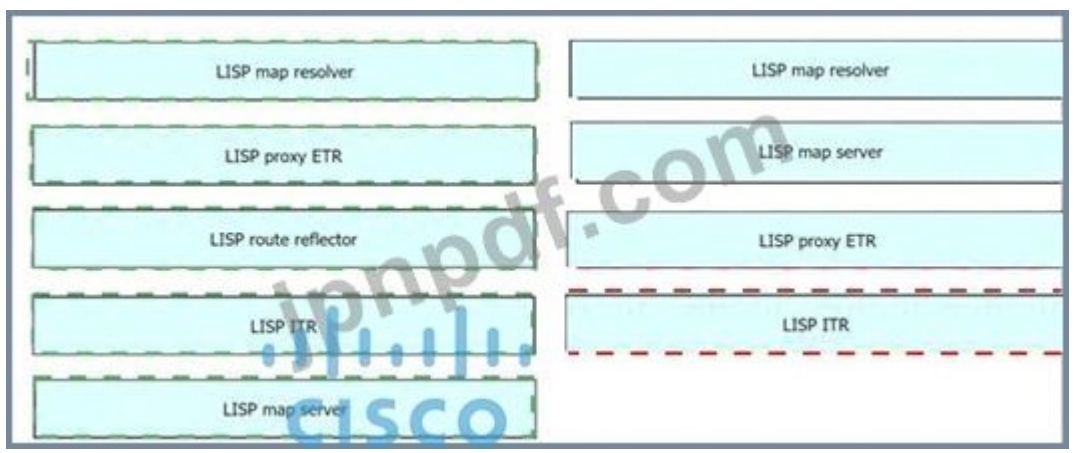
A. SW2 のポート チャネルは、互換性のないプロトコルを使用しています。
B. ポート チャネル トランクがネイティブ VLAN を許可していません。
C. ポートチャネルは auto に設定する必要があります。
D. ポート チャネル インターフェイスのリード バランスは、src-mac に設定する必要があります。
Answer: (解答を表示する**)**
説明
Cisco スイッチは、Cisco 独自のプロトコルである PAgP で構成されているため、Cisco 以外のスイッチは通信できませんでした。

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら:
https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

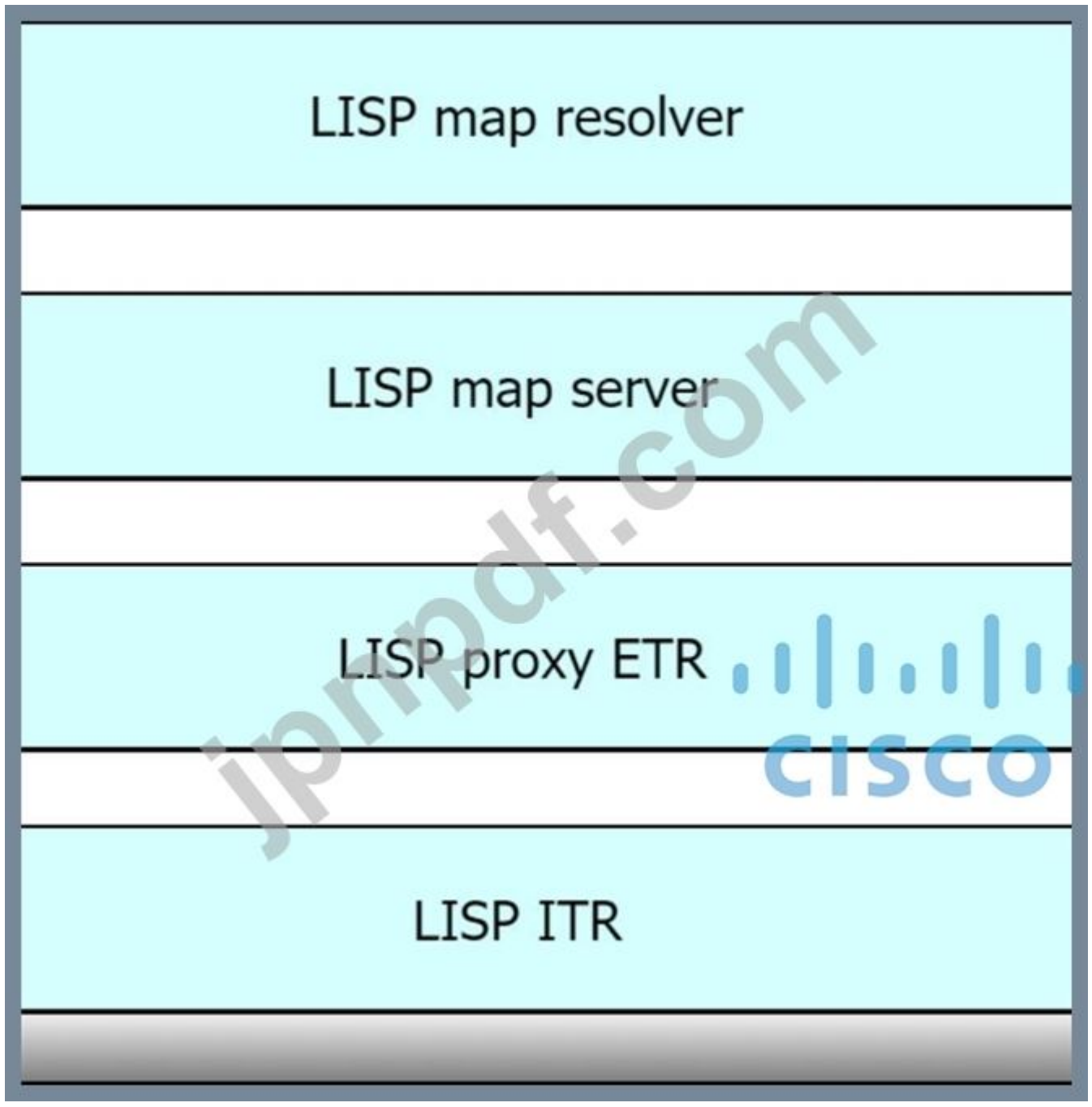
最新問題: **152**
LISP コンポーネントを左側から右側の機能にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。


LISP map resolver
LISP proxy ETR
LISP route reflector
LISP ITR
LISP map server
accepts LISP encapsulated map requests
learns of EID prefix mapping entries from an ETR
receives traffic from LISP sites and sends it to non-LISP sites
receives packets from site-facing interfaces

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

説明



jpnpdf.com
cisco

+ LISP カプセル化されたマップ要求を受け入れます: LISP マップ リゾルバー
+ ETR からの EID プレフィックス マッピング エントリの学習: 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: LISP プロキシ ETR
+ サイトに面した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 Egress Tunnel Router (ETR) の RLOC の宛先 IP アドレスを持つ追加のヘッダーを使用して元のパケットをカプセル化する機能です。

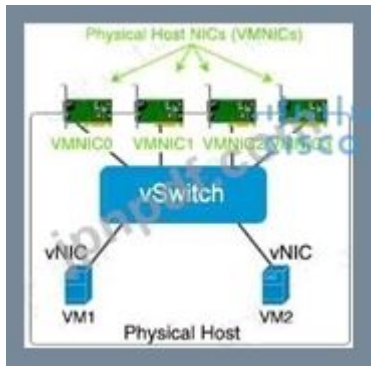
カプセル化後、元のパケットは LISP パケットになります。

ETR は、LISP カプセル化パケットを受信し、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ので、「map-server」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 LISP 以外のサイトにトラフィックを送信する必要がある場合に使用されますが、パケット ソースとしてルーティング可能な EID を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ます。PETR は ETR と同じように機能しますが、非 LISP サイトの宛先にトラフィックを送信する EID に対して機能します。
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、定期的に Map-Register メッセージを構成済みのすべてのマップ サーバーに送信します。
Map Resolver (MR): 通常は ITR からの LISP Encapsulated Map Request 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: **153**
エンジニアは、VTY 回線のパスワードを肩越しの攻撃から保護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. 行 vty 0 15 p3ssword XD822j
B. ユーザー名 netadmin シークレット 7$1$42J36k33008Pyh4QzwXyZ4
C. ユーザー名 netadmin シークレット 9 9vFpMf8elb4RVV8$seZ/bDA
D. サービス パスワード暗号化
Answer: (解答を表示する**)**

最新問題: **154**
仮想マシン環境でブロードキャスト放射が発生する理由を 2 つ挙げてください。2つ選んでください。）
A. ブロードキャスト パケットを処理するには、vSwitch がサーバーの 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 モードで通信します。
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: (解答を表示する**)**
ブロードキャスト放射は、コンピューター ネットワーク上のブロードキャストおよびマルチキャスト 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 ドメイン内で見られるブロードキャスト 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。そのため、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 -> VLAN を使用してブロードキャスト放射を減らす必要があります。
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への (VLAN を拡張するための) トランクの使用です。
ハイパーバイザーでの仮想化の構造に関する注意:
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 が外界へのレイヤー 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、物理スイッチに出向かなくてもレイヤー 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 から入るフレームは、VMNIC の外には出ません。
別の VMNIC カードからの物理ホスト。

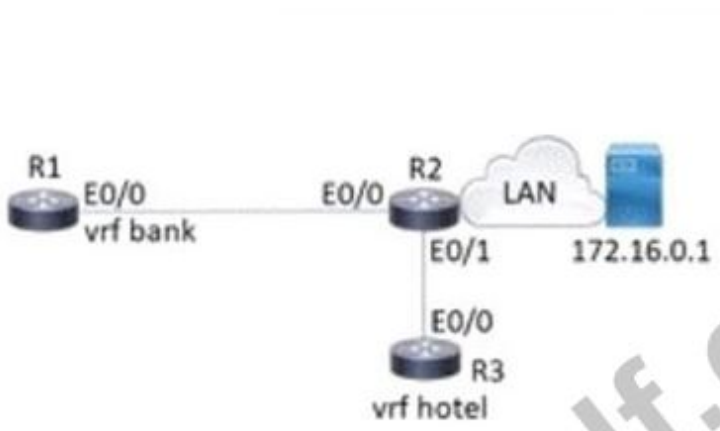
最新問題: **155**
パケットが到着した順序でインターフェイスからパケットを送信する QoS キューイング方式はどれですか?
A. カスタム
B. 加重公平
C. FIFO
D. 優先度
Answer: (解答を表示する**)**

- FIFO (first-in, first-out). FIFO entails no concept of priority or classes of traffic. With FIFO, transmission of packets out the interface occurs in the order the packets arrive.

先入れ先出し (FIFO): FIFO には、トラフィックの優先順位やクラスの概念はありません。FIFO を使用すると、インターフェイスからのパケットの送信は、パケットが到着した順序で行われます。つまり、QoS はありません。

最新問題: **156**
Cisco SD-WAN 導入における VPN とは何ですか?
A. コントロール プレーン情報を伝送するために使用される仮想チャネル
B. 2 つの異なるサービス間の共通の交換ポイント
C. SD-WAN ファブリックでトラフィックの分離とセグメンテーションを提供する仮想化環境
D. SD-WAN ファブリックの特定の場所で提供される一連のサービスを識別する属性
Answer: C (メーッセージを残す**)**

最新問題: **157**




```
vrf definition hotel
 address-family ipv4
 exit-address-family

vrf definition bank
 address-family ipv4
 exit-address-family

interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.4 255.255.0.0

interface Ethernet0/1
 vrf forwarding hotel
 ip address 172.1.0.5 255.255.0.0

router ospf 42 vrf bank
 router-id 1.1.1.1
 network 172.16.0.0 0.0.255.255 area 0

router ospf 43 vrf hotel
 router-id 3.3.3.3
 network 172.16.0.0 0.0.255.255 area 0

R1:
vrf definition bank
!
 address-family ipv4
 exit-address-family
```

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、R にどの構成を適用する必要がありますか?

A.
```
interface Ethernet0/0
 ip address 172.16.0.7 255.255.0.0
router ospf 44 vrf hotel
 network 172.16.0.0 255.255.0.0
```

B.
```
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf bank
 network 172.16.0.0 255.255.0.0
```

C.
```
interface Ethernet0/0
 vrf forwarding hotel
 ip address 172.16.0.7 255.255.0.0

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

D.

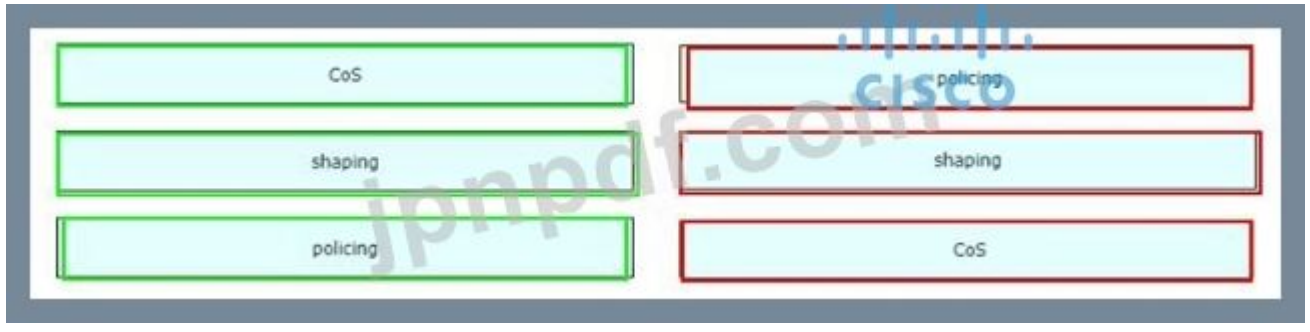
```
interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.7 255.255.0.0

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

Answer: (解答を表示する)

最新問題: **158**

左側の QoS メカニズムを右側の説明にドラッグ アンド ドロップします。

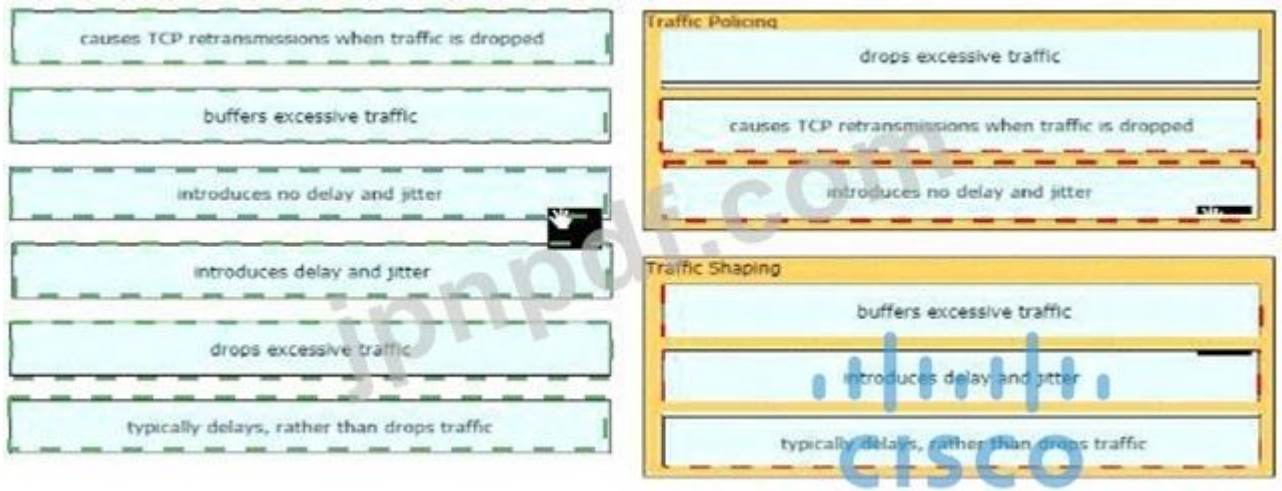
Answer:



最新問題: **159**

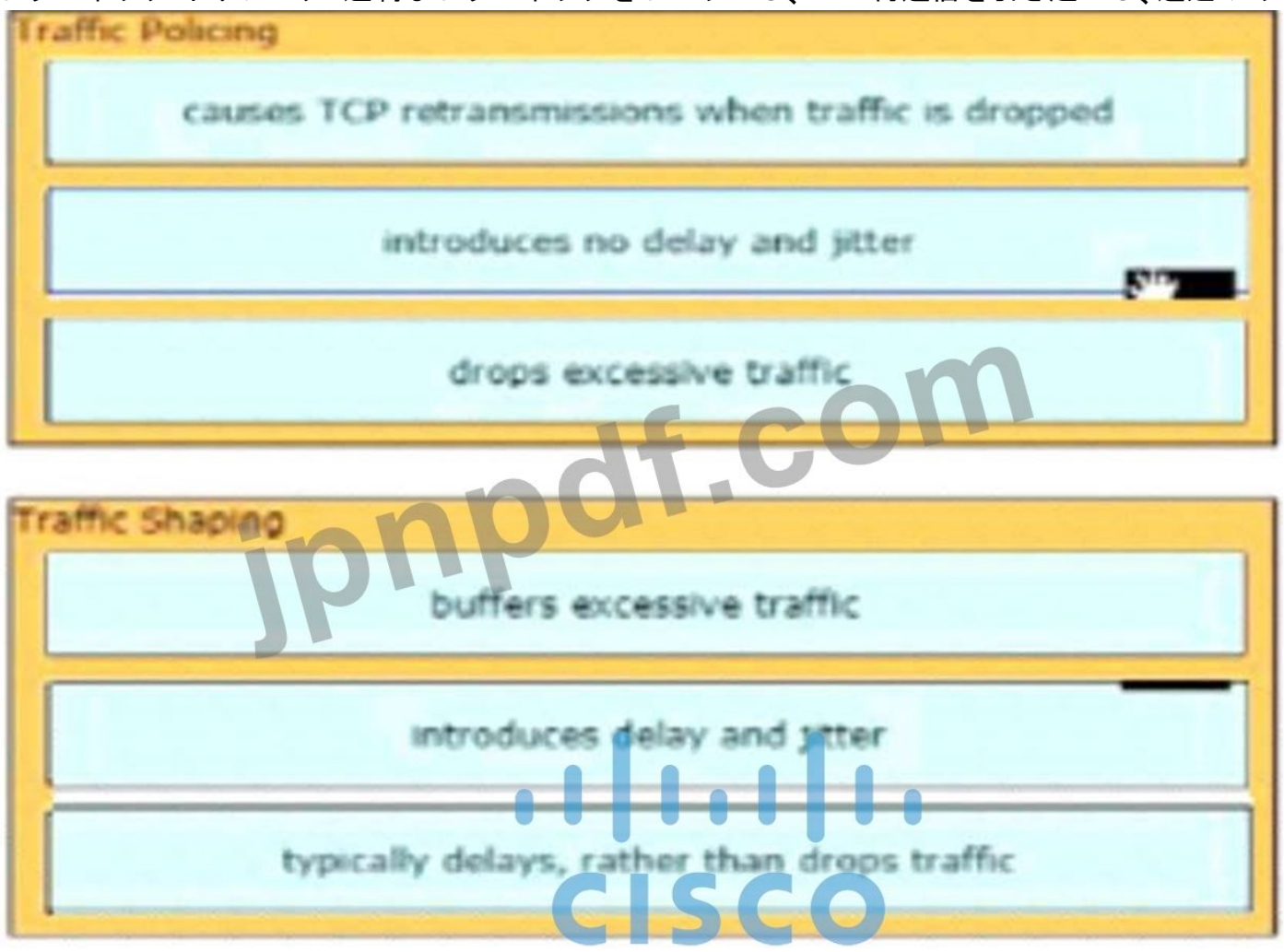
左側の説明を右側の正しい QoS コンポーネントにドラッグ アンド ドロップします。

Answer:



説明

トラフィック ポリシング: 過剰なトラフィックをドロップし、TCP 再送信を引き起こし、遅延/ジッターを導入しません



最新問題: 160

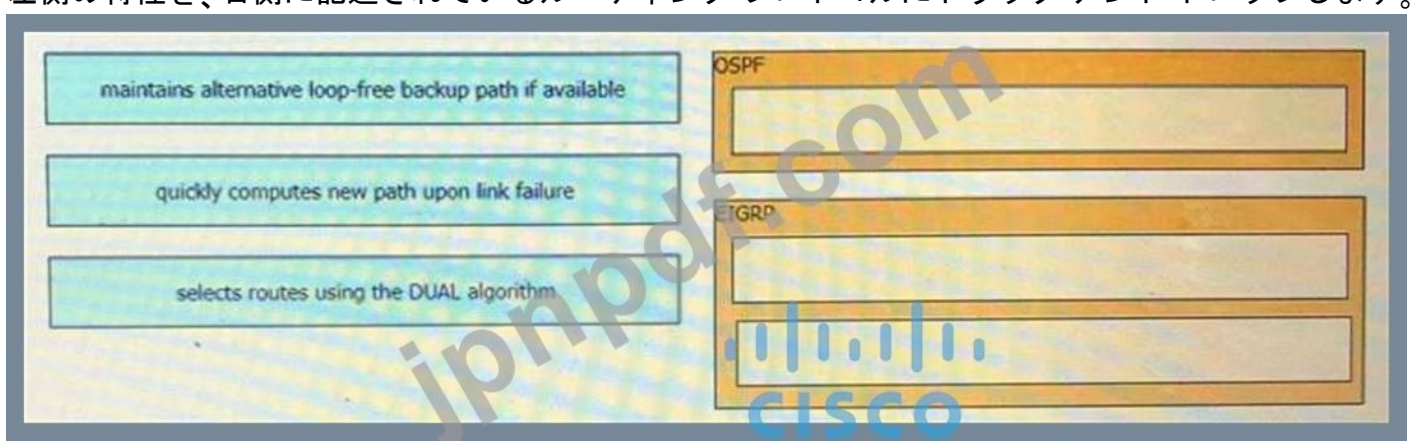
JSON オブジェクト {"cat_9k": "FXS193202SE") を返すには、Python 関数にどの行を追加する必要がありますか?

```
import json
def get_data():
    test_json = """
    {
        "response": [{
        "managementIpAddress": "10.10.2.253",
        "memorySize": "3398345152",
        "serialNumber": "FXS1932Q2SE",
        "softwareVersion": "16.3.2",
        "hostname": "cat_9k"
        }],
        "version": "1.0"
    }
    """
```

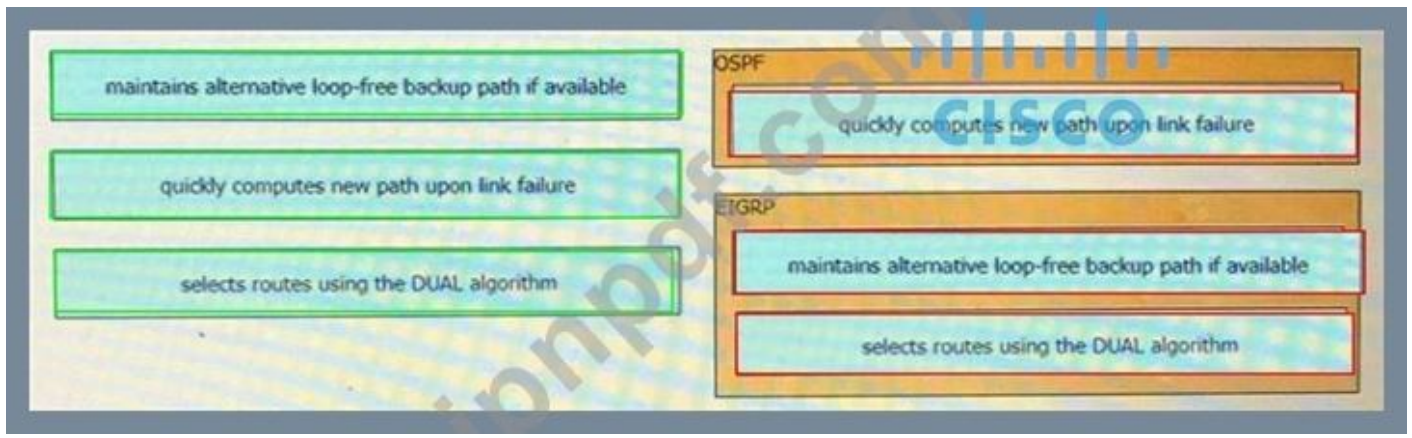
```
return (json.dumps({d['hostname']: d['serialNumber'] for d in json.loads(test_json)['response']}))
return (json.dumps({for d in json.loads(test_json)['response']: d['hostname']: d['serialNumber']}))
return (json.loads({d['hostname']: d['serialNumber'] for d in json.dumps(test_json)['response']}))
return (json.loads({for d in json.dumps(test_json)['response']: d['hostname']: d['serialNumber']}))
```

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

最新問題**: 161**
左側の特性を、右側に記述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:

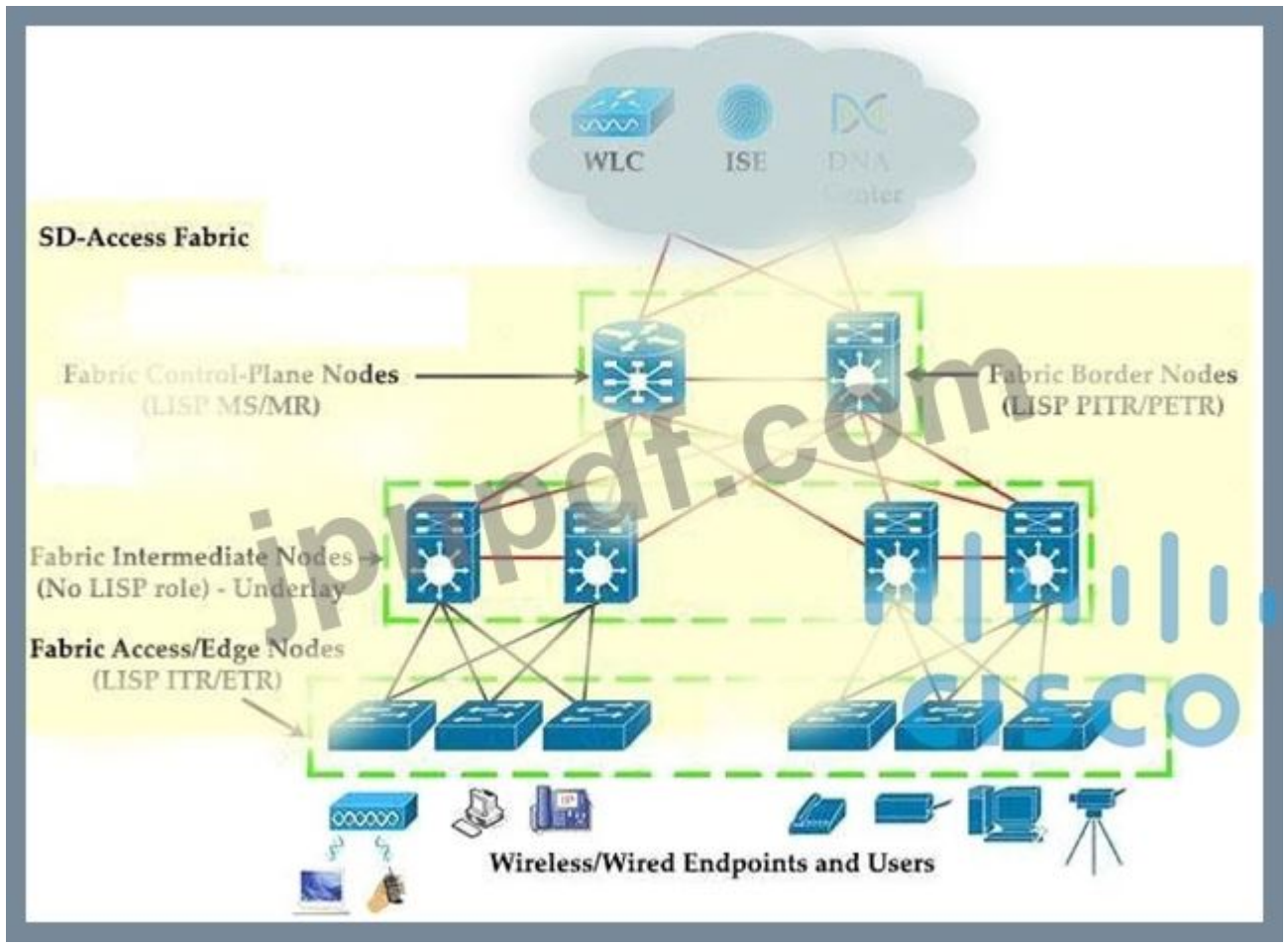


最新問題: **162**
WLC への接続が失われた後、ネットワークに接続されているワイヤレス ユーザが作業を継続できる Cisco FlexConnect の状態はどれですか?
A. 認証ダウン/スイッチダウン
B. Authentication-Central/Switch-Local
C. 認証 - ダウン/スイッチ ローカル
D. Authentication-Central/Switch-Central
Answer: C (メーッセージを残す**)**
動作モード
FlexConnect AP には 2 つの動作モードがあります。
接続モード: WLC は到達可能です。このモードでは、FlexConnect AP は WLC との CAPWAP 接続を備えています。
スタンドアロン モード :WLC に到達できません。FlexConnect が WLC との CAPWAP 接続を失ったか、確立できませんでした。ブランチとその中央サイト間の WAN リンクの停止は、このような動作モードの例です。
FlexConnect の状態
FlexConnect WLAN は、その構成とネットワーク接続に応じて、次の定義された状態のいずれかに分類されます。
Authentication-Central/Switch-Central: この状態は、802.1X、VPN、または Web などの集中認証方式を使用する WLAN を表します。ユーザ トラフィックは、CAPWAP（中央スイッチング）経由で WLC に送信されます。この状態は、FlexConnect が接続モードの場合にのみサポートされます。
Authentication Down/Switching Down: FlexConnect AP がスタンドアロン モードの場合、中央スイッチ WLAN はビーコンを送信したり、プローブ要求に応答したりしなくなりました。既存のクライアントの関連付けが解除されます。
Authentication-Central/Switch-Local: この状態は、集中認証を使用する WLAN を表しますが、ユーザー トラフィックはローカルでスイッチングされます。この状態は、FlexConnect AP が接続モードの場合にのみサポートされます。
Authentication-Down/Switch-Local: 中央認証を必要とする WLAN は、新しいユーザーを拒否します。既存の認証済みユーザーは、構成されている場合、セッション タイムアウトまでローカルで切り替えられ続けます。WLAN は、WLAN に関連付けられている既存のユーザーがなくなるまで、引き続きビーコンを送信し、プローブに応答します。この状態は、AP がスタンドアロン モードになった結果として発生します。
Authentication-local/switch-local: この状態は、オープン、静的 WEP、共有、または WPA2 PSK セキュリティ メソッドを使用する WLAN を表します。ユーザー トラフィックはローカルでスイッチングされます。これらは、FlexConnect がスタンドアロン モードになった場合にローカルでサポートされる唯一のセキュリティ メソッドです。WLAN は引き続きビーコンを送信し、プローブに応答します。既存のユーザーは接続されたままになり、新しいユーザーの関連付けが受け入れられます。AP が接続モードの場合、これらのセキュリティ タイプの認証情報が WLC に転送されます。

最新問題: **163**
ファイアウォールを通過するフローをブロックする NGFW モードはどれですか?

A. パッシブ
B. タップ
C. インラインタップ
D. インライン
Answer: D (メーッセージを残す**)**
参照：
Firepower Threat Defense（FTD）は、ルーテッド、スイッチド、インライン ペア、タップ付きインライン ペア、パッシブ、パッシブ（ERSPAN）の 6 つのインターフェイス モードを提供します。
インライン ペア モードが使用されている場合、パケットはインラインで処理されるため、ブロックされる可能性があります インライン ペア モードを使用している場合、パケットは主に FTD Snort エンジンを通過します実際のトラフィックは変更されずに FTD を通過します
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuringfirepower-threat-defense-int.html

最新問題**: 164**
Cisco SD-Access ファブリックの 2 つのデバイス ロールは何ですか？（2つ選んでください。）
A. コア スイッチ
B. vBond コントローラー
C. エッジ ノード
D. アクセススイッチ
E. 境界ノード
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 ロールがあります。
+ 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 ボーダー ノード: このファブリック デバイス (コア レイヤー デバイスなど) は、外部のレイヤー 3 ネットワークを SDA ファブリックに接続します。
+ ファブリック エッジ ノード: このファブリック デバイス (アクセスまたはディストリビューション レイヤー 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 アクセス 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。



jpnpdf.com

最新問題: **165**

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 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ギング」を取得します

B. イベント マネージャ アプレット ブーム

イベント syslog パターン「UP」

action 1.0 syslog priority direct msg 'コンソールに直接記録'

C. イベント マネージャ 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「ログをコンソールに直接出力」します

D. イベント マネージャ 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ギング'

Answer: B (メーッセージを残す**)**

Embedded Event Manager（EEM）アプレットがトリガーされたときにデータをローカル tty に直接出力するアクションをイネーブルにするには、アプレット コンフィギュレーション モードで action puts 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。同期アプレットに対するこのコマンドの出力は、syslog をバイパスして tty に直接表示されます。
参考 :a1.html

最新問題: **166**
LISP でサポートされている 2 つのコンポーネントはどれですか? (2 つ選択)
A. プロキシ ETR
B. 出口トンネル ルーター
C. ルート リフレクター
D. HMAC アルゴリズム
E. スポーク
Answer: A,B (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html 出口トンネルルーター (ETR) は、サイトをコア ネットワーク (インターネットなど) の LISP 対応部分に接続し、サイトの EID から RLOC へのマッピングを発行し、Map-Request メッセージに応答し、LISP カプセル化されたユーザーをカプセル化解除して配信します。サイトのエンド システムへのデータ。
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、LISP サイトが、ルーティング不可能な 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接続されている場合に使用されます。PETR は ETR と同じように機能しますが、非 LISP サイトの宛先にトラフィックを送信する EID に対して機能します。

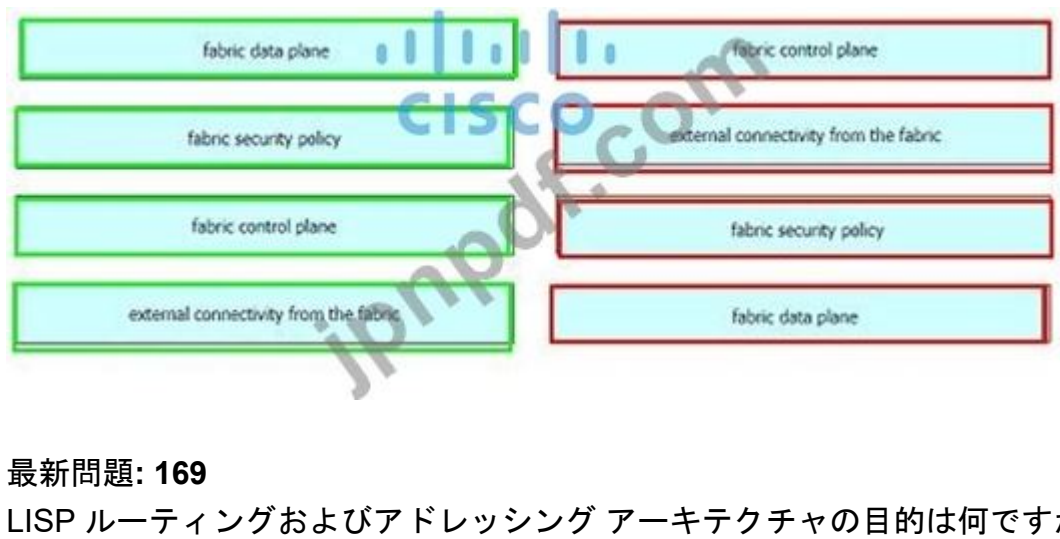
有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら:
https://www.goshiken.com/Cisco/350-401-mondaishu.html (**36130%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **167**
VRRP に関する 2 つの記述のうち、正しいものはどれですか？ 2つ選んでください。）
A. IP プロトコル番号は 115 です。
B. マルチキャストアドレス 224.0.0.9 が割り当てられます。
C. MD5 認証と SHA1 認証の両方をサポートします。
D. VRRP プロトコルには 3 つのバージョンが定義されています。

E. VRRP パケットの TTL は 255 である必要があります。
F. マルチキャストアドレス 224.0.0.18 が割り当てられます。
Answer: E,F (メーッセージを残す**)**

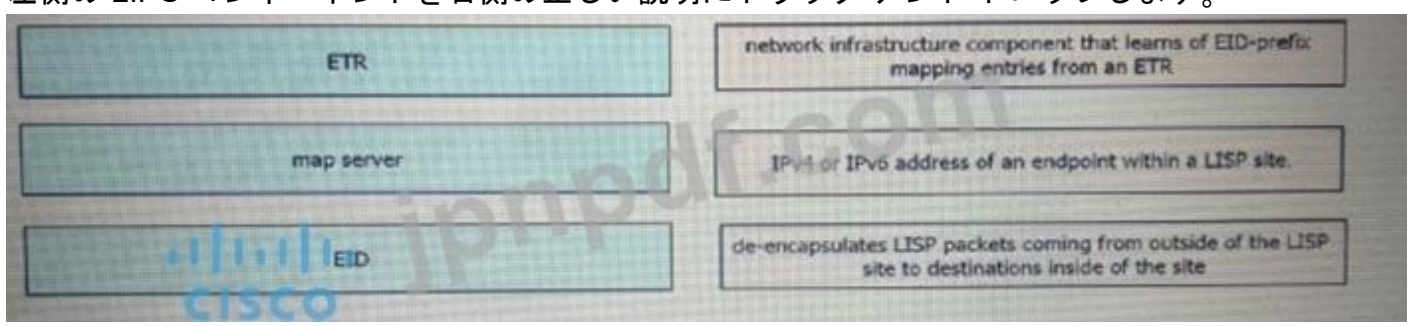
最新問題**: 168**
Cisco SD-Access ソリューションの領域を左側から右側の使用するプロトコルにドラッグ アンド ドロップします。

Answer:

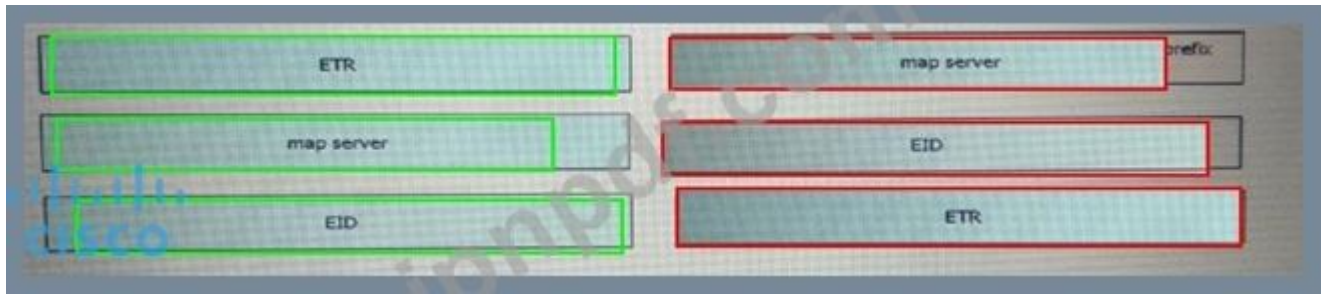


最新問題**: 169**
LISP ルーティングおよびアドレッシング アーキテクチャの目的は何ですか?
A. ネットワーク ノードごとに 2 つのエントリを作成します。1 つは ID 用、もう 1 つはネットワーク上の場所用です。
B. ブロードキャストおよびマルチキャスト フレームをネットワーク全体に配信するために使用されるヘッドエンド レプリケーションを作成します。
C. ルーティング テーブルの複数のインスタンスが同じルーター内に共存できるようにします。
D. カプセル化により、LISP をネットワーク仮想化オーバーレイとして適用できます。
Answer: A (メーッセージを残す**)**

最新問題**: 170**
左側の LIPS コンポーネント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**: 171**
GRE トンネルがダウンし、エラー メッセージ %TUN-5-RECUR DOWN:

Tunnel0 temporarily disabled due to recursive routing error.

エラーの考えられる原因を説明する 2 つのオプションはどれですか? (2つ選んでください)
A. トンネルでリンク フラッピングが発生しています
B. トンネルに誤った宛先 IP アドレスが構成されている
C. トンネル モードとトンネル IP アドレスが正しく構成されていません
D. 経路フラッピングによりネットワークが不安定
E. トンネルの宛先がトンネル インターフェイスの外にルーティングされています。
Answer: D,E (メーッセージを残す**)**
説明
%TUN-5-RECURDOWN: Tunnel0 temporary disabled due to recursive routing エラー メッセージは、Generic Routing Encapsulation (GRE) トンネル ルーターが再帰ルーティングの問題を検出したことを意味します。この状態は通常、次のいずれかの原因によるものです。
+ ルーターがトンネル インターフェイス自体を使用してトンネルの宛先アドレスにルーティングしようとする構成ミス (再帰ルーティング)
+ ネットワークの他の場所でのルート フラッピングによって引き起こされる一時的な不安定性
参照: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routingprotocol-eigrp/22327-gre-flap.html

最新問題**: 172**
展示を参照してください。

```
R1#show ip bgp sum
BGP router identifier 1.1.1.1, local AS number 65001
<output omitted>

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.50.2    4        65002       0       0        1    0    0 00:00:46 Idle (Admin)
```

ネイバーの状態を Idle (Admin) から Active に変更するコマンド セットはどれですか?
A)

```
R1(config)#router bgp 65002
R1(config-router)#neighbor 192.168.50.2 activate
```

B)

```
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 activate
```

ハ)

```
R1(config)#router bgp 65001
R1(config-router)#no neighbor 192.168.50.2 shutdown
```

D)

```
R1(config)#router bgp 65001
R1(config-router)#neighbor 192.168.50.2 remote-as 65001
```

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

最新問題**: 173**
マスター コントローラ モードの WLC の特徴は何ですか?
A. WLAN に参加するすべての新しい AP は、マスター コントローラーに割り当てられます。
B. マスター コントローラーは、接続しているすべてのクライアントを他のコントローラーに負荷分散する役割を担います。
C. すべてのワイヤレス LAN コントローラーは、マスター コントローラーによって管理されます。
D. マスター コントローラーの設定は、すべての無線 LAN コントローラーで実行されます。
Answer: A (メーッセージを残す**)**
説明
WLC でマスター コントローラ モードを使用する必要があるのはいつですか? - マスター コントローラが有効になっている場合、プライマリ、セカンダリ、またはターシャリ コントローラが割り当てられていない新しく追加されたすべてのアクセス ポイントは、同じサブネット上のマスター コントローラに関連付けられます。

最新問題**: 174**
saltstack と ansible の違いは何ですか?
A. SaltStack は SSH を使用して Cisco デバイスと対話しますが、Ansible はイベント バスを使用します。
B. SaltStack は minion で構築され、Ansible は YAML で構築されます。
C. SaltStack は API プロキシ エージェントを使用して Cisco ボックスをエージェント モードでプログラムしますが、Ansible は Telnet 接続を使用します。
D. SaltStack はボックスで Ansible エージェントを使用しますが、Ansible はボックスで Telnet サーバーを使用します。
Answer: C (メーッセージを残す**)**

最新問題**: 175**
展示を参照してください。

```
aaa new-model
aaa authentication login authorizationlist tacacs+
tacacs-server host 192.168.0.202
tacacs-server key ciscotestkey
line vty 04
login authentication authorizationlist
```

この構成の効果は何ですか?
A. デバイスは、192.168.0.202 のユーザーがパスワード ciscotestkey を使用して vty 回線 0 ～ 4 に接続できるようにします。
B. デバイスは、vty 回線 0 ～ 4 に接続するすべてのユーザーを TACACS+ に対して認証します。
C. デバイスは、192.168.0.202 のユーザーのみが vty 回線 0 ～ 4 に接続できるようにします。
D. ユーザーが vty 回線 0 ～ 4 に接続しようとすると、デバイスは TACACS に対してユーザーを認証します。
+ ローカル認証が失敗した場合。
Answer: B (メーッセージを残す**)**
解説 参考：

最新問題**: 176**
展示を参照してください。

```
switch1(config)# interface GigabitEthernet 1/1
switch1(config-if)# switchport mode trunk
switch1(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-90
switch1(config)# exit
switch1(config)# monitor session 1 source vlan 10
switch1(config)# monitor session 1 destination remote vlan 70

switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)# switchport mode trunk
switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,80-90
switch2(config)# exit
switch2(config)# monitor session 2 source remote vlan 70
switch2(config)# monitor session 2 destination interface GigabitEthernet1/1
```

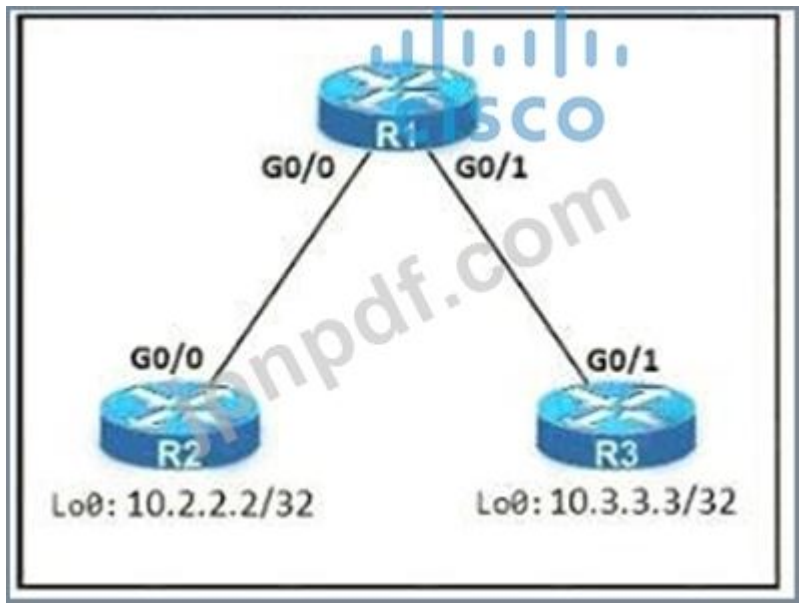
ネットワーク管理者は、スイッチ 1 とスイッチ 2 の間の問題をトラブルシューティングするために RSPAN を構成しました。スイッチは、インターフェイス GigabitEthernet 1/1 を使用して接続されています 外部パケット キャプチャ デバイスは、swich2 インターフェイス GigabitEthernet1/2 に接続されています この設定を完了するために追加する必要がある 2 つのコマンドはどれですか?
(2つ選んでください)

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

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

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

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

Answer: (解答を表示する**)**

最新問題**: 177**
展示を参照してください。



エンジニアは、週末の時間帯にルーター R3 のループバック インターフェイスからルーター R2 のループバック インターフェイスへの Telnet トラフィックを拒否する必要があります。ルーター R3 と R2 のループバック インターフェイス間の他のすべてのトラフィックは、常に許可する必要があります。このタスクを実行するコマンドはどれですか?

A)

```
R3(config)#time-range WEEKEND
R3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59

R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R3(config)#access-list 150 permit ip any any time-range WEEKEND

R3(config)#interface G0/1
R3(config-if)#ip access-group 150 out
```

B)

```
R1(config)#time-range WEEKEND
R1(config-time-range)#periodic Friday Sunday 00:00 to 00:00

R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R1(config)#access-list 150 permit ip any any

R1(config)#interface G0/1
R1(config-if)#ip access-group 150 in
```

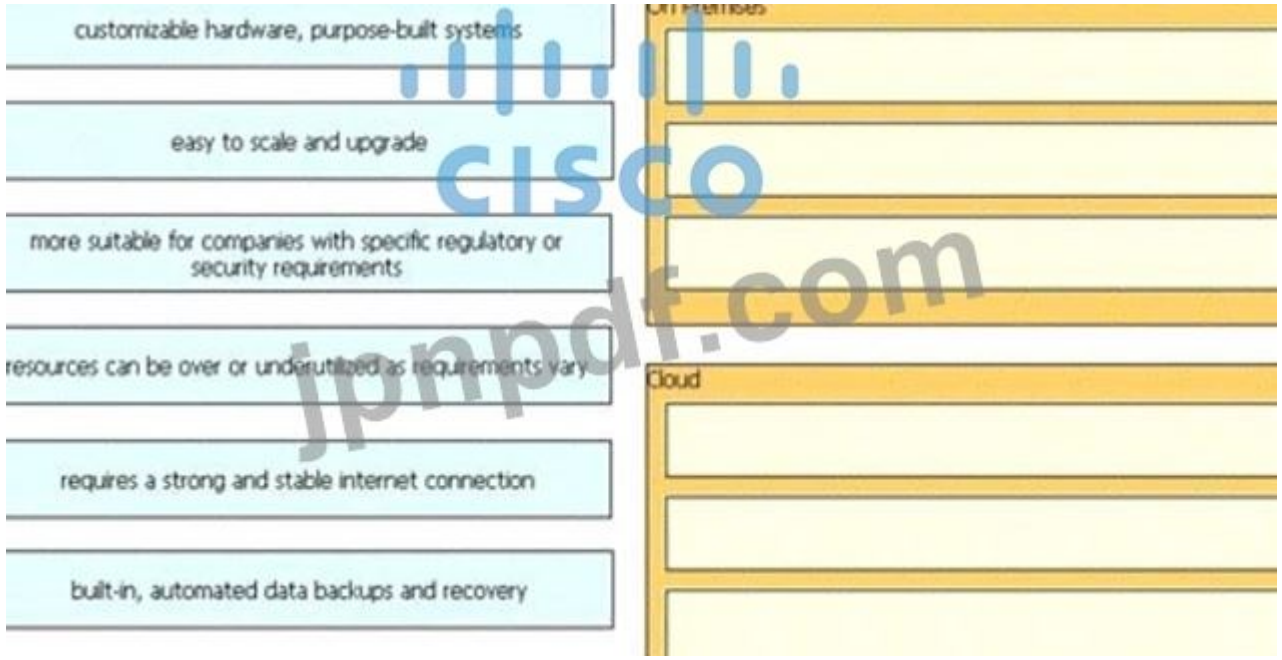
C)

```
R1(config)#time-range WEEKEND
R1(config-time-range)#periodic weekend 00:00 to 23:59

R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R1(config)#access-list 150 permit ip any any

R1(config)#interface G0/1
R1(config-if)#ip access-group 150 in
```

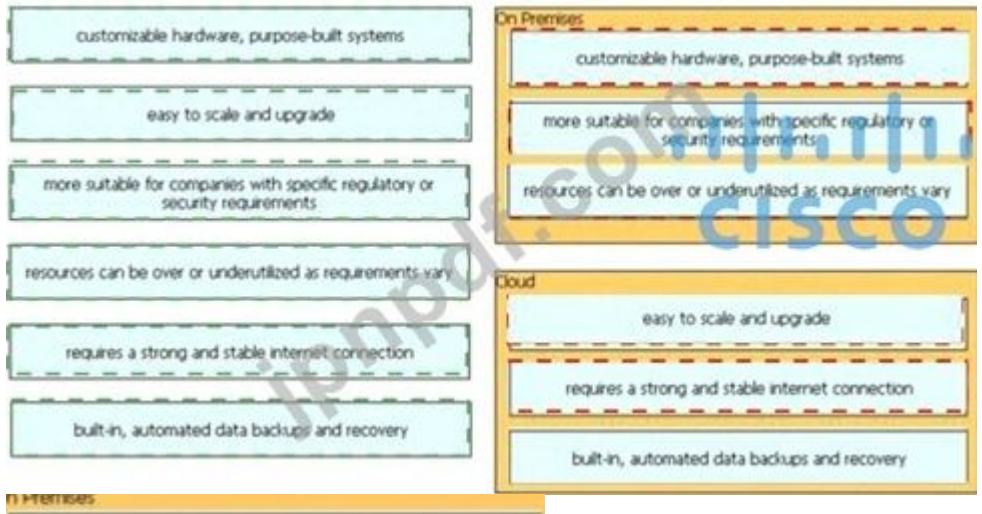
D)

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
ローカル ルータ (この場合は R3)から発信されたトラフィックをフィルタリングできないため、R1 または R2 でのみ ACL を設定できます。 週末の時間」とは、土曜日の朝から日曜日の夜までを意味するため、 定期的な週末の 00:00 から 23:59」に設定する必要があります。
注: 時間は 24 時間制 (hh:mm) で指定されます。時間は 0 から 23 の範囲で、分の範囲は 0 から 59 です。

最新問題: **178**
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: **179**
展示を参照してください。ネットワーク エンジニアは R1 で NAT を設定し、show コマンドを入力して設定を確認します。出力で何が確認されますか?
A. 160.1.1 1 から 10.1.1.10 への Telnet が開始されました。
B. 最初のポケットによって NAT がトリガーされ、NAT テーブルにエントリが追加されました
C. R1 は NAT 過負荷パラメータで構成されています
D. PAT 過負荷パラメータで構成された R1
Answer: B (メーッセージを残す**)**

最新問題: **180**
ルーターが受け入れる SSH トラフィックの量を 100 kbps に制限する構成はどれですか?

A.

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
  interface GigabitEthernet0/1
     ip address 209.165.200.225 255.255.255.0
     ip access-group EGRESS out
     service-policy input CoPP_SSH
!
   ip access-list extended CoPP_SSH
      deny tcp any any eq 22
!
```

B.

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
   control-plane
      service-policy input CoPP_SSH
!
  ip access-list extended CoPP_SSH
      permit tcp any any eq 22
!
```

C.

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
  interface GigabitEthernet0/1
     ip address 209.165.200.225 255.255.255.0
     ip access-group EGRESS out
     service-policy input CoPP_SSH
!
   ip access-list extended CoPP_SSH
      permit tcp any any eq 22
!
```

D.

```
class-map match-all CoPP_SSH
      match access-group name CoPP_SSH
      !
policy-map CoPP_SSH
      class CoPP_SSH
   police cir 100000
      exceed-action drop
      !
!
!
   control-plane transit
      service-policy input CoPP_SSH
!
  ip access-list extended CoPP_SSH
     permit tcp any any eq 22
!
```

Answer: B (メーッセージを残す)

最新問題: **181**

エンジニアは、パケット間の遅延変動に敏感な新しいアプリケーションの展開に関心があります。ルータをジッタ測定の宛先に設定するコマンドはどれですか?

A. Router(config)# ip sla Responder udp-connect 172.29.139.134 5000
B. Router(config)# ip sla Responder tcp-connect 172.29.139.134 5000
C. Router(config)# ip sla Responder udp-echo 172.29.139.134 5000
D. Router(config)# ip sla Responder tcp-echo 172.29.139.134 5000
Answer: C (メーッセージを残す)
説明
Cisco IOS IP SLA Responder は、Cisco IOS IP SLA 要求パケットに応答する機能を持つ Cisco IOS ソフトウェア コンポーネントです。IP SLA ソースは、応答側への接続を確立する操作が開始される前に、制御パケットを送信します。制御パケットが確認応答されると、テスト パケットが応答側に送信されます。
レスポンダは、パケットを受信したときにタイムスタンプを挿入し、宛先の処理時間を計算して、送信されたパケットにタイムスタンプを追加します。この機能により、一方向のパケット損失、遅延、およびジッターの測定値を、ping やその他の専用プローブ テストでは不可能な精度で計算できます。

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: 182
展示を参照してください。

これら 2 つの直接接続されたネイバー間に EBGP ネイバーシップを確立し、BGP を介して 2 つのルーターのループバック 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
```

Answer: (解答を表示する**)**

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 のネットワーク 10.1.1.0/24 と R2 のネットワーク 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れると、または 「network x.0.0.0 mask 255.0.0.0」または 「network xxxx mask 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。しかし、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する場合に何が必要かを見てみましょう。2 つのコマンドが必要です。

+ R1 のコマンド 「neighbor 10.1.1.1 ebgp-multihop 2」と 「neighbor 10.2.2.2 ebgpmultihop

このコマンドは、TTL 値を 2 に増やして、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。

+ Answer '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 (構成) #router bgp 2

R2 (config-router) #neighbor 192.168.10.1 remote-as 1

R2 (config-router) #network 10.2.2.0 マスク 255.255.255.0

クイック ワイヤレス サマリー

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。

+ 自律的: 自給自足でスタンドアロン。小規模なワイヤレス ネットワークに使用されます。

+ Lightweight: Cisco Lightweight AP (LAP) が機能するには、ワイヤレス LAN コントローラ (WLC) に参加する必要があります。

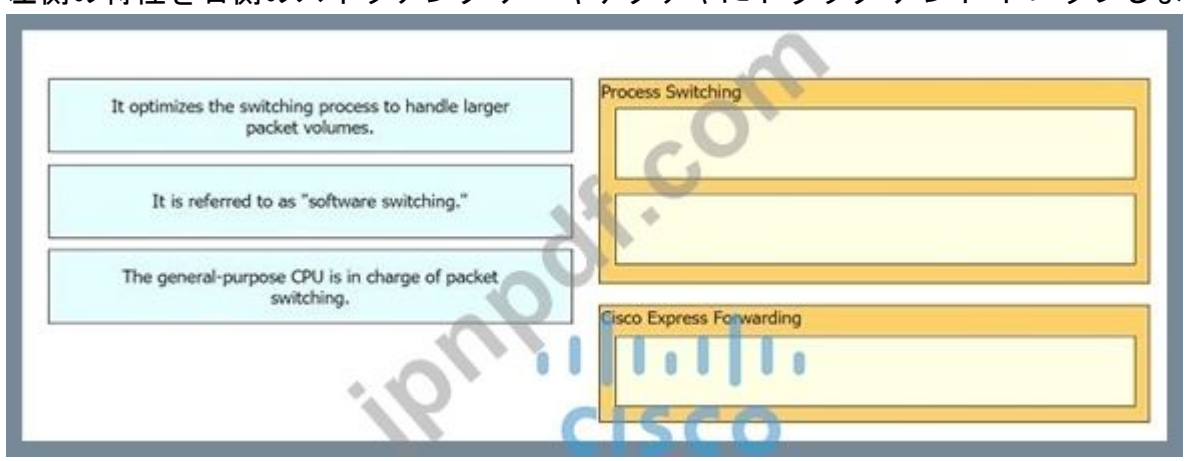
LAP と WLC は、CAPWAP トンネルの論理ペアを介して相互に通信します。
- Control and Provisioning for Wireless Access Point (CAPWAP) は、AP と WLC 間のセットアップ、認証、および操作のための制御メッセージングの IETF 標準です。CAPWAP は、次の違いを除いて LWAPP に似ています。
+CAPWAP は、認証と暗号化に Datagram Transport Layer Security (DTLS) を使用して、AP とコントローラ間のトラフィックを保護します。LWAPP は AES を使用します。
+ 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。
+ 以前はハイブリッド リモート エッジ AP (H-REAP) と呼ばれていた FlexConnect モード: データ トラフィックをローカルで切り替え、コントローラに戻らないようにします。FlexConnect AP は、WLC 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に切り替えることができます (Local Switched)。FlexConnect AP は、ユーザーのワイヤレス データと制御トラフィックの両方を (CAPWAP 経由で) 中央の WLC (Central Switched) にトンネリングすることもできます。
+ 監視モード: クライアントとインフラストラクチャ間のデータ トラフィックを処理しません。ロケーションベース サービス (LBS)、不正 AP 検出、および IDS のセンサーのように機能します。
+ Rogue Detector モード: 不正 AP を監視します。データをまったく処理しません。
+ スニファ モード: スニファとして実行し、特定のチャネル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厳密に使用されます。
+ ブリッジ モード: WLAN と有線インフラストラクチャを一緒にブリッジします。
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、専用の WLC に投資したくない小規模から中規模の、またはマルチサイト 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 個の AP をサポートできます

最新問題**: 183**
展示を参照してください。
パブリック IP ネットワークのルーターが使用する LISP コンポーネントはどれですか
2 つのネットワーク間でトラフィックを転送しますか?
A. RLOC
B. マップ リゾルバ
C. EID
D. マップ サーバー
Answer: A (メーッセージを残す**)**
説明
Locator ID Separation Protocol (LISP) は、1 つの IP アドレスではなく 2 つの名前空間の使用を実装するネットワーク アーキテクチャおよびプロトコルです。
+ エンドポイント識別子 (EID) - エンド ホストに割り当てられます。
+ ルーティング ロケーター (RLOC) - グローバル ルーティング システムを構成するデバイス (主にルーター) に割り当てられます。

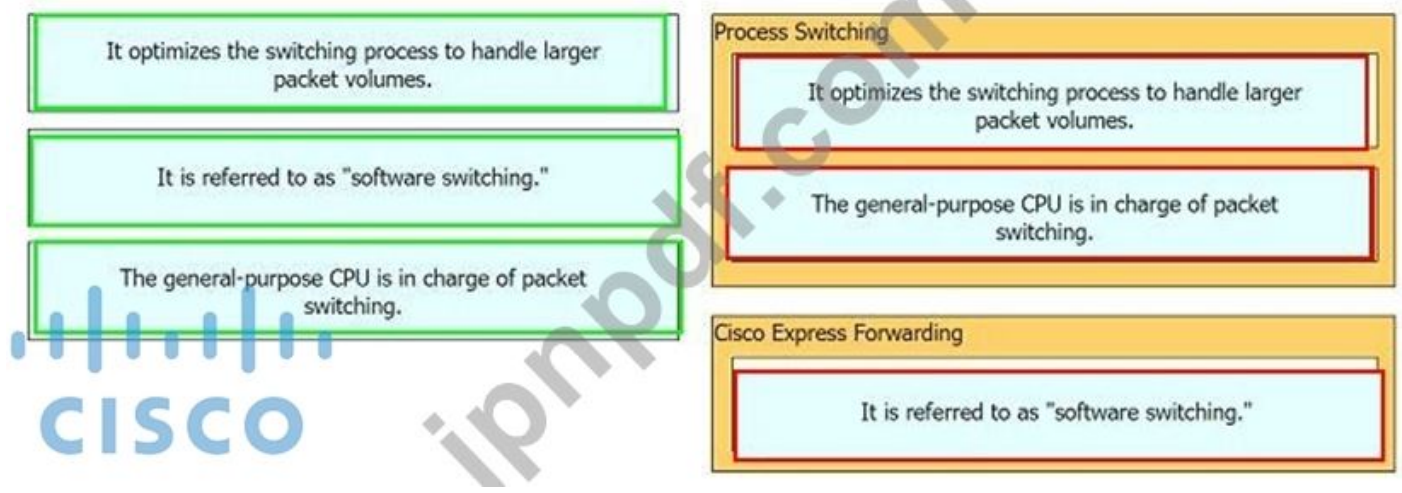
最新問題: **184**
Cisco SD-Access 展開でファブリック ワイヤレス LAN コントローラが実行する機能はどれですか?
A. ファブリック対応 AP を管理し、クライアント登録とローミング情報をコントロール プレーン ノードに転送します。
B. ファブリック内の自律的な非ファブリック アクセス ポイントの構成を調整します。
C. 有線クライアントとワイヤレス クライアントの両方に対して保証エンジンの役割を実行します。
D. ファブリック内のファブリック対応および非ファブリック対応 AP のオンボード クライアント専用です。
Answer: (解答を表示する**)**
ファブリック対応 WLC:
ファブリック対応の WLC は、LISP コントロール プレーンと統合されています。この WLC は、AP イメージ /Config、無線リソース管理、クライアント セッション管理とローミング、およびその他すべてのワイヤレス コントロール プレーン機能を担当します。
WLC ファブリック統合の場合:
ワイヤレス クライアントの MAC アドレスが EID として使用されます
SGT や仮想ネットワーク情報などの他の情報とともに、ワイヤレス MAC アドレスについて通知します VN 情報は FE 上の VLAN にマッピングされます WLC は、ローミング情報を使用してホスト データベース トラッキング DB を更新する役割を担います

最新問題: **185**
展示を参照してください。AS 1000 と AS 2000 間の完全な到達可能性を可能にするために必要な 2 つのコマンドはどれですか? (2つ選んでください)
A. R2#ネットワーク 209.165.201.0 マスク 255.255.192.0
B. R1#ネットワーク 19.168.0.0 マスク 255.255.0.0
C. R2#ネットワークなし 10.0.0.0 255.255.255.0
D. R2#ネットワーク 19.168.0.0 マスク 255.255.0.0
E. R1#ネットワークなし 10.0.0.0 255.255.255.0
Answer: C,D (メーッセージを残す**)**

最新問題: **186**
左側の特性を右側のスイッチング アーキテクチャにドラッグ アンド ドロップします。

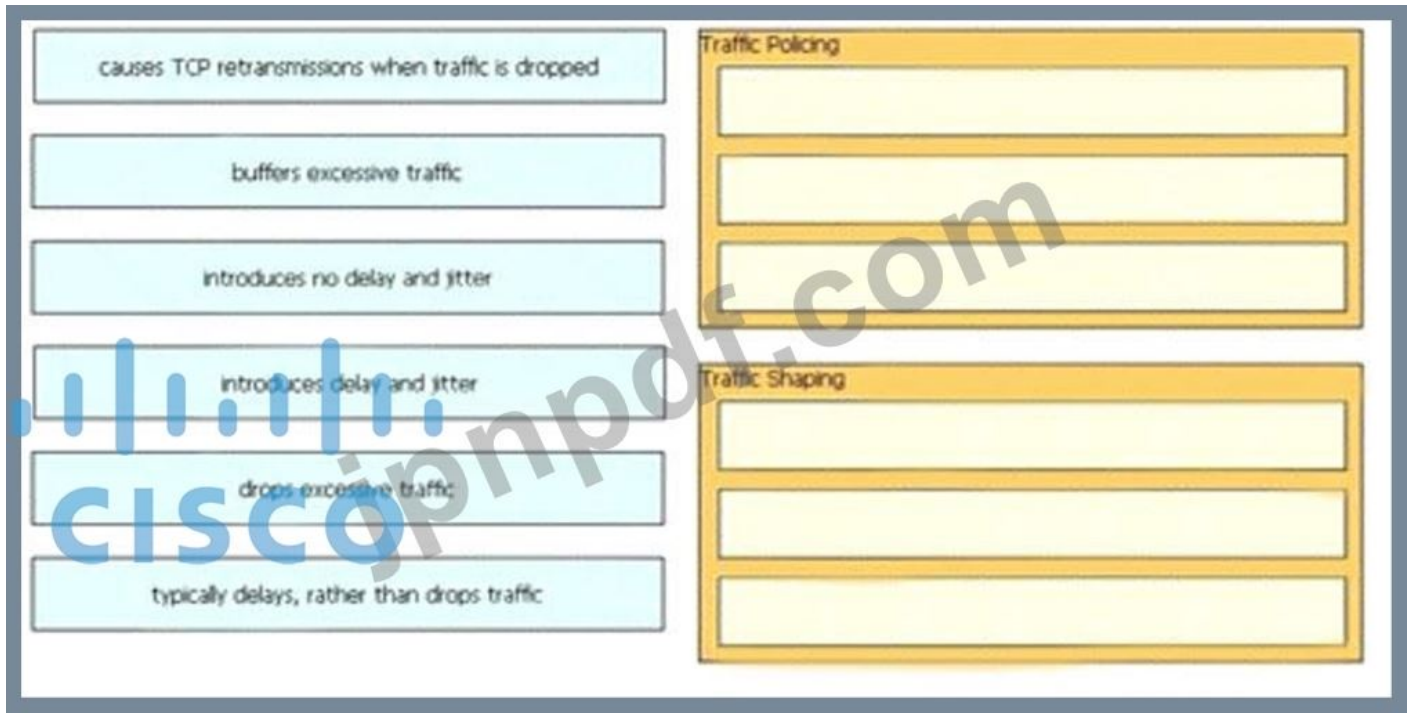


Answer:



最新問題: 187

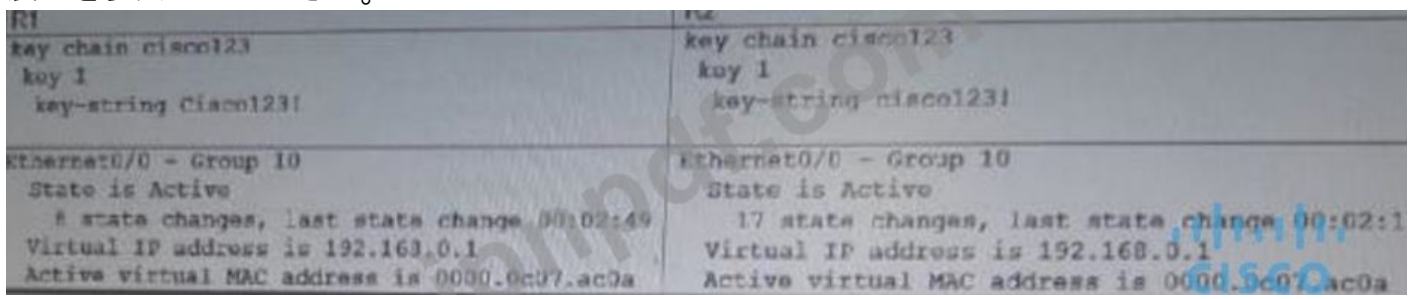
左側の説明を右側の QoS コンポーネントにドラッグ アンド ドロップします。



Answer:

最新問題: 188

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ようにするプロトコルはどれですか?

A. HSRPv1
B. GLBP
C. VRRP
D. HSRPv2
Answer: A (メーッセージを残す)
説明
仮想 MAC アドレスは 0000.0c07.acXX (XX は 16 進数のグループ番号) であるため、HSRPv1 を使用しています。
注: HSRP バージョン 2 は、0000.0C9F.F000 から 0000.0C9F.FFFF の範囲の新しい MAC アドレスを使用します。

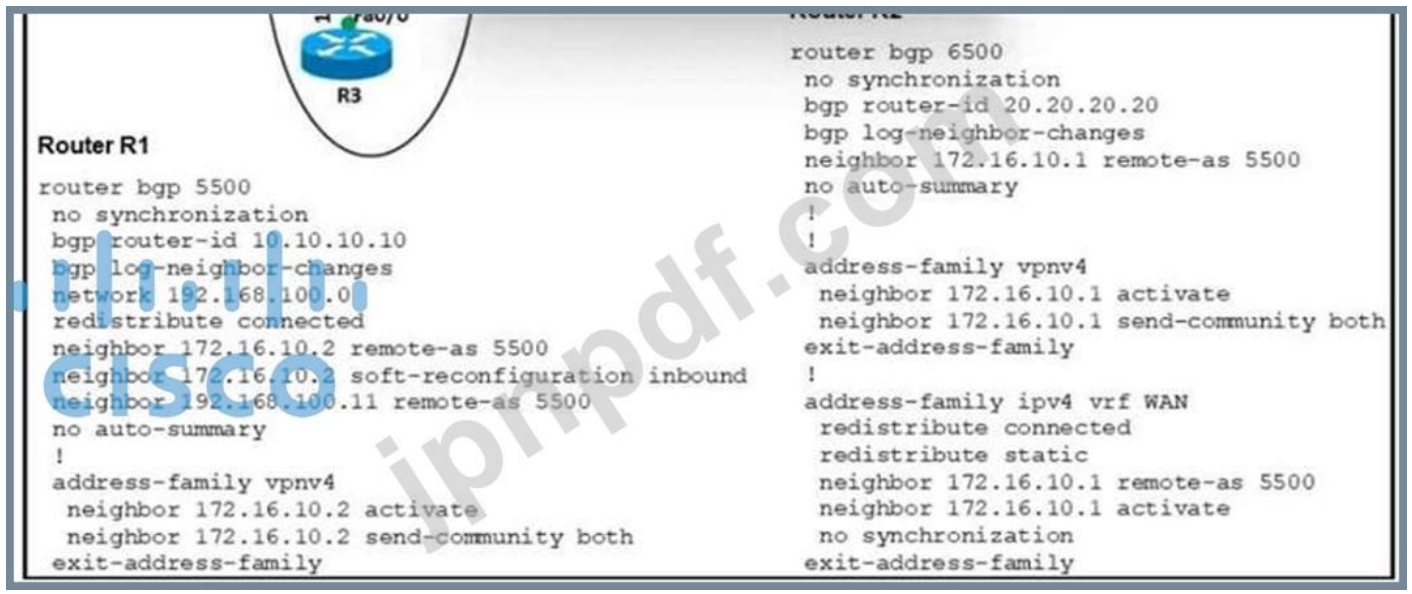
最新問題: **189**
Cisco IOS ベースのルータで 4 つのスタティック キューを使用する輻輳キューイング方式はどれですか?
A. カスタム
B. 加重フェア
C. 低遅延
D. 優先
Answer: D (メーッセージを残す)

最新問題: **190**
展示を参照してください。

```
access-list 1 permit 172.16.1.0 0.0.0.255
ip nat inside source list 1 interface gigabitethernet0/0 overload
```

このデバイスの NAT 構成の内部インターフェイスと外部インターフェイスは正しく識別されています。この構成の効果は何ですか?
A. ダイナミック NAT
B. 静的 NAT
C. NAT64
D. パット
Answer: D (メーッセージを残す)

最新問題: **191**
展示を参照してください。



エンジニアは R1 と R2 の間の BGP 隣接関係を構成しますが、確立に失敗します。どのアクションで問題を解決しますか?

A. R1 のネットワーク ステートメントを 172.16 10.0 に変更します。

B. R1 の remote-as 番号を 6500 に変更します。

C. 192 168.100.11 の remote-as 番号を変更します。

D. R1 と R2 で同期を有効にします。

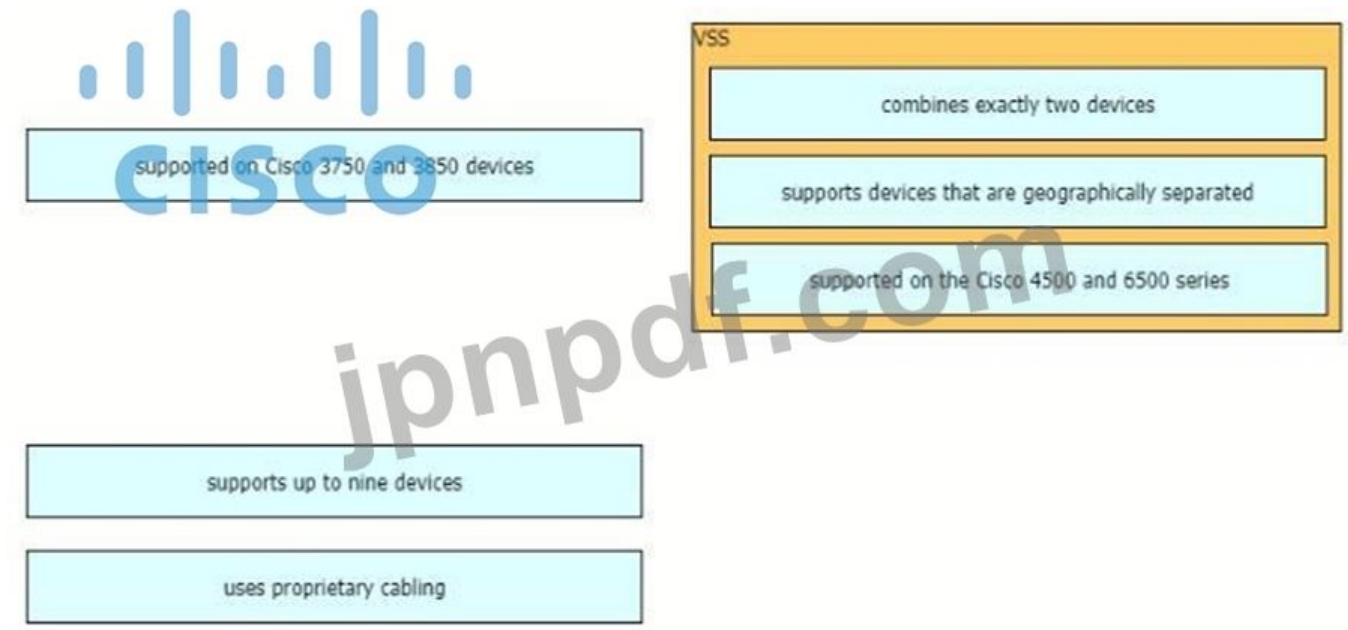
Answer: B (メーッセージを残す)

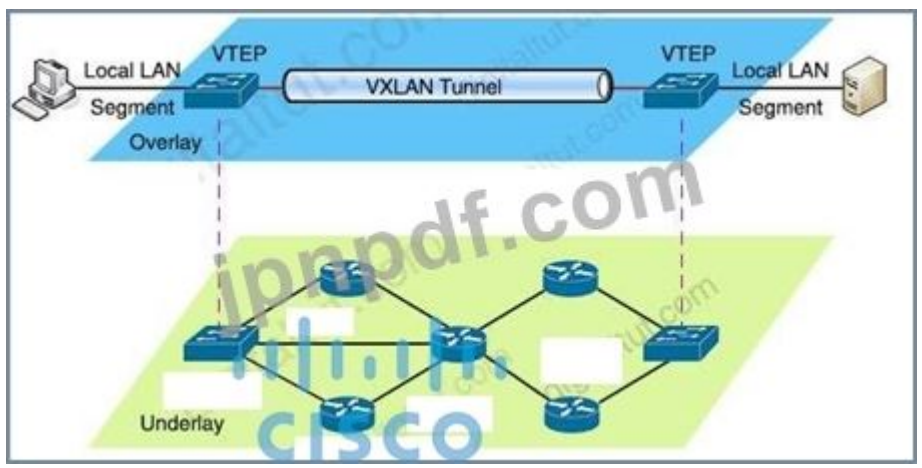
最新問題: **192**

VSS テクノロジ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。

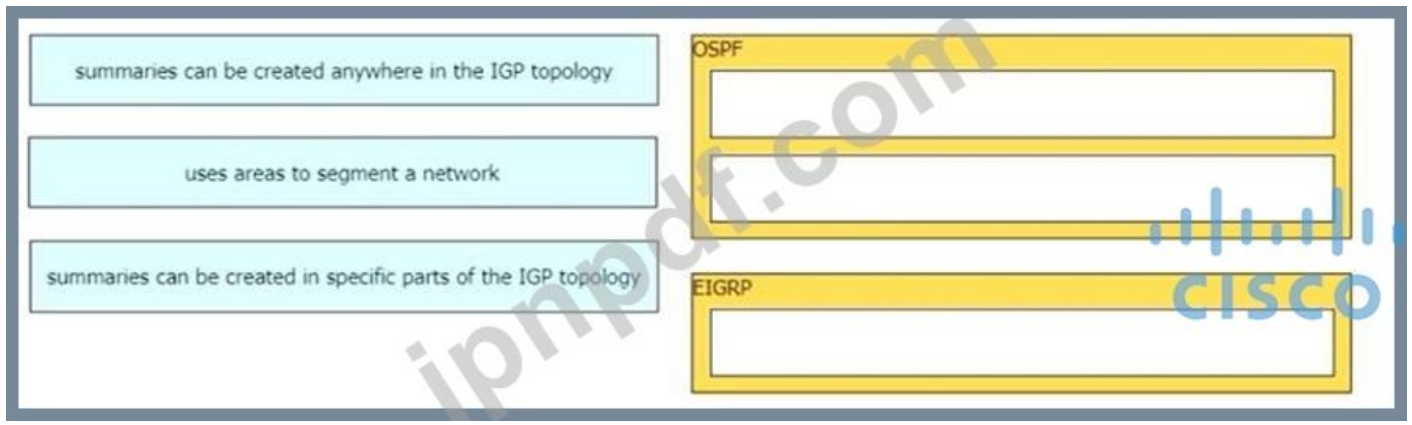
Answer:

説明

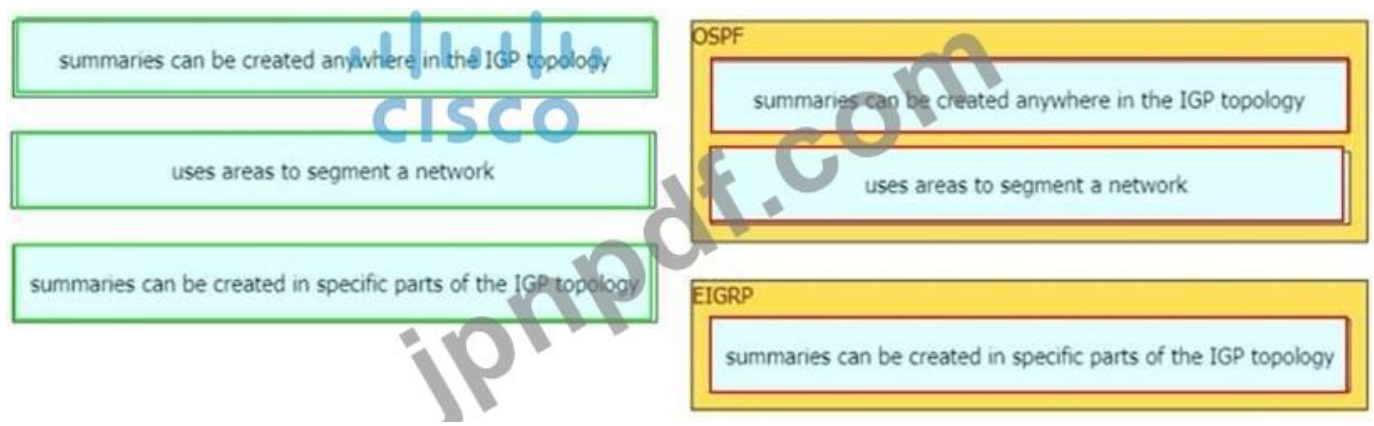


最新問題: **193**
VXLAN の VTEP の機能はどれですか?
A. IPv6 から IPv4 VXLAN へのトンネリング トラフィック
B. ローカル VXLAN イーサネット セグメントで暗号化通信を許可する
C. VXLAN イーサネット フレームのカプセル化とカプセル化解除
D. IPv4 から IPv6 VXLAN へのトンネリング トラフィック
Answer: C (メーッセージを残す)
VTEP はオーバーレイ ネットワークとアンダーレイ ネットワークの間を接続し、
フレームを VXLAN パケットにカプセル化し、IP ネットワーク (アンダーレイ) 経由で送信する
パケットが VXLAN トンネルを離れるときにカプセル化を解除します。
VTEP はオーバーレイ ネットワークとアンダーレイ ネットワークの間を接続し、
フレームを VXLAN パケットにカプセル化し、IP ネットワーク (アンダーレイ) 経由で送信する
パケットが VXLAN トンネルを離れるときにカプセル化を解除します。


最新問題: **194**
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。

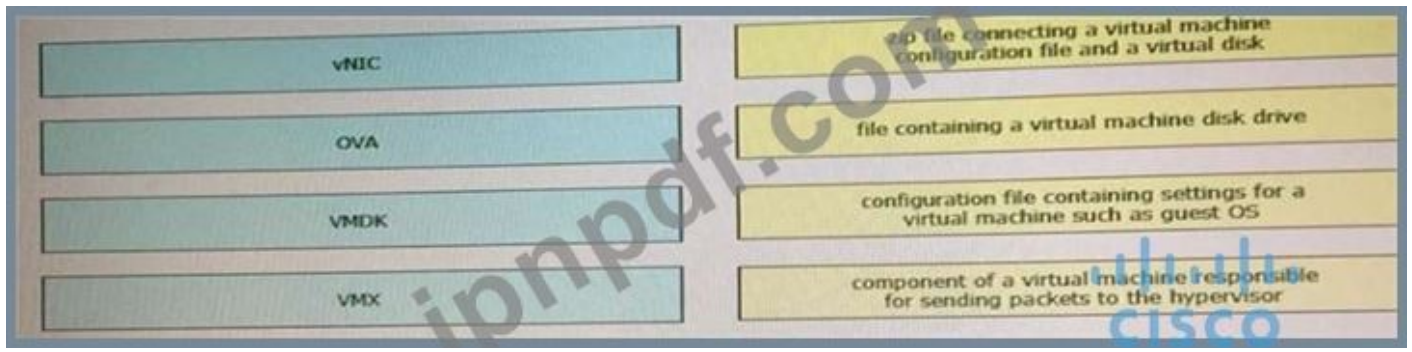


Answer:

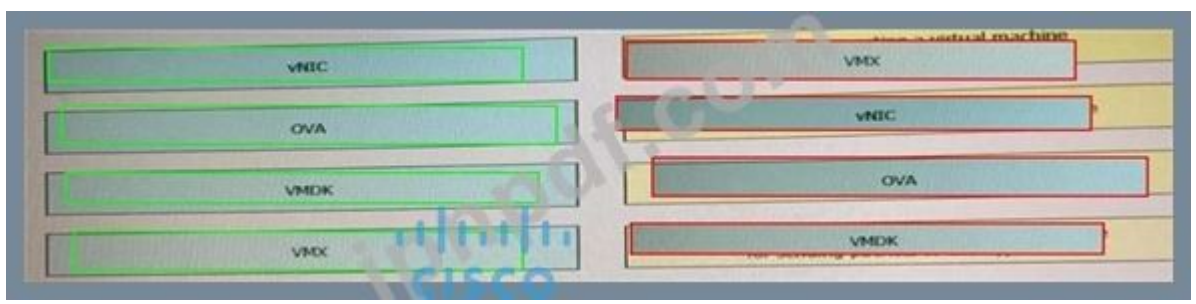


最新問題: **195**

仮想コンポーネントを左側から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: **196**

アップリンクの使用率を最大化し、必要な設定量を最小化するファースト ホップ冗長プロトコルはどれですか?

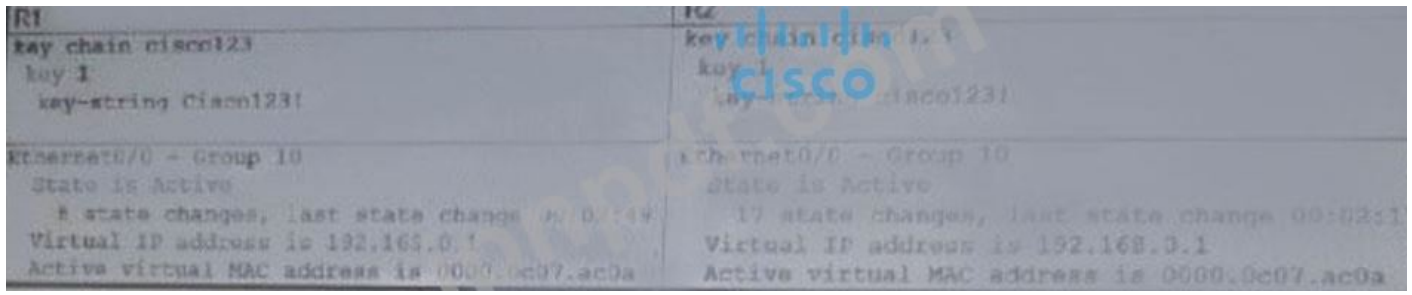
A. GLBP

B. HSRP v2

C. VRRP
D. HSRP v1
Answer: A (メーッセージを残す**)**
HSRP と VRRP の主な欠点は、1 つのゲートウェイのみがアクティブ ゲートウェイとして選択され、トラフィックの転送に使用され、残りのゲートウェイはアクティブ ゲートウェイに障害が発生するまで使用されないことです。ゲートウェイ ロード バランシング プロトコル (GLBP) はシスコ独自のプロトコルであり、HSRP および VRRP と同様の機能を実行しますが、GLBP グループ内のメンバー間のロード バランシングをサポートします。

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **197**
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ようにするプロトコルはどれですか?
A. VRRP
B. HSRPv1
C. HSRPv2
D. GLBP
Answer: (解答を表示する)

最新問題: **198**
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利点は何ですか? (2つ選んでください。)
A. ラック スペース、電力、および冷却要件の削減
B. 迅速な展開
C. セキュリティ強化
D. IP および MAC アドレス要件の軽減
E. より小さいレイヤー 2 ドメイン
Answer: B,C (メーッセージを残す**)**

最新問題: **199**
ログ ファイルの日付の横に * が含まれるのはなぜですか?

A. ログ メッセージが記録されたときにネットワーク デバイスが NTP 時刻を受信していた
B. ログ メッセージが記録されたときに、ネットワーク デバイスが NTP サーバーに到達できませんでした。
C. ネットワーク デバイスが NTP を使用するように構成されていません
D. ネットワーク デバイスは、ログに NTP タイム スタンプを使用するように構成されていません。
Answer: (解答を表示する**)**
説明
システム クロックが設定されていない場合、日付と時刻の前にアスタリスク (*) が表示され、日付と時刻が正しくない可能性があることが示されます。
参照：
https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/service_timestamp

最新問題**: 200**
エンジニアは、Cisco ワイヤレス LAN コントローラでローカル WebAuth を設定しています。RFC 5737 によると、この構成ではどの仮想 IP アドレスを使用する必要がありますか?
A. 172.20.10.1
B. 192.0.2.1
C. 1.1.1.1
D. 192.168.0.1
Answer: B (メーッセージを残す**)**

最新問題**: 201**
2 つのスーパーバイザ モジュールを搭載した Cisco Catalyst スイッチでは、管理者はシャーシからアクティブ スーパーバイザを一時的に取り外して、ハードウェア メンテナンスを実行する必要があります。アクティブなスーパーバイザの削除がネットワーク運用に影響を与えないことを保証するメカニズムはどれですか?
A. NSF/NSR
B. SSO
C. HSRP
D. VRRP
Answer: B (メーッセージを残す**)**
説明
ステートフル スイッチオーバー （SSO）は、ネットワーク設計の単一障害点であり、停止によって顧客へのサービスが失われる可能性があるデュアル ルート プロセッサ （RP）を備えたネットワーク エッジ デバイスを保護します。
参照：
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/statef

最新問題**: 202**
左側の特性を、右側に記述されている QoS コンポーネントにドラッグ アンド ドロップします。

Answer:

説明

マーキング = ダウンストリーム デバイスに情報を伝達するためにトラフィックに適用されます。分類 = トラフィック タイプを区別します。信頼 = DSCP/COS 値を保持しながらデバイスを通過するトラフィックを許可します。

最新問題: **203**

仮想マシンを実行するには何が必要ですか?

A. ハイパーバイザーと物理サーバー ハードウェア

B. タイプ 1 ハイパーバイザーのみ

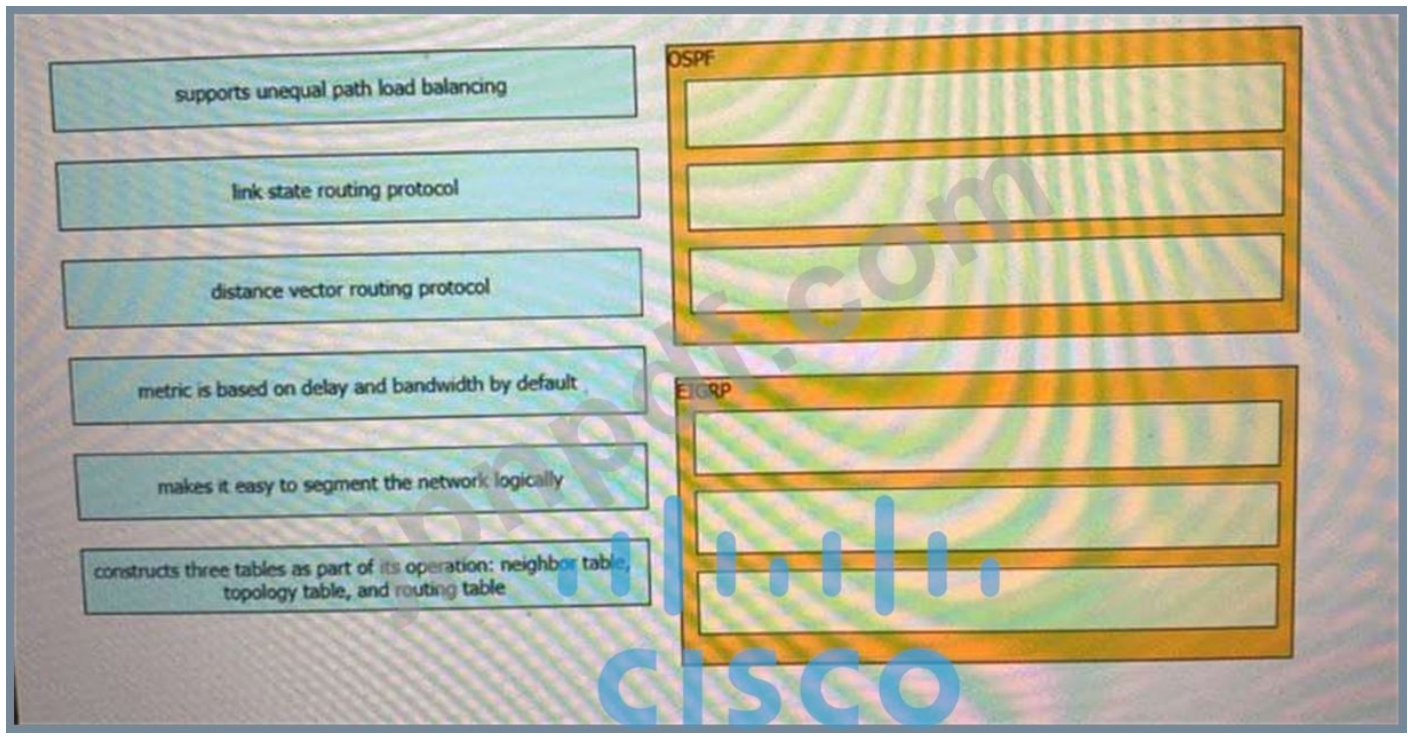
C. タイプ 2 ハイパーバイザーのみ

D. タイプ 1 ハイパーバイザーとホスト オペレーティング システム

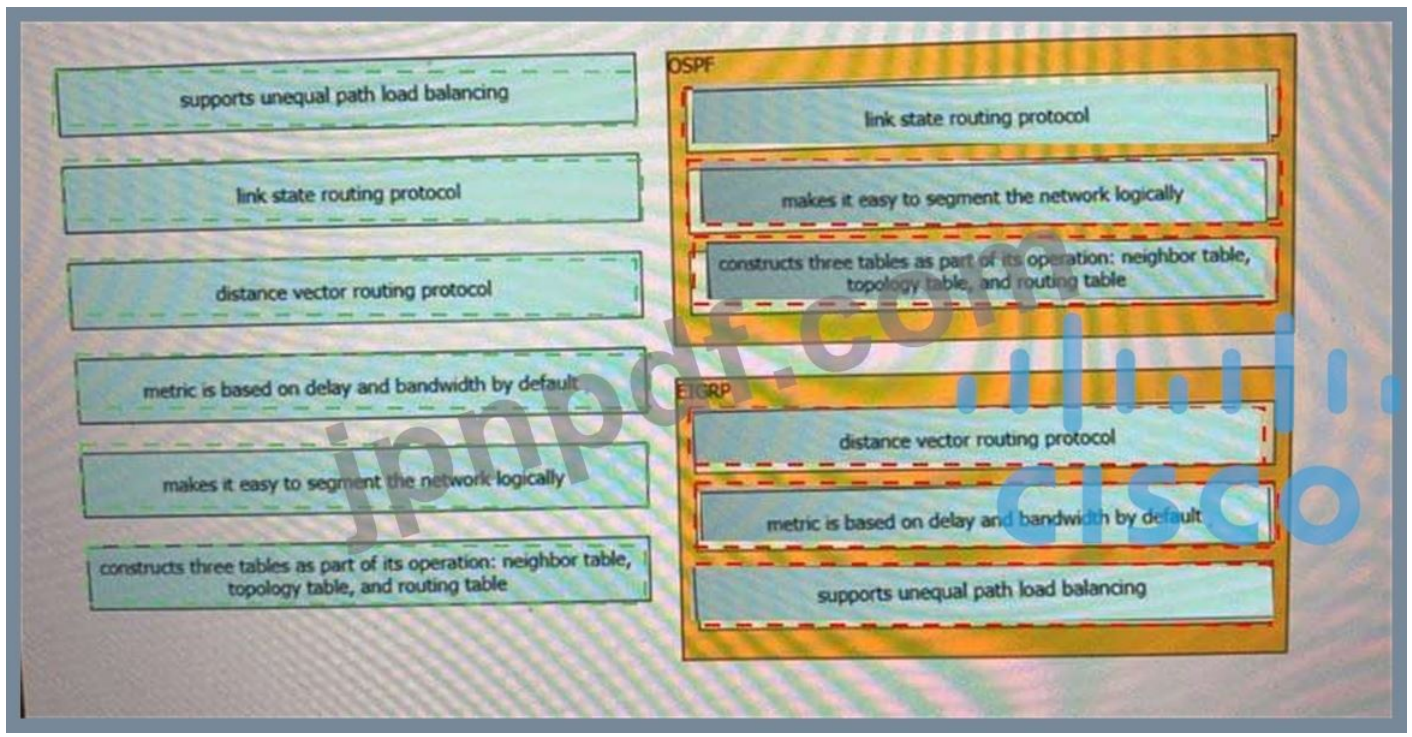
Answer: A (メーッセージを残す**)**

最新問題: **204**

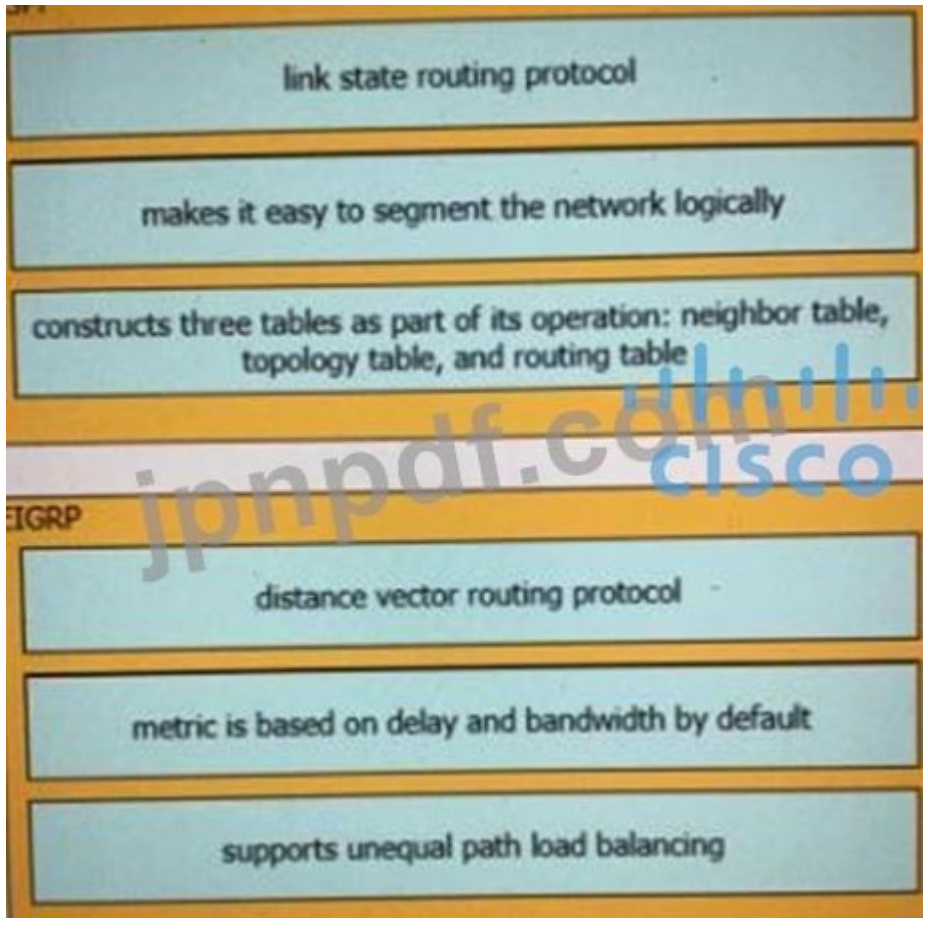
左側の説明を右側のルーティング プロトコルにドラッグ アンド ドロップします。


supports unequal path load balancing
link state routing protocol
distance vector routing protocol
metric is based on delay and bandwidth by default
makes it easy to segment the network logically
constructs three tables as part of its operation: neighbor table, topology table, and routing table
OSPF
EIGRP

Answer:


supports unequal path load balancing
link state routing protocol
distance vector routing protocol
metric is based on delay and bandwidth by default
makes it easy to segment the network logically
constructs three tables as part of its operation: neighbor table, topology table, and routing table
OSPF
link state routing protocol
makes it easy to segment the network logically
constructs three tables as part of its operation: neighbor table, topology table, and routing table
EIGRP
distance vector routing protocol
metric is based on delay and bandwidth by default
supports unequal path load balancing

説明



最新問題: **205**

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説明はどれですか?

A. 出力には、ルーター R1 がインターフェイス 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、ルーター R1 がすべてのインターフェー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、ルーター R1 が送信した OSPF hello メッセージがインターフェイス Fa0/1 で受信されたことが表示されます。

D. 出力には、ルーター R1 が送受信した OSPF の hello および LSACK メッセージが表示されます。

Answer: C (メーッセージを残す)

説明

このコマンドの組み合わせは 条件付きデバッグ」と呼ばれ、条件に基づいてデバッグ出力をフィルタリングします。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: **206**

有効な JSON ファイルを表示する展示はどれですか?

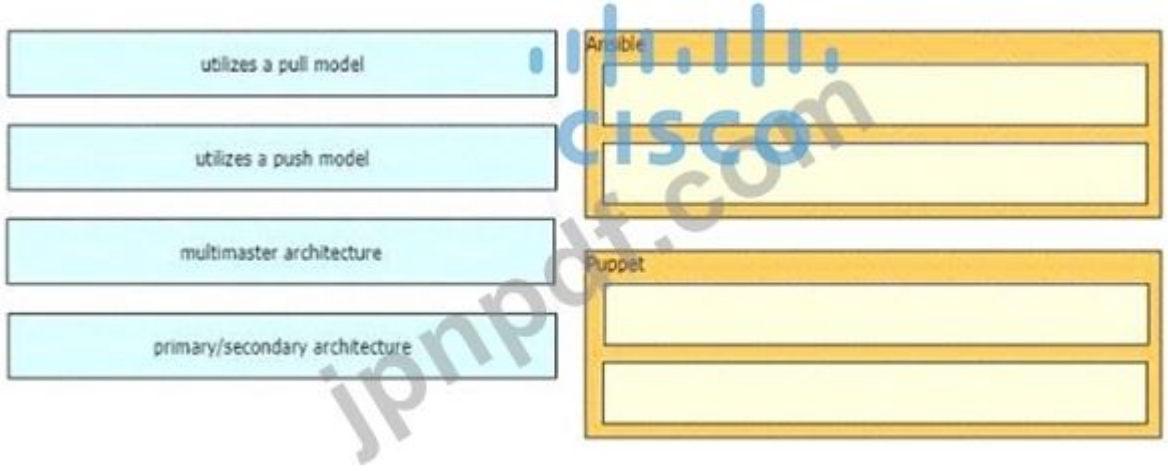
A. オプション D
B. オプション B
C. オプション C
D. オプション A
Answer: A (メーッセージを残す**)**

最新問題**: 207**
LISP マップ リゾルバーの機能は何ですか?
A. ルーティング不可能な EID をパケット ソースとして受け入れないサービス プロバイダーに接続されている場合に、LISP 以外のサイトにトラフィックを送信します。
B. サイトをコア ネットワークの LISP 対応部分に接続するには、サイトの EID から RLOC へのマッピングを公開し、マップ要求メッセージに応答します。
C. ITR からのマップ要求メッセージをカプセル化解除し、メッセージを MS に転送します。
D. ルーティング可能な非 LISP トラフィックを、あるアドレス ファミリから別のアドレス ファミリの LISP サイトにアドバタイズします。
Answer: (解答を表示する**)**
説明
マップ リゾルバ (MR): MR は次の機能を実行します。ITR によってカプセル化された MAP 要求を受信します。ALT ルーターにサービス インターフェイスを提供し、MAP 要求のカプセル化を解除し、ALT トポロジで転送します。

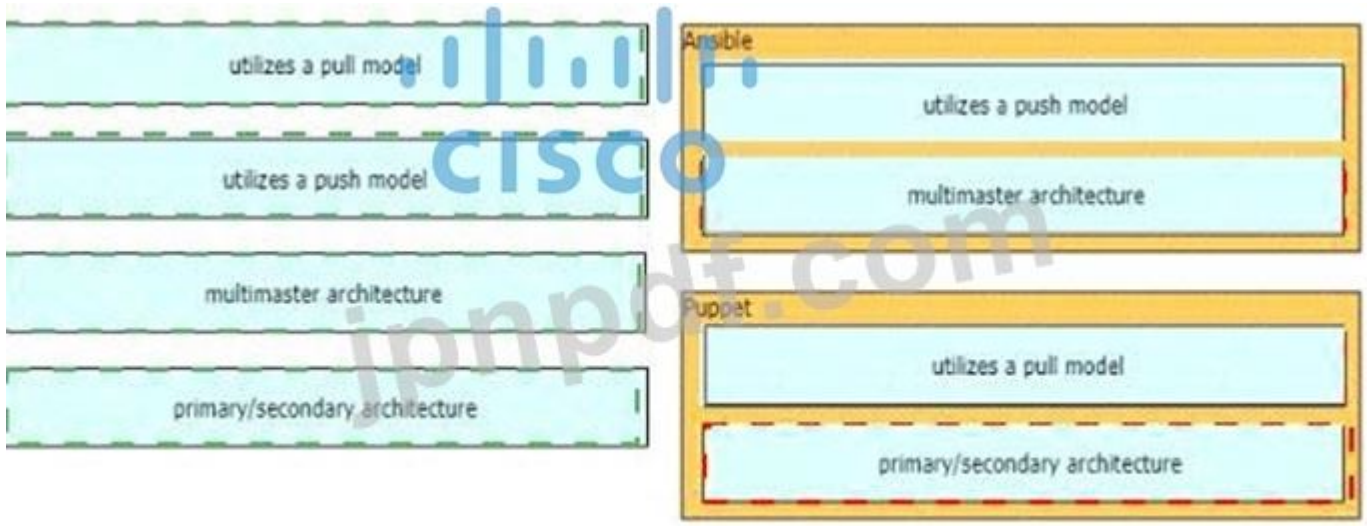
最新問題: **208**
展示を参照してください。

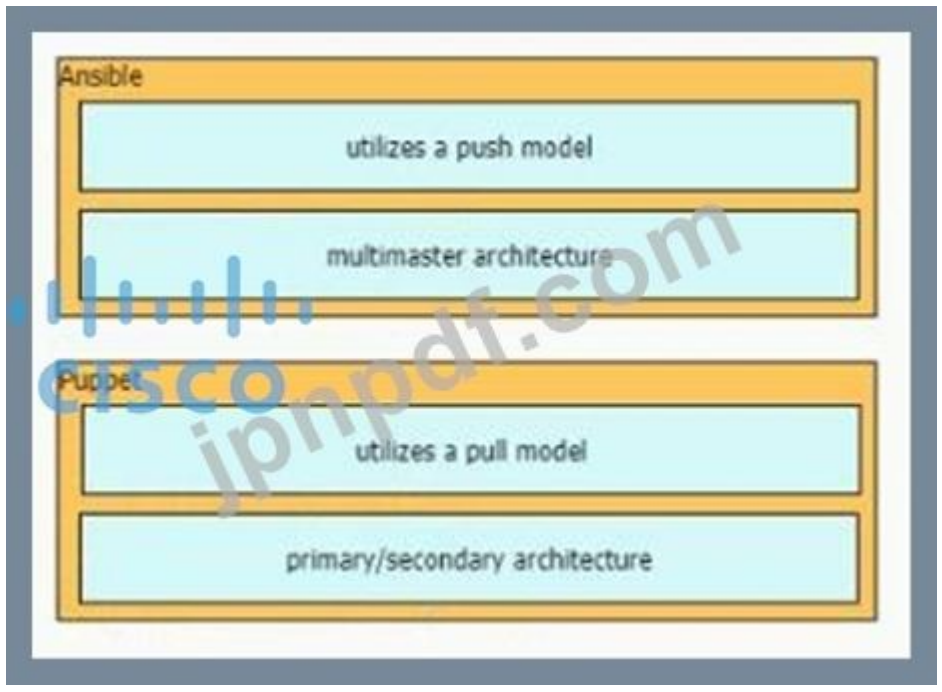
R2 のインターフェイス Fa0/0 に適用される IPv6 OSPF ネットワーク タイプはどれですか
デフォルトで？
A. マルチポイント
B. ブロードキャスト
C. イーサネット
D. ポイントツーポイント
Answer: B (メーッセージを残す**)**
ブロードキャスト ネットワーク タイプは、OSPF が有効なイーサネット インターフェイスのデフォルトです (ポイントツー
Point は、HDLC および PPP カプセル化を使用するシリアル インターフェイスのデフォルトの OSPF ネットワーク タイプです。

最新問題: **209**
特性を左側から、右側に記述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。



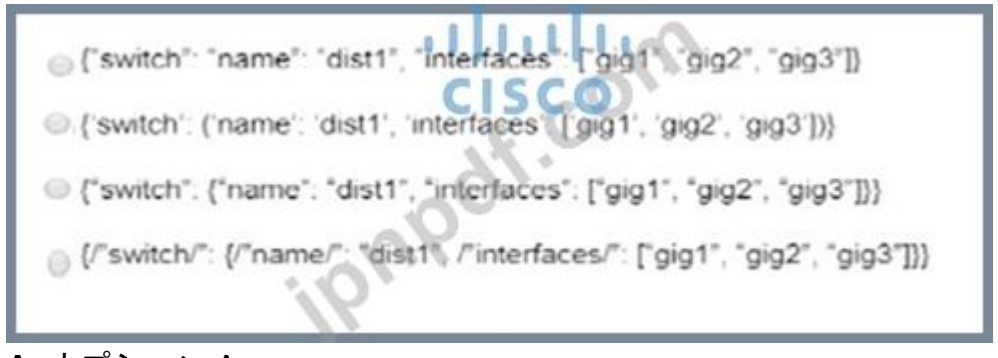
Answer:





最新問題**: 210**

有効な JSON 構文はどれですか?



A. オプション A

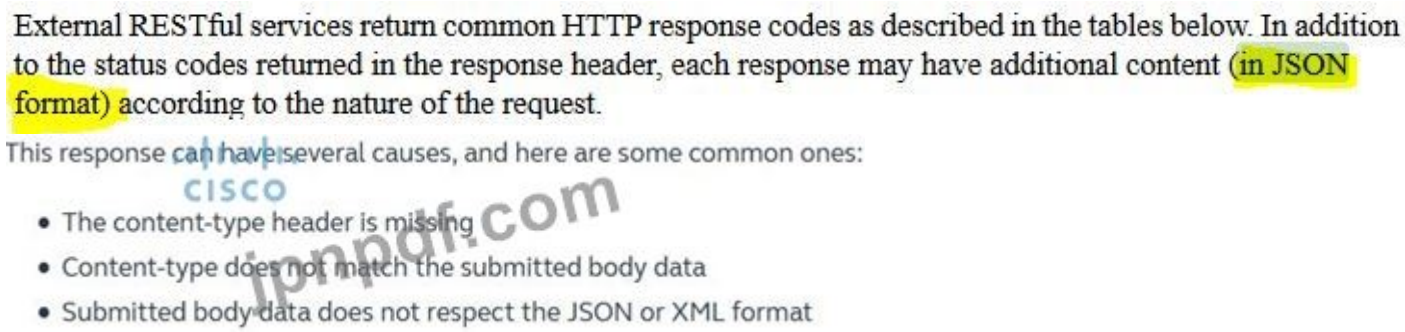
B. オプション B

C. オプション C

D. オプション D

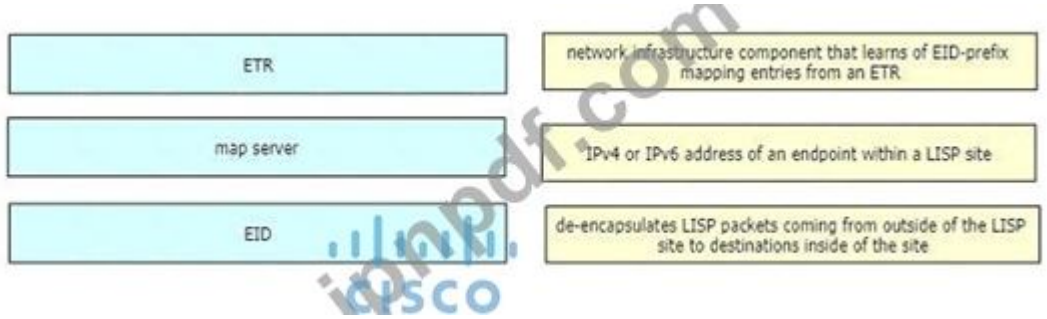
Answer: C (メーッセージを残す)
参照：
この JSON は次のように記述できます。
{
'スイッチ': {
'名前': 'dist1',
「インターフェイス」: [「gig1」、「gig2」、「gig3」]
}
}

最新問題**: 211**
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。要求を送信した後、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ますか?
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)

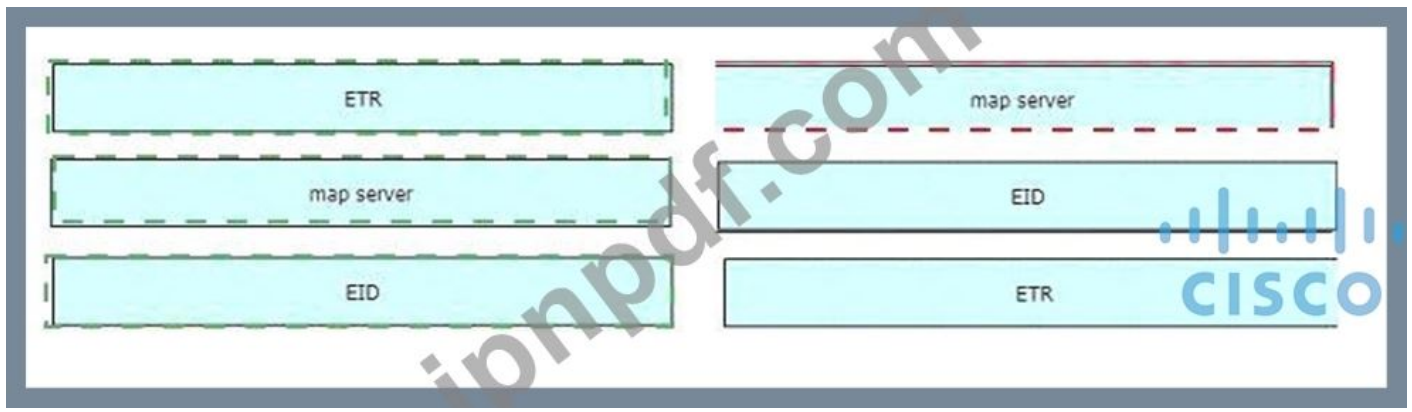

External RESTful services return common HTTP response codes as described in the tables below. In addition to the status codes returned in the response header, each response may have additional content (in JSON format) according to the nature of the request.
This response can have several causes, and here are some common ones:
- The content-type header is missing
- Content-type does not match the submitted body data
- Submitted body data does not respect the JSON or XML format

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 212**
左側の LISP コンポーネント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

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irloverview.h

最新問題**: 213**

正しくないパスワードが REST API セッションに適用された要求に対する正しい応答は、どの HHTP 状態コードですか?

A. HTTP ステータス コード 200

B. HTTP ステータス コード 302

C. HTTP ステータス コード 401

D. HTTP ステータス コード: 504

Answer: C (メーッセージを残す**)**

説明

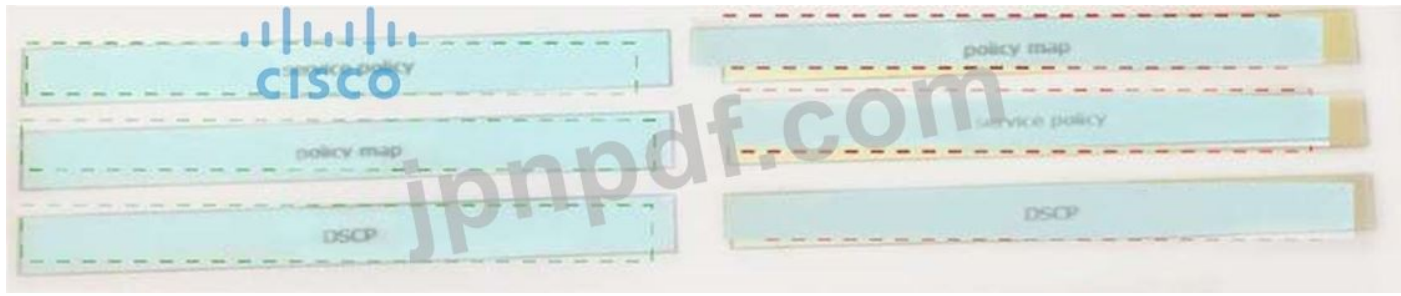
401 エラー応答は、クライアントが適切な承認を提供せずに保護されたリソースを操作しようとしたことを示します。間違った資格情報を提供したか、まったく提供しなかった可能性があります。

注: HTTP ステータス コード 200」に回答してください。4xx コードは クライアント エラー」を示し、5xx コードは サーバー エラー」を示します。

最新問題**: 214**

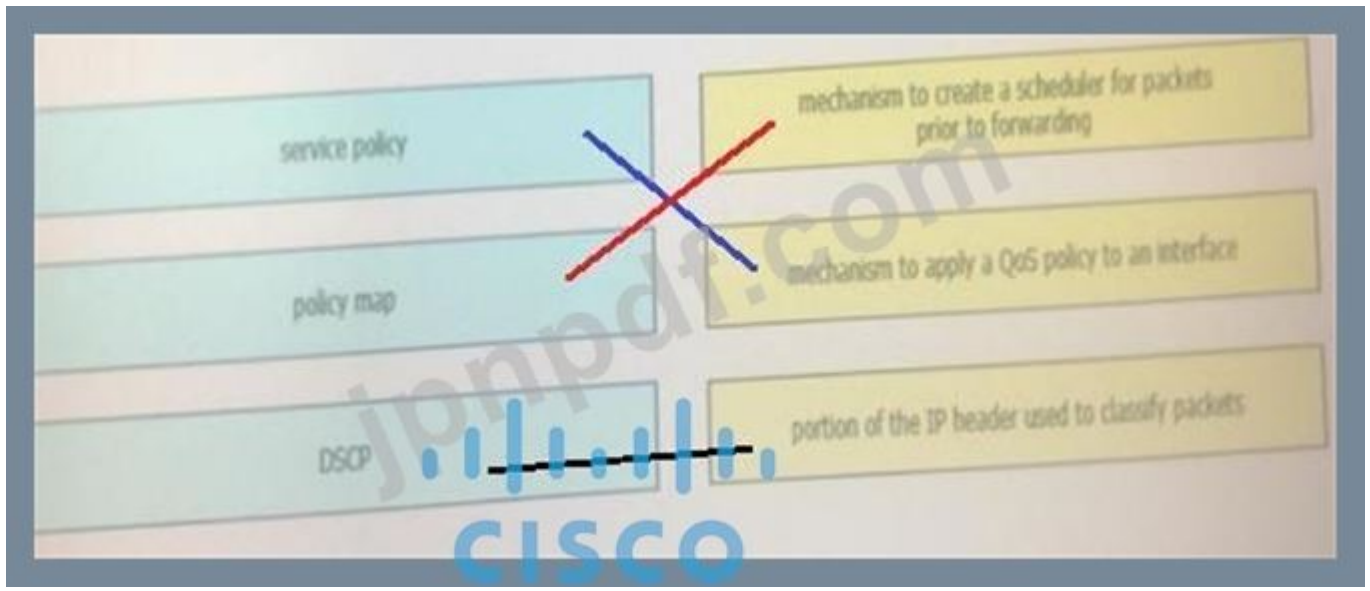
Qos メカニズムを左から右の正しい説明にドラッグ アンド ドロップします。

Answer:



説明

図を含む画像 自動生成された説明



最新問題**: 215**

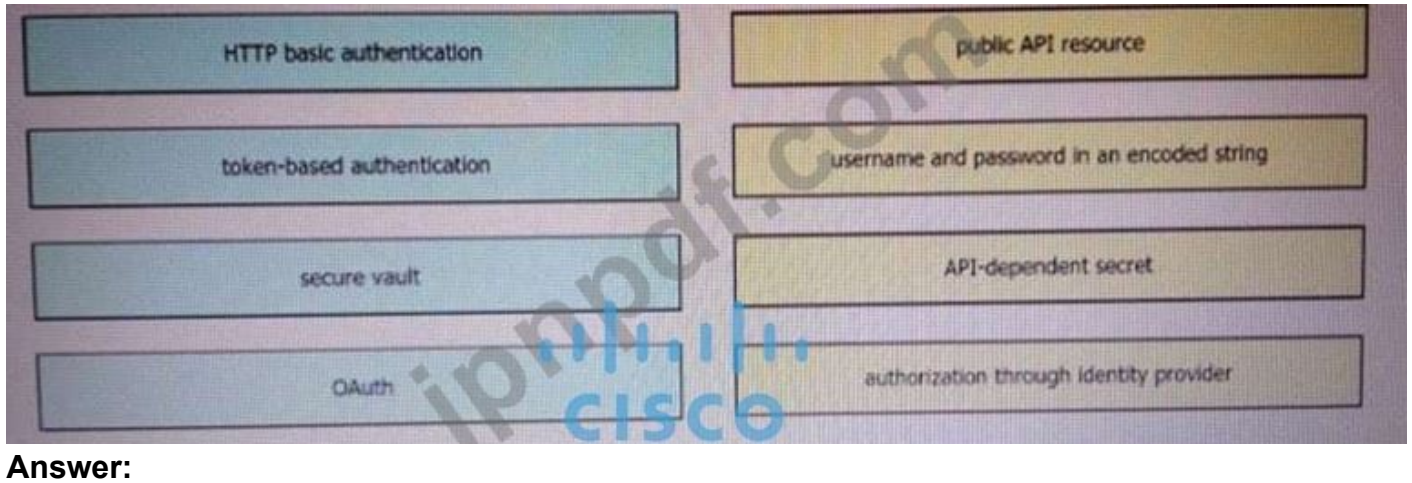
脅威防御ソリューションを左側から右側の説明にドラッグ アンド ドロップします。

Answer:

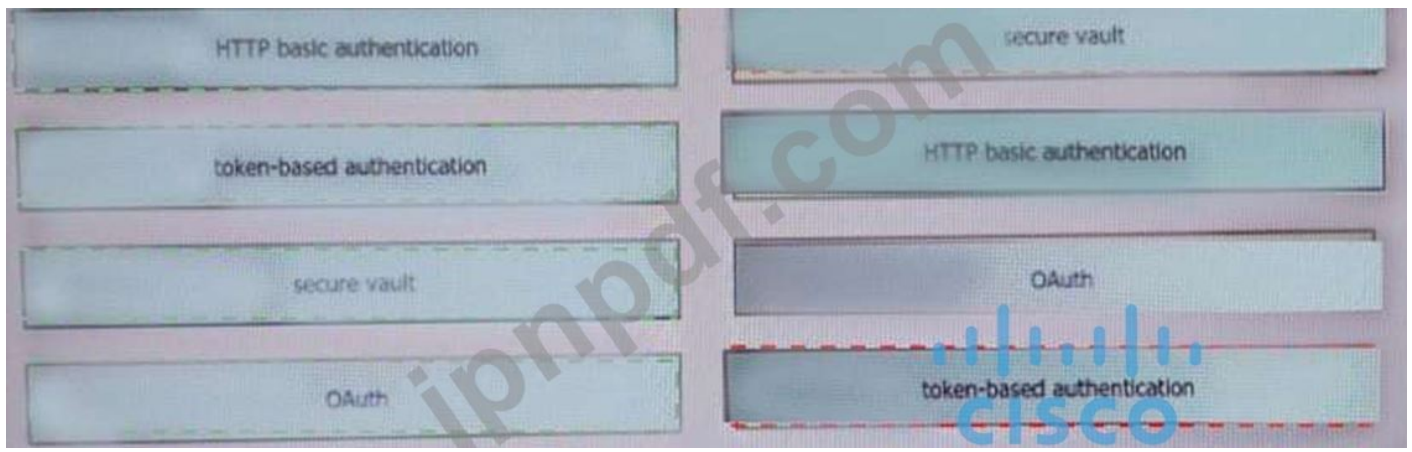
説明

最新問題: **216**

REST API の認証方法を左から右の説明にドラッグ アンド ドロップします。



Answer:



説明

最新問題: **217**

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**)**

About Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations.

最新問題: **218**

アップリンクの使用率を最大化し、必要な設定量を最小化するファースト ホップ冗長プロトコルはどれですか?

A. HSRP v2

B. VRRP

C. GLBP

D. HSRP v1

Answer: C (メーッセージを残す**)**

最新問題: **219**
OSI モデルのレイヤ 2 ですべてのトラフィックに安全な通信チャネルを提供するテクノロジはどれですか?
A. MACsec
B. IPsec
C. SSL
D. Cisco Trustsec
Answer: (解答を表示する**)**
802.1AE で定義された MACsec は、アウトオブバンドを使用して、有線ネットワーク上で MAC 層の暗号化を提供します。
暗号化キーイングの方法。MACsec Key Agreement (MKA) プロトコルは、

最新問題: **220**
私の出品物を参照してください。ログ メッセージの原因は何ですか?
A. OSPFエリア変更
B. MTU の不一致
C. hello パケットの不一致
D. IP アドレスの不一致
Answer: A (メーッセージを残す**)**

最新問題: **221**
エンジニアは、TCP ヘッダーに ACK を含むパケットを許可する ACL を構成する必要があります。ACL に含める必要があるエントリはどれですか?
A. access-list 110 permit tcp any any eq 21 確立
B. access-list 10 permit ip any any eq 21 tcp-ack
C. access-list 10 permit tcp any any eq 21 確立
D. access-list 110 permit tcp any any eq 21 tcp-ack
Answer: A (メーッセージを残す**)**

最新問題: **222**
展示を参照してください :

エンジニアは VRRP を構成し、show コマンドを発行して動作を確認します。エンジニアは出力から VRRP グループ 1 について何を確認しますか?

A. 10.10.1.1/32 がルーティング テーブルにある場合、R1 はマスターです。

B. R2 のルーティング テーブルに 10.10.1.1/32 へのルートがありません

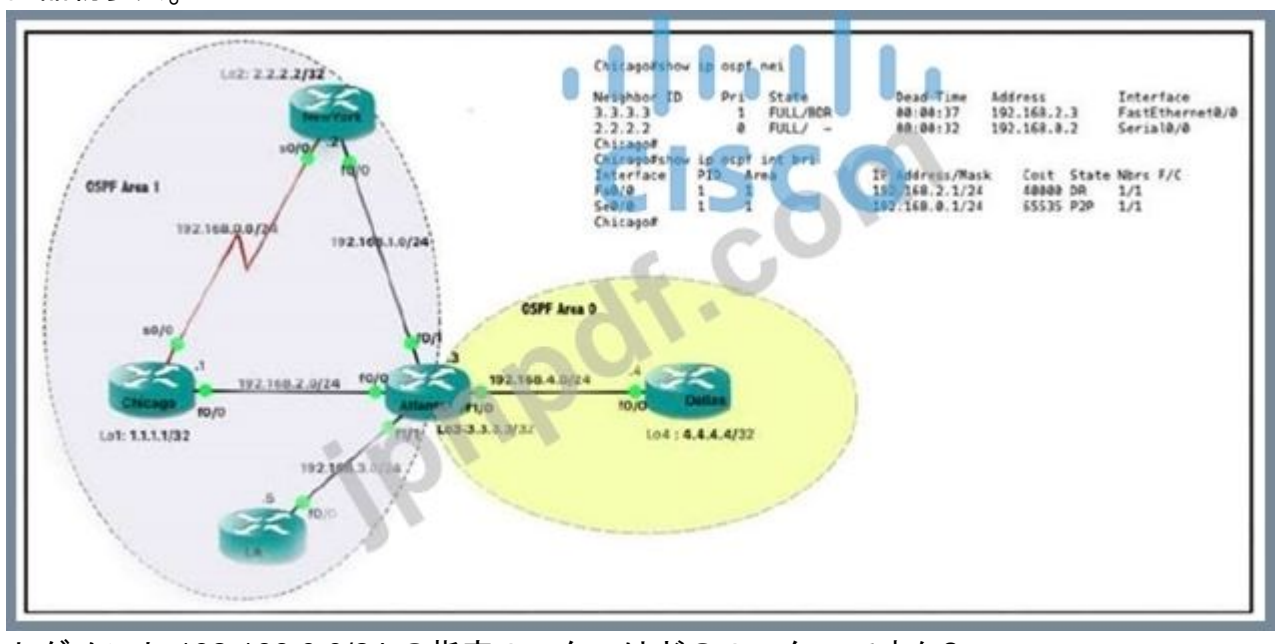
C. VRRP メンバー間の通信は MD5 を使用して暗号化されます

D. R1 が再起動すると、R2 が再起動するまで R2 がマスター仮想ルーターになります。

Answer: (解答を表示する**)**

最新問題: **223**

出品物参照。



セグメント 192.168.0.0/24 の指定ルーターはどのルーターですか?

A. このセグメントは、p2p ネットワーク タイプであるため、代表ルーターがありません。

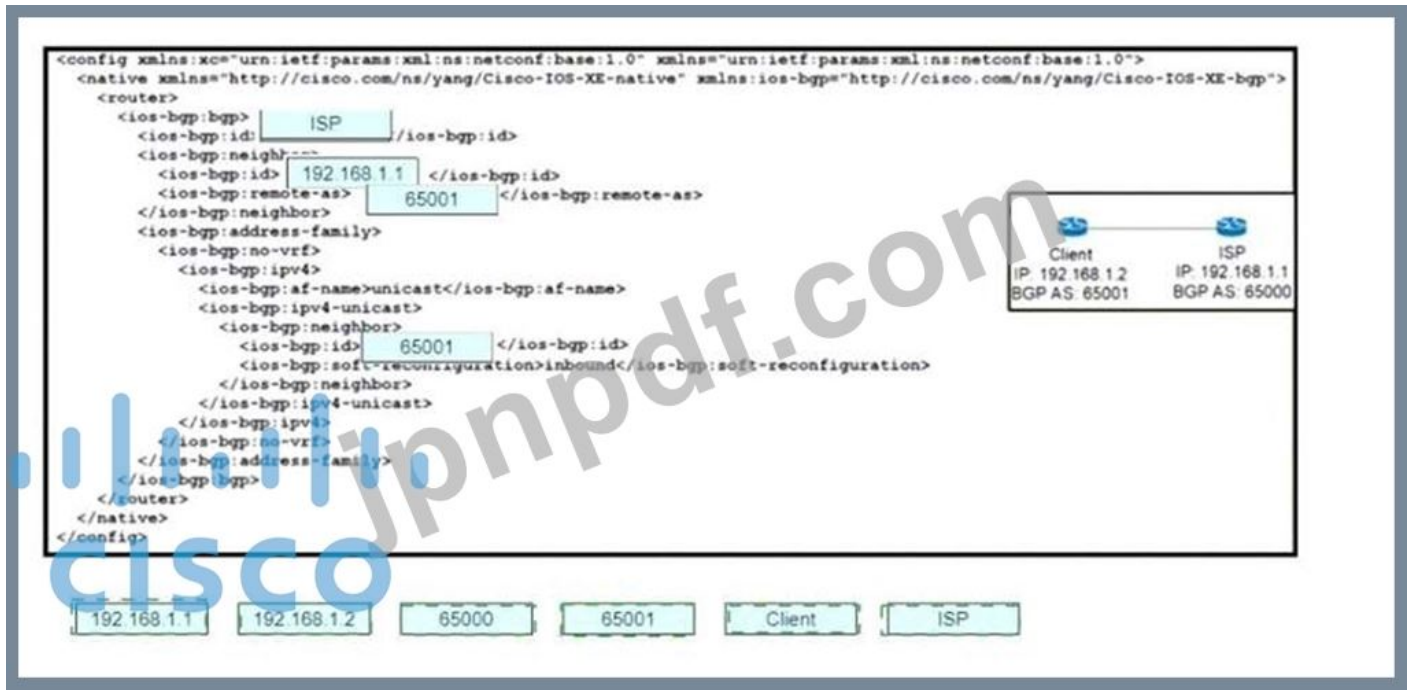
B. このセグメントは、非ブロードキャスト ネットワーク タイプであるため、指定ルーターがありません。

C. ルーター ID が低いため、ルーター シカゴ
D. ルーター ID が大きいため、Router NewYork
Answer: (解答を表示する**)**

最新問題**: 224**
SNR を計算するために必要な 2 つの情報はどれですか？ 2つ選んでください。）
A. 送信電力
B. アンテナゲイン
C. EIRP
D. ノイズフロア
E. RSSI
Answer: D,E (メーッセージを残す**)**

最新問題**: 225**
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、トポロジに従って BGP を構成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なく、一部のオプションは 2 回使用される場合があります。

Answer:



説明

グラフィカル ユーザー インターフェイス、テキスト、アプリケーション、電子メール 説明が自動的に生成される

最新問題: **226**

展示に戻ります。

```
event manager applet config-alert
event cli pattern "conf t.*" sync yes
```

展示を参照してください。ユーザーが構成モードに切り替えたときに、ネットワーク エンジニアに通知する必要があります。SNMP トラップとクリティカル レベルのログ メッセージを受信するには、どのスクリプトを適用する必要がありますか?

A)

```
action 1.0 snmp-trap strdata "Configuration change alarm"
action 2.0 syslog msg "Configuration change alarm"
```

B)

```
action 1.0 snmp-trap strdata "Configuration change critical alarm"
```

ハ）

```
action 1.0 snmp-trap strdata "Configuration change alarm"
action 1.0 syslog priority critical msg "Configuration change alarm"
```

D)

```
action 1.0 snmp-trap strdata "Configuration change alarm"
action 1.1 syslog priority critical msg "Configuration change alarm"
```

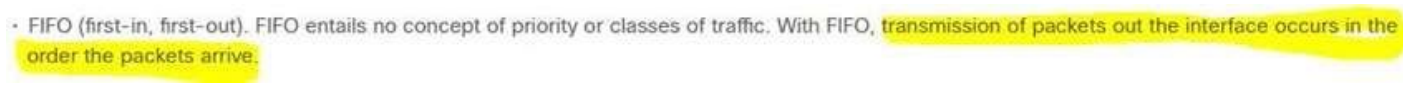
A. オプション B
B. オプション C
C. オプション A
D. オプション D
Answer: D (メーッセージを残す)

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 227**
LISP から非 LISP へのインターネットワーキングをサポートするために必要な 2 つの LISP インフラストラクチャ要素はどれですか? (2つ選んでください)
A. PETR
B. PITR
C. MR
D. MS
E. ALT
Answer: (解答を表示する)
説明
https://netmindblog.com/2019/12/04/lisp-locator-id-separation-protocol-part-ii-pxtr/

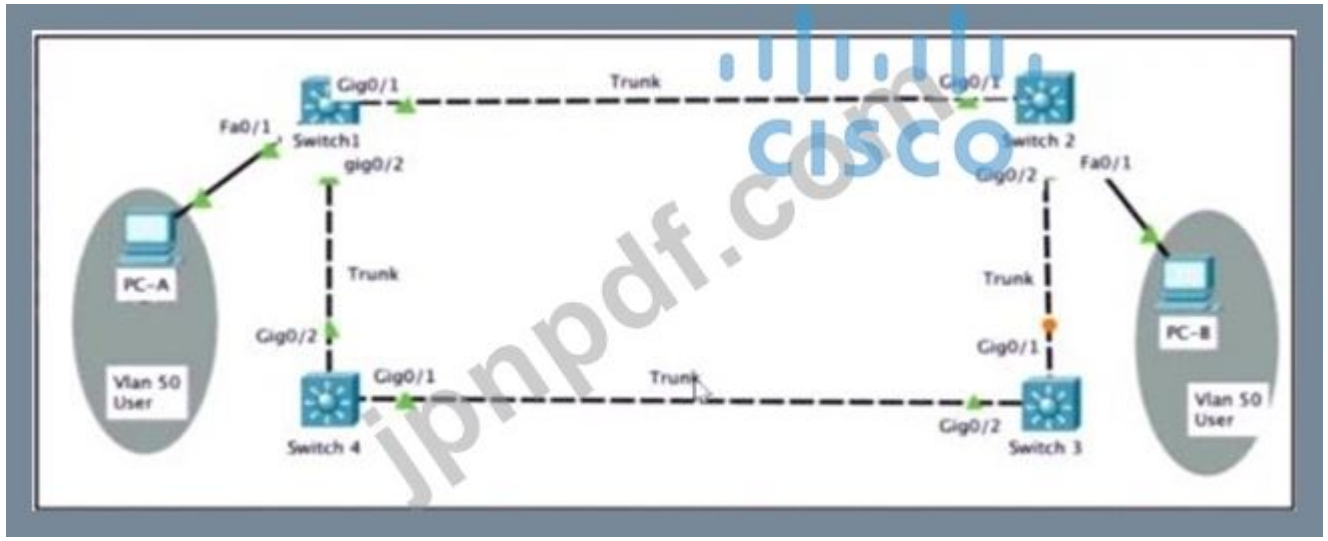
最新問題**: 228**
Cisco DNA Center がデバイスを検出するために使用する 3 つの方法はどれですか? (3つ選んでください)
A. CDP
B. SNMP
C. LLDP
D. ping
E. ネットコンフ
F. 指定された範囲の IP アドレス
Answer: (解答を表示する)

最新問題: **229**
パケットが到着した順序でインターフェイスからパケットを送信する QoS キューイング方式はどれですか?
A. カスタム
B. 加重公平
C. FIFO
D. 優先度
Answer: C (メーッセージを残す**)**
説明

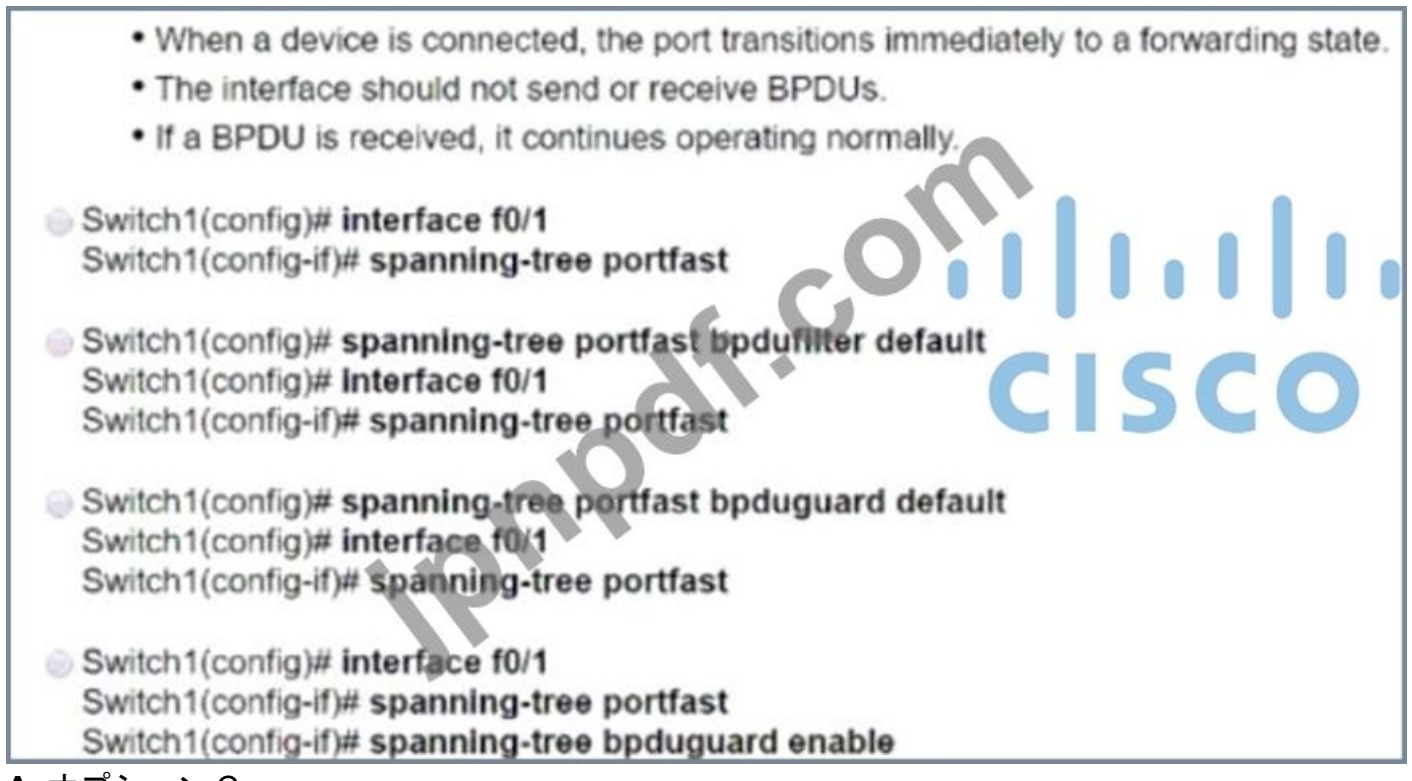


先入れ先出し (FIFO): FIFO には、トラフィックの優先順位やクラスの概念はありません。FIFO を使用すると、インターフェイスからのパケットの送信は、パケットが到着した順序で行われます。つまり、QoS はありません。

最新問題: **230**
展示を参照してください。



すべてのスイッチで Rapid PVST+ がイネーブルになっています。ポート fa0/1 で次の結果を得るには、switch1 でどのコマンド セットを設定する必要がありますか?



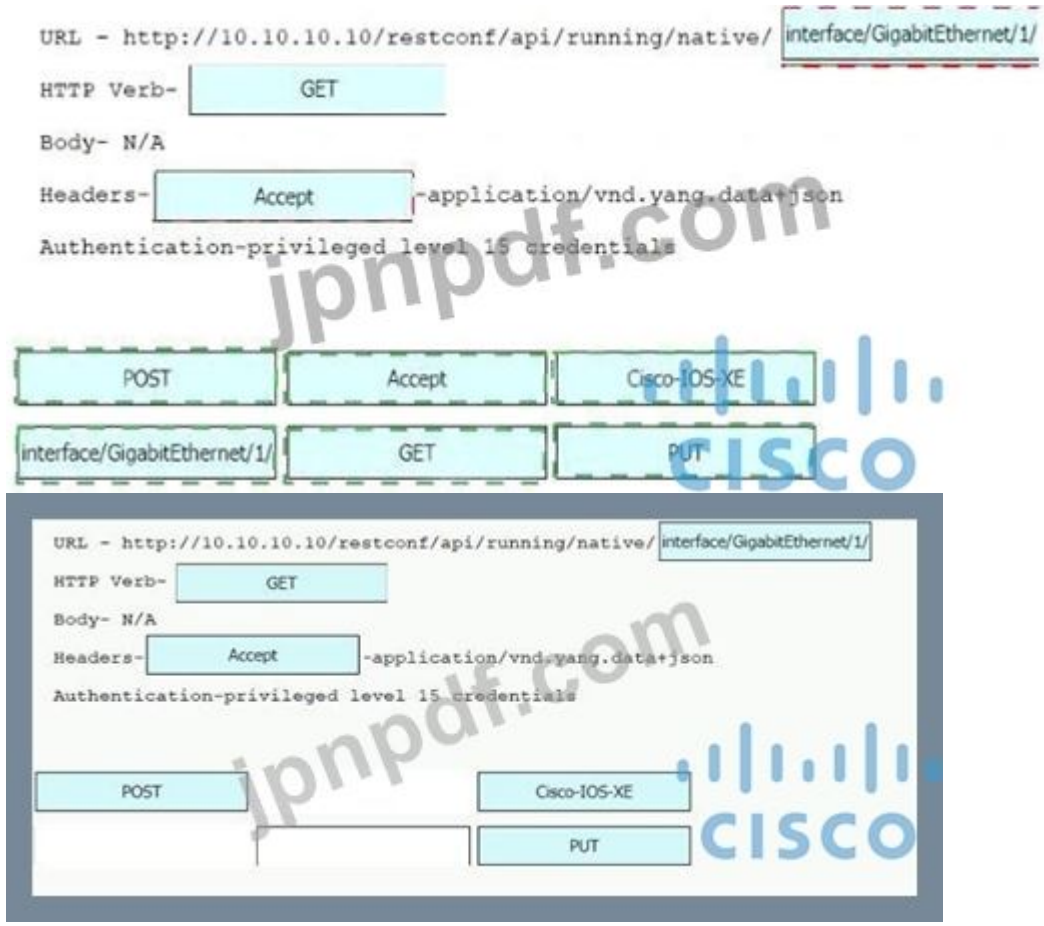
A. オプション C
B. オプション A
C. オプション B
D. オプション D

Answer: (解答を表示する)

最新問題: **231**

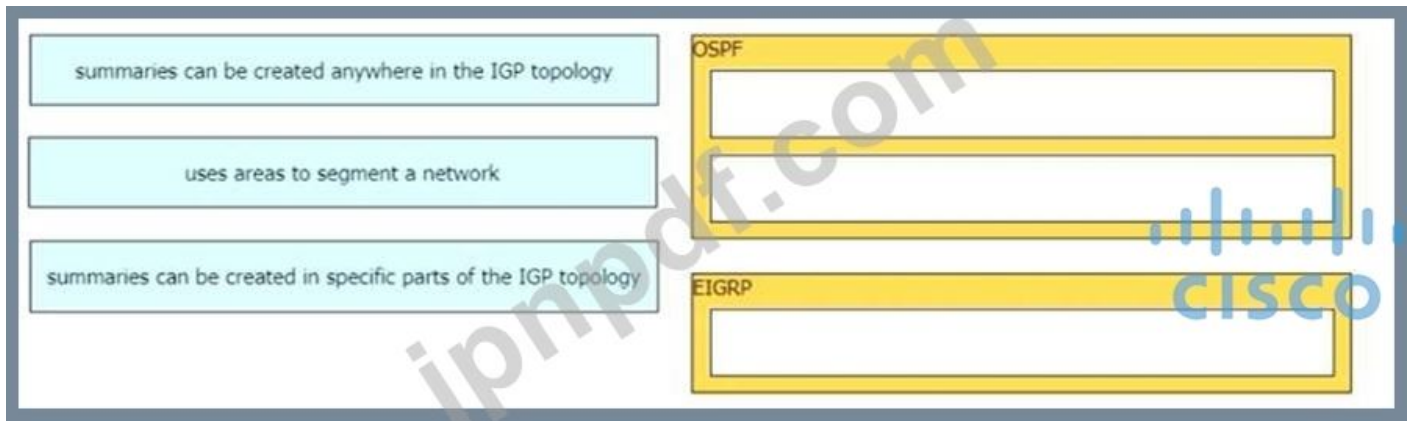
展示を参照してください スニペットを RESTCONF リクエストにドラッグ アンド ドロップして、このレスポンスを返すリクエストを作成します すべてのオプションが使用されるわけではありません

Answer:



最新問題**: 232**

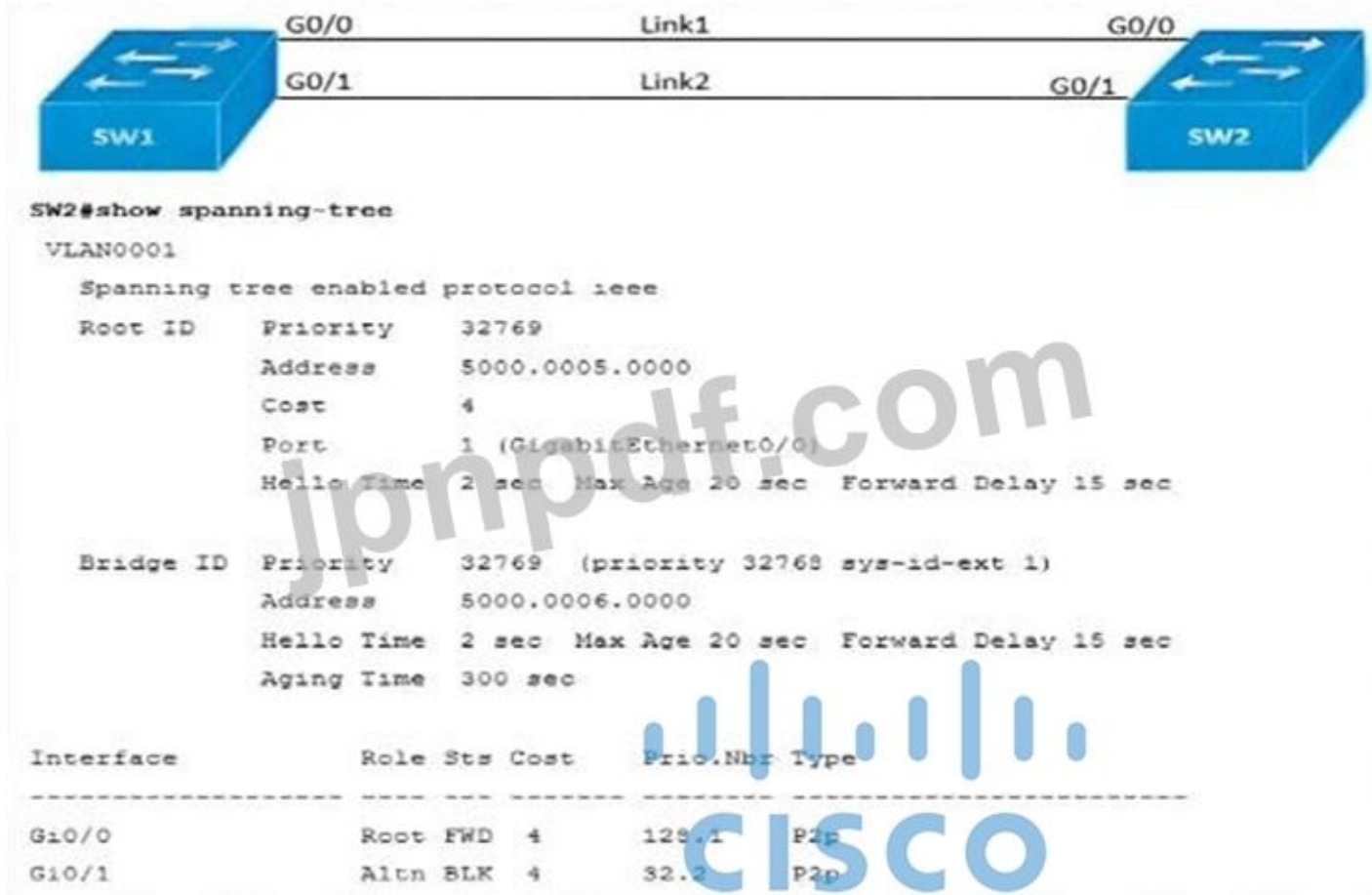
左側の説明を右側のルーティング プロトコルにドラッグ アンド ドロップします。



Answer:

最新問題**: 233**

展示を参照してください。



Link1 は銅線接続で、Link2 はファイバー接続です。ファイバー ポートは、すべての転送のプライマリ ポートである必要があります。SW2 での show spanning-tree コマンドの出力は、ファイバ ポートがスパニング ツリーによってブロックされていることを示しています。エンジニアが SW2 の GO/1 で spanning-tree port-priority 32 コマンドを入力しますが、ポートはブロックされたままです。問題を解決するには、Link2 に接続されているポートでどのコマンドを入力する必要がありますか?

A. SW1 でスパニング ツリー ポート プライオリティ 32 を入力します。

B. SW1 でスパニング ツリー ポート プライオリティ 224 を入力します。

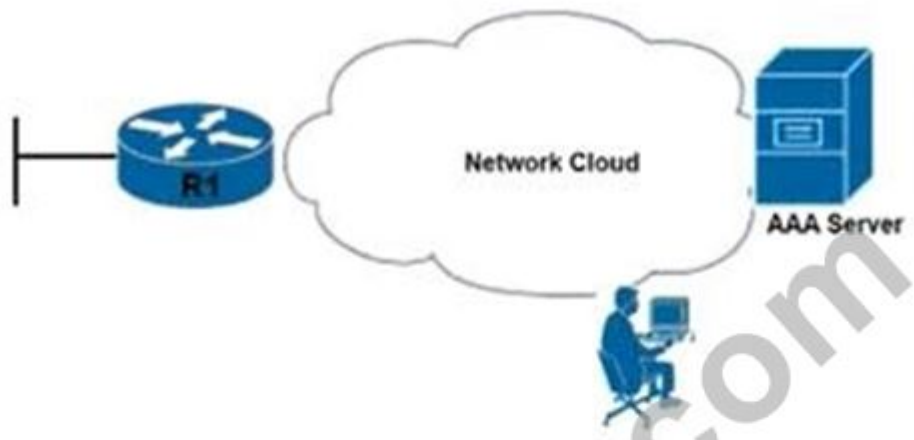
C. SW2 でスパニング ツリー ポート プライオリティ 4 を入力します。

D. SW2 でスパニング ツリー ポート プライオリティ 64 を入力します。

Answer: A (メーッセージを残す**)**

説明
SW1 は、2 つのスイッチ間のブリッジング ループを回避するために、SW2 へのポートの 1 つをブロックする必要があります。
残念ながら、ファイバー ポート Link2 がブロックされました。しかし、SW2 はブロックされたポートをどのように選択するのでしょうか? その答えは、SW1 から受信した BPDU に基づいています。answer 'Enter spanning-tree port-priority 32 on SW1' BPDU は、次の場合に他のものよりも優れています。
1. SW1 でスパニング ツリー ポート プライオリティ 32 を入力してください」と答え、ルート ブリッジ ID を下げます。
2. SW1 でスパニング ツリー ポート プライオリティ 32 を入力してください」と答えて、ルートへのパス コストを下げます
3. SW1 でスパニング ツリー ポート プライオリティ 32 を入力してください」と回答し、送信ブリッジ ID を下げます。
4. answer 'Enter spanning-tree port-priority 32 on SW1' Lower 送信ポート ID これら 4 つのパラメータが順番に検査されます。この特定のケースでは、SW1 によって送信されたすべての BPDU は、同じルート ブリッジ ID、ルートへの同じパス コスト、および同じ送信ブリッジ ID を持ちます。最適なものを選択するために残された唯一のパラメーターは、送信ポート ID (ポート ID = ポート優先度 + ポート インデックス) です。また、Gi0/0 のポート インデックスは Gi0/1 のポート インデックスよりも小さいため、リンク 1 がプライマリ リンクとして選択されています。
したがって、プライマリ リンクを変更するには、ポート プライオリティを変更する必要があります。ポート プライオリティの数値が小さいほど、そのポートのプライオリティは高くなります。つまり、SW1 の Gi0/1 (SW2 の Gi0/1 ではなく) のポート プライオリティを、Gi0/0 のポート プライオリティよりも低い値に変更する必要があります。

最新問題: **234**
展示に戻ります。




```
Router1$ ssh -s admin@192.168.20.3 -p 830 netconf
admin@192.168.20.3's password: cisco123

<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
<capability>urn:ietf:params:netconf:base:1.1</capability>
<capability>urn:ietf:params:netconf:capability:writable-
running:1.0</capability>
<capability>urn:ietf:params:netconf:capability:xpath:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
<capability>urn:ietf:params:netconf:capability:rollback-on-
error:1.0</capability
--snip--
</capabilities>
<session-id>2870</session-id></ hello>]]>]]>

Use < ^C > to exit
```

展示を参照してください。エンジニアがルーター R1 へのログインを試みます。ログインに成功するのはどの構成ですか?

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
```

ハ）

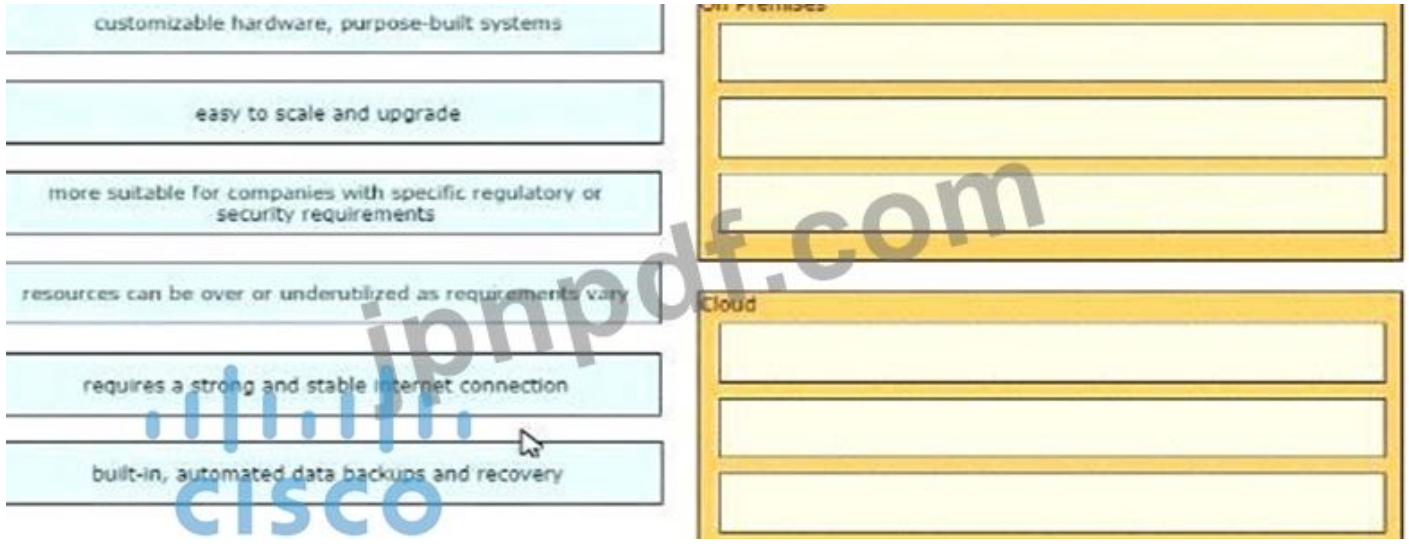
```
R1# aaa new-model
aaa authorization exec default local
enable aaa admin privilege 15
```

D)

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

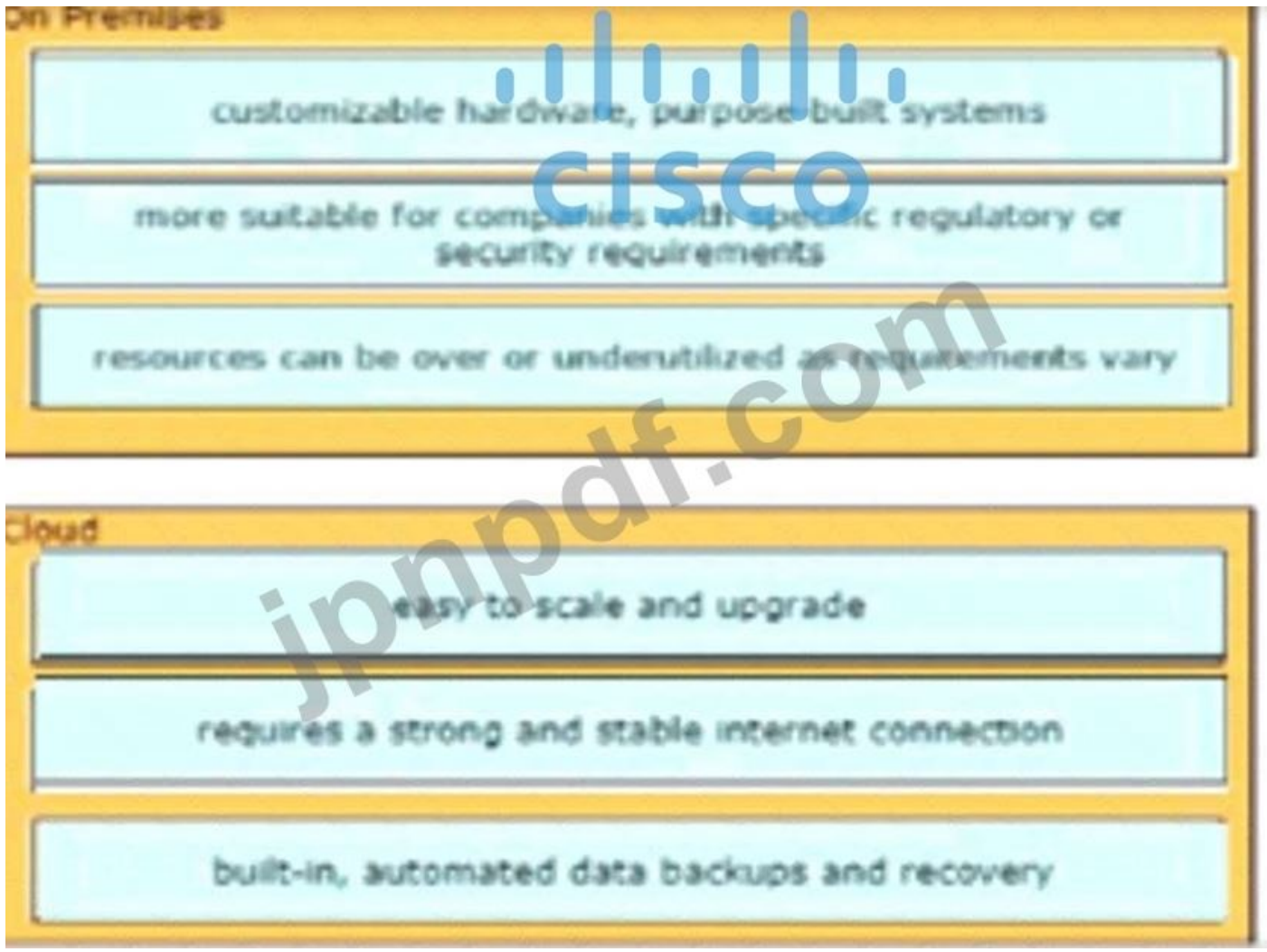
A. オプション D
B. オプション A
C. オプション C
D. オプション B
Answer: (解答を表示する)

最新問題: **235**
特性を左側から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:

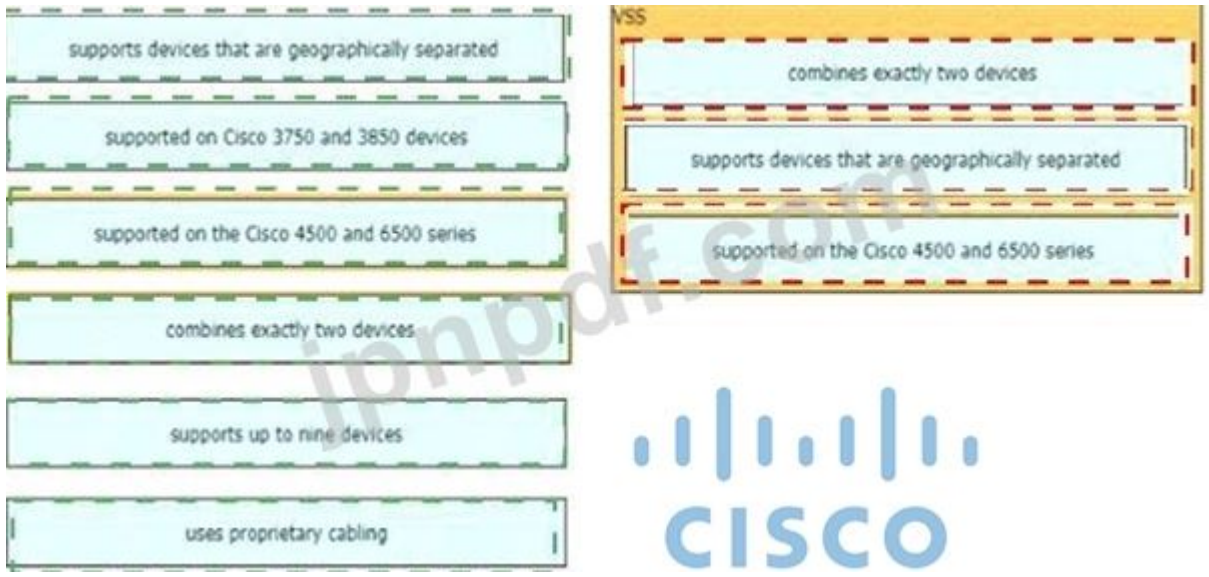
説明
オンプレミス: カスタマイズ可能な特定の要件、リソース
クラウド: スケール、組み込みの自動バックアップ、強力で安定したインターネット



最新問題: **236**

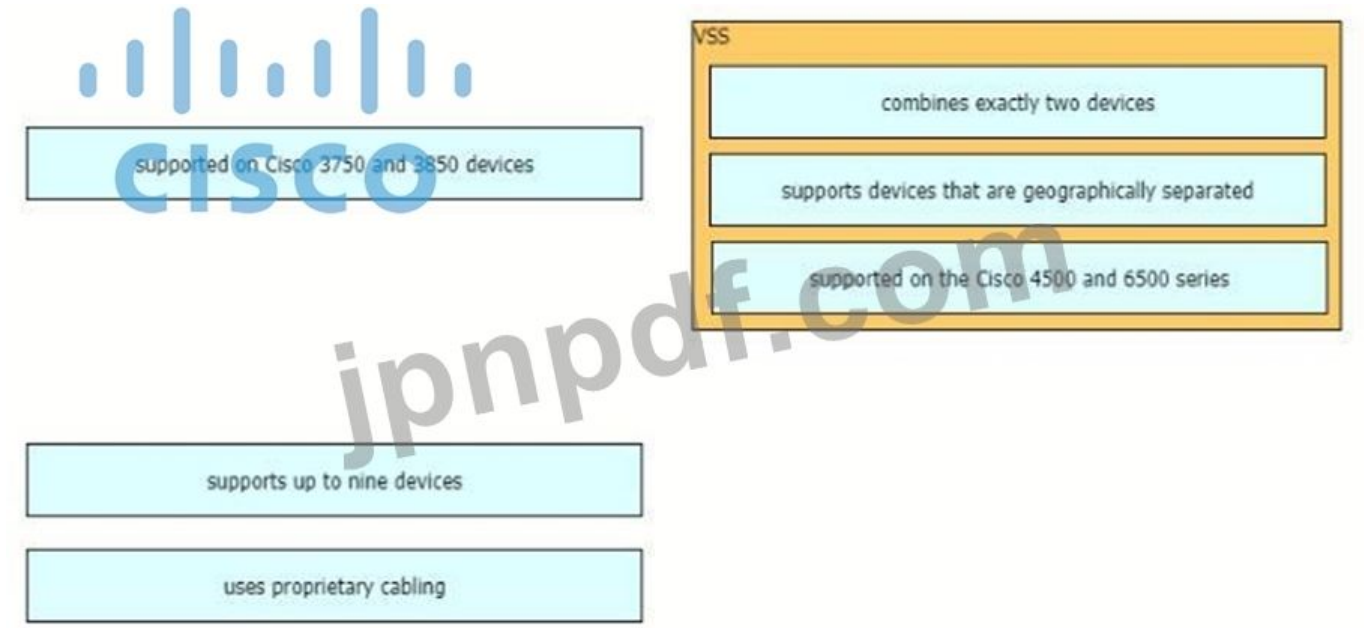
VSS テクノロジの説明を左から右にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。

Answer:



説明

グラフィカル ユーザー インターフェイス 説明の自動生成



最新問題: **237**

BFD を使用する利点は何ですか?

A. レイヤー 1 およびレイヤー 3 の問題に対して、1 秒未満の障害検出が可能です。

B. レイヤ 3 でローカル リンク障害を検出し、ルーティング プロトコルを更新します。

C. レイヤー 1 およびレイヤー 2 の問題を 1 秒未満で検出します。

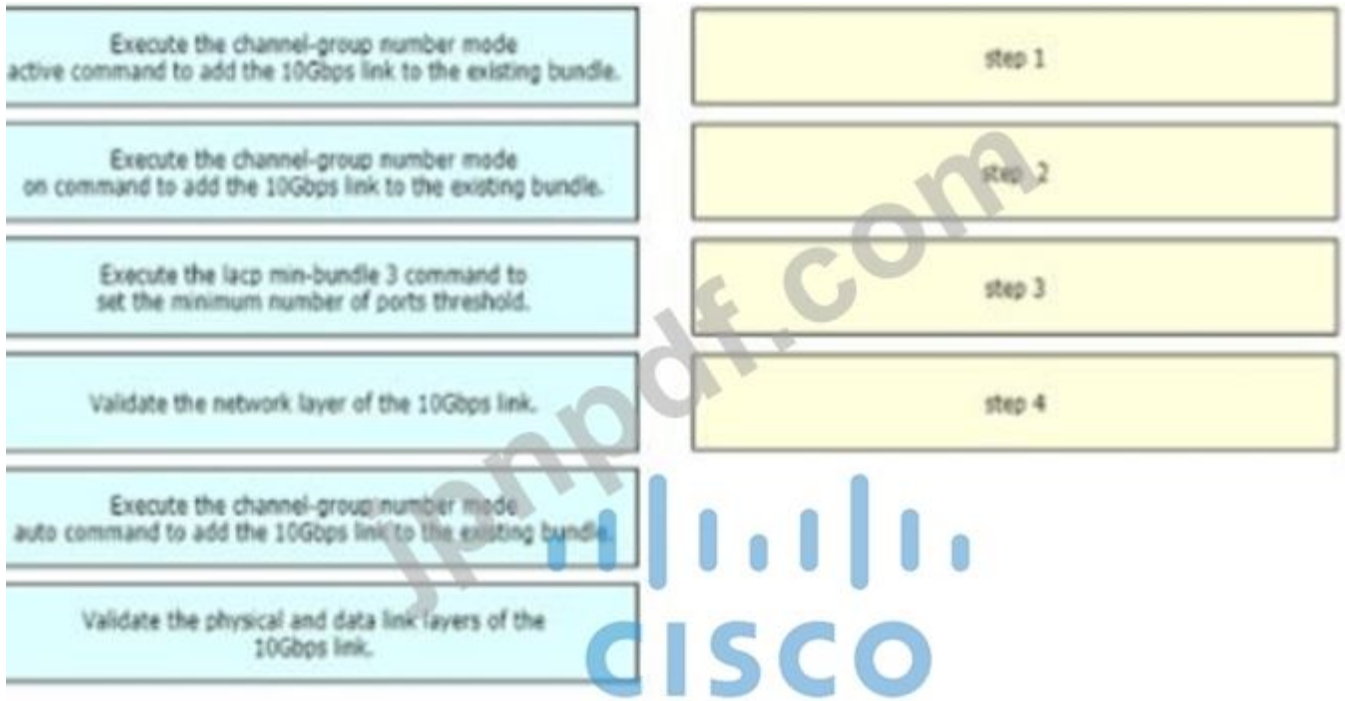
D. レイヤ 1 でローカル リンク障害が発生し、ルーティング テーブルを更新します。

Answer: A (メーッセージを残す**)**

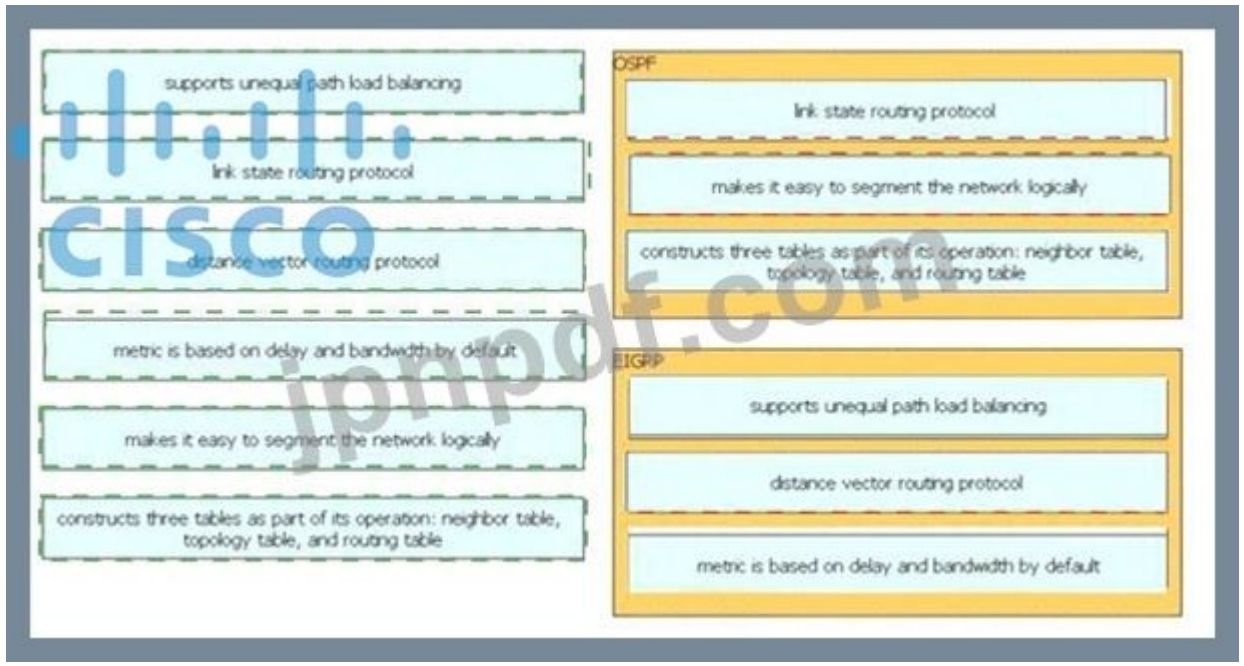
最新問題: **238**

ネットワーク エンジニアは、既存の 2x10Gps LACP ベースの LAG に 10Gps リンクを追加して、その容量を増やしています。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にバンドル インターフェイスをアウト オブ サービスにする必要があり、実稼働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のあるタスクを左から右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。

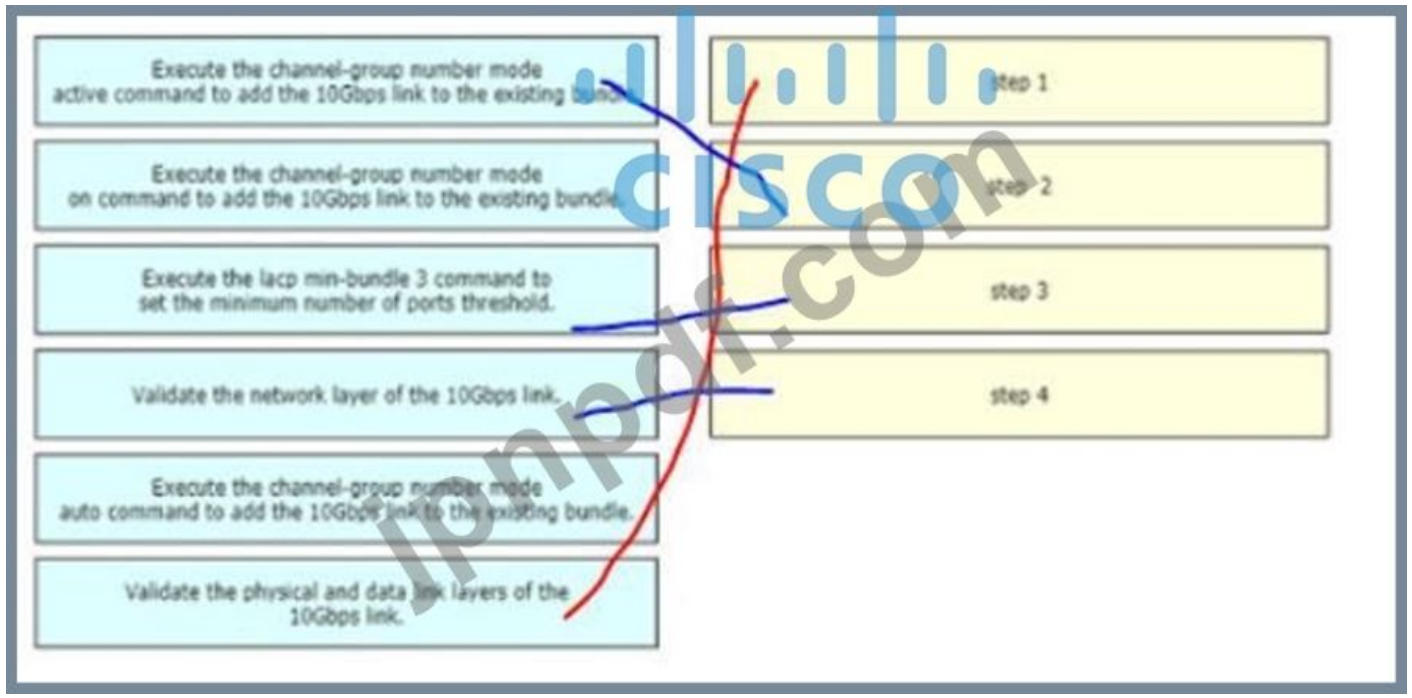


Answer:



説明

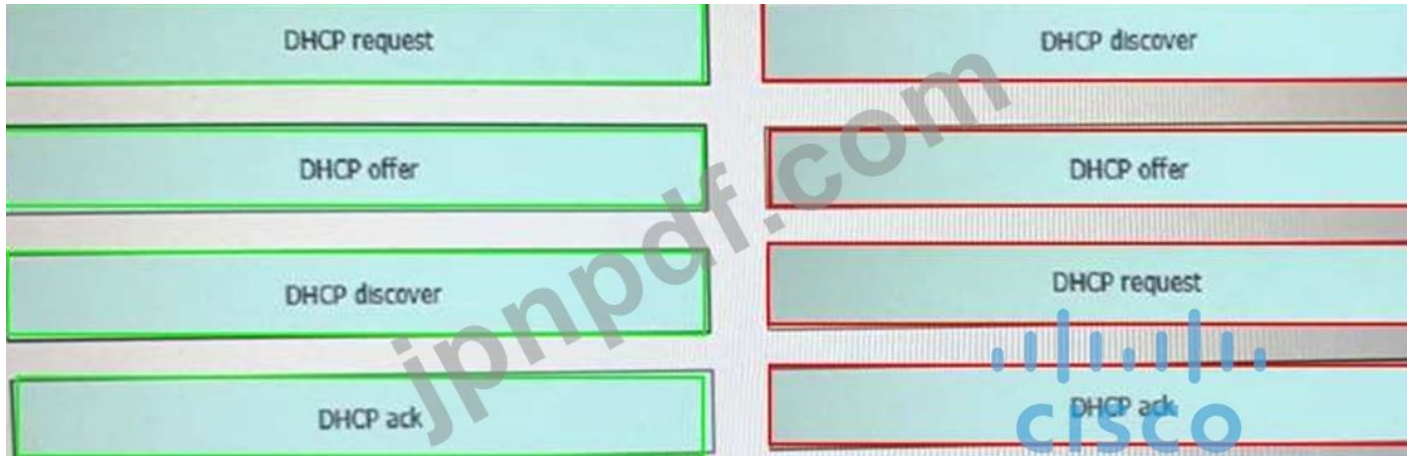
図を含む画像 自動生成された説明



最新問題**: 239**

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

Answer:



最新問題**: 240**

cisco SD-WAN ファブリックで vManage によって処理される機能はどれですか?

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

最新問題**: 241**

展示を参照してください。エンジニアが新しい HSRP グループを設定します。HSRP ステータスを確認しているときに、エンジニアは R2 で生成されたロギング メッセージを確認します。メッセージの原因はどれですか?
A. PC が IP アドレス 10.10.1.1 を使用してネットワーク上にある
B. HSRP 構成が原因でルーティング ループが発生しました
C. 2 つの HSRP グループに同じ仮想 IP アドレスが設定されています
D. HSRP 構成が原因で、スパニング ツリー ループが発生しました。
Answer: C (メーッセージを残す**)**

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード**: Freepdfdumps**)

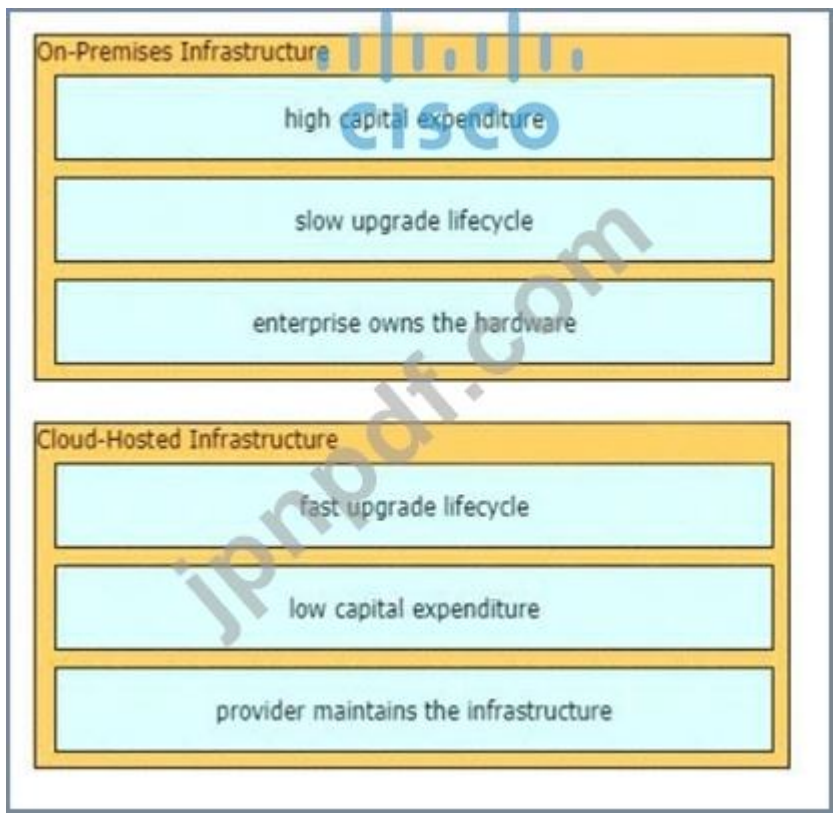
最新問題**: 242**
左側の特性を右側のインフラストラクチャ タイプにドラッグ アンド ドロップします。


enterprise owns the hardware
low capital expenditure
provider maintains the infrastructure
slow upgrade lifecycle
high capital expenditure
fast upgrade lifecycle
On-Premises Infrastructure
Cloud-Hosted Infrastructure

Answer:

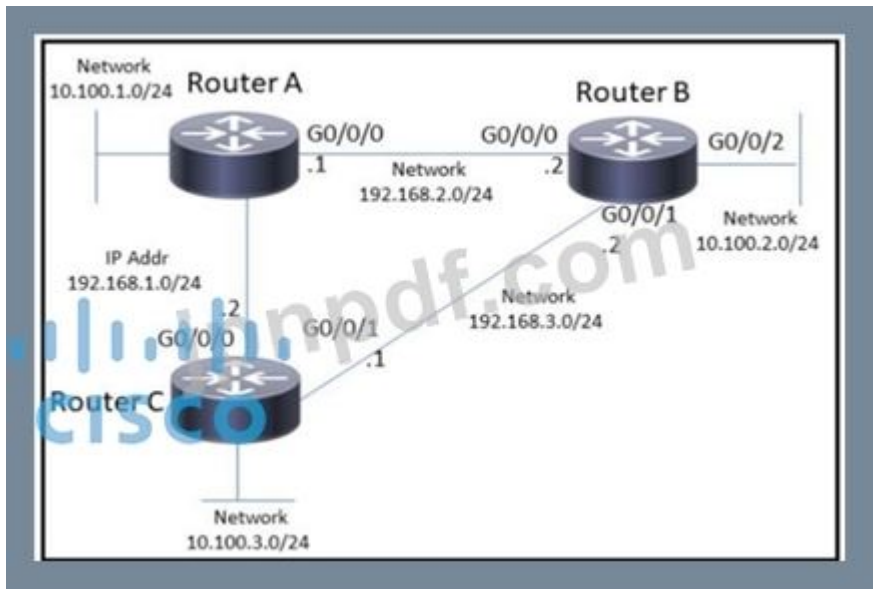

enterprise owns the hardware
low capital expenditure
provider maintains the infrastructure
slow upgrade lifecycle
high capital expenditure
fast upgrade lifecycle
On-Premises Infrastructure
high capital expenditure
slow upgrade lifecycle
enterprise owns the hardware
Cloud-Hosted Infrastructure
fast upgrade lifecycle
low capital expenditure
provider maintains the infrastructure

説明


On-Premises Infrastructure
high capital expenditure
slow upgrade lifecycle
enterprise owns the hardware
Cloud-Hosted Infrastructure
fast upgrade lifecycle
low capital expenditure
provider maintains the infrastructure

最新問題**: 243**
TCP パフォーマンスの低下を防ぐ QoS メカニズムはどれですか?
A. シェイパー
B. ポリサー
C. WRED
D. レート制限
E. LLQ
F. フェアキュー
Answer: (解答を表示する**)**
Weighted Random Early Detection (WRED; 加重ランダム早期検出)は、単なる輻輳回避メカニズムです。WRED は、IP 優先順位に基づいてパケットを選択的にドロップします。エッジ ルーターは、パケットがネットワークに入るときに IP 優先順位を割り当てます。パケットが到着すると、次のイベントが発生します。
1. 平均キュー サイズが計算されます。
2. 平均値が最小キューしきい値未満の場合、到着パケットはキューに入れられます。
3. 平均がそのタイプのトラフィックの最小キューしきい値とインターフェイスの最大しきい値の間にある場合、そのタイプのトラフィックのパケットドロップ確率に応じて、パケットはドロップされるかキューに入れられます。
4. 平均キュー サイズが最大しきい値より大きい場合、パケットはドロップされます。
WRED は、出力インターフェイスが輻輳の兆候を示し始めたときにパケットを選択的にドロップすることで、テール ドロップ (キューがいっぱいになるとパケットがドロップされる)の可能性を減らします (したがって、キューがいっぱいになるのを防ぐことで輻輳を緩和できます)。キューがいっぱいになるまで待機するのではなく、一部のパケットを早期にドロップすることで、WRED は一度に大量のパケットをドロップすることを回避し、グローバル同期の可能性を最小限に抑えます。したがって、WRED を使用すると、伝送回線を常にフルに使用できます。
WRED は通常、IP 優先順位に基づいてパケットを選択的にドロップします。IP 優先順位が高いパケットは、優先順位が低いパケットよりもドロップされる可能性が低くなります。したがって、パケットの優先順位が高いほど、パケットが配信される可能性が高くなります。
参考 :https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/15-mt/qos-conavd-15-mt-book/qos-conavd- cfg-wred.html WRED は、トラフィックの大部分が TCP/IP トラフィックである場合にのみ役立ちます。TCP では、ドロップされたパケットは輻輳を示しているため、パケット ソースはその伝送速度を低下させます。他のプロトコルでは、パケット ソースが応答しないか、ドロップされたパケットを同じレートで再送信する場合があります。したがって、パケットをドロップしても輻輳は減少しません。
参考 :https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/xe-16/qos-conavd-xe-16-book/qos-conavd-oview.html

最新問題**: 244**
展示を参照してください。ネットワーク エンジニアは、10.100 2.248 ～ 2.248 の範囲のホストからの Telnet トラフィックをブロックする必要があります。
10.100.2 255 をネットワーク 10.100.3.0 に送信し、それ以外はすべて許可します。エンジニアはどの構成を適用する必要がありますか?



A)

```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 22
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

B)

```
RouterB(config)# access-list 101 deny icmp 10.100.2.0 0.0.0.248 10.100.2.0 0.0.0.248
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

ハ）

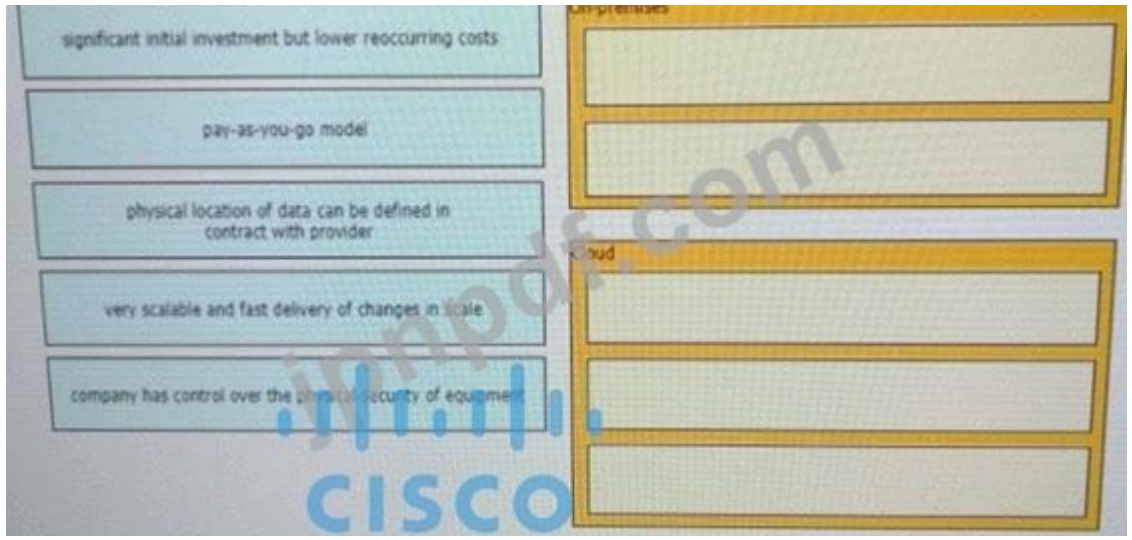
```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 23
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

D)

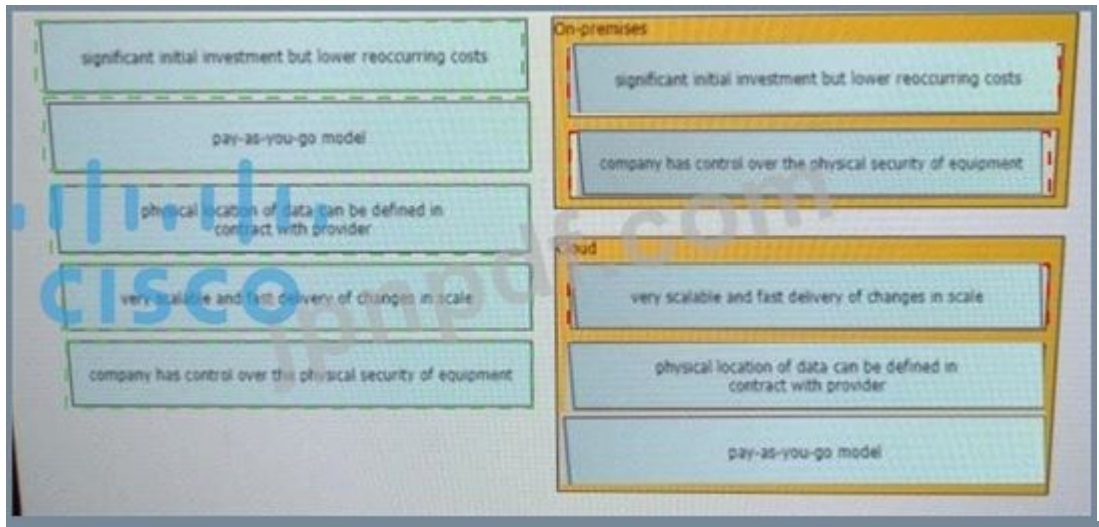
```
RouterB(config)# access-list 101 permit tcp 10.100.2.0 0.0.0.252 10.100.3.0 0.0.0.255
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

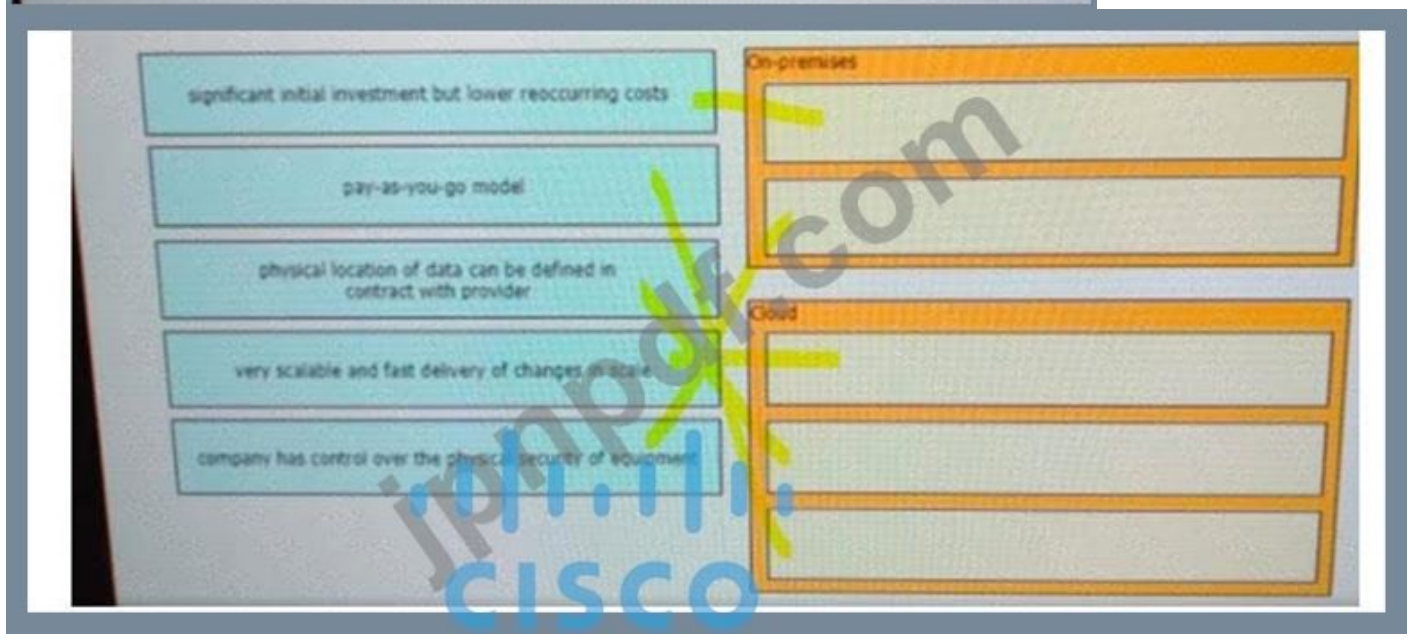
A. オプション B
B. オプション D
C. オプション A
D. オプション C
Answer: (解答を表示する**)**

最新問題**: 245**
特性を左側から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: **246**

展示を参照してください。

ネットワーク エンジニアは、認証に ISE-Servers グループを使用するようにルータを設定する必要があります。両方の ISE サーバが使用できない場合は、ローカル ユーザ名データベースを使用する必要があります。設定でユーザ名が定義されていない場合、イネーブル パスワードはログインするための最後の手段である必要があります。この結果を得るには、どの設定を適用する必要がありますか?

A. AAA 認証ログイン デフォルト グループ ISE-Servers ローカル イネーブル

B. aaa authentication login default group enable local ISE-Servers

C. AAA 認証 exec デフォルト グループ ISE-Servers ローカル イネーブル

D. aaa authentication login error-enable

Answer: A (メーッセージを残す**)**

aaa authentication login default group enable local ISE-Servers

最新問題**: 247**

別紙参照。

基礎となる物理トポロジで MTU が構成されており、トンネル インターフェイスで MTU コマンドが構成されていません。DF ビットがクリアされていると仮定すると、1500 バイの IPv4 パケットがホスト X からホスト Y への GRE トンネルを通過するとどうなりますか?

A. パケットはフラグメント化されてルーター C に到着します。

B. パケットはルーター B で破棄されます

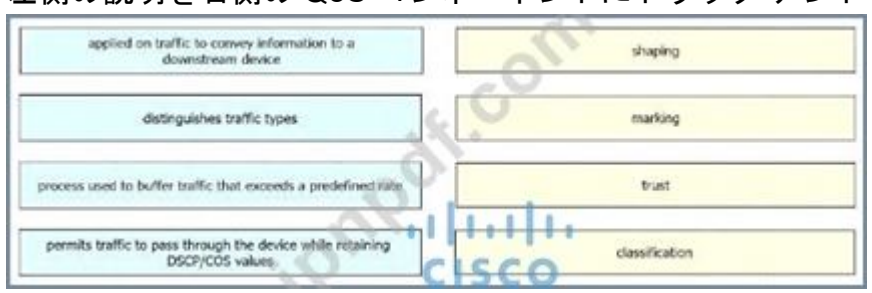
C. パケットはルーター A で破棄されます

D. パケットはフラグメント化されずにルーター C に到着します。

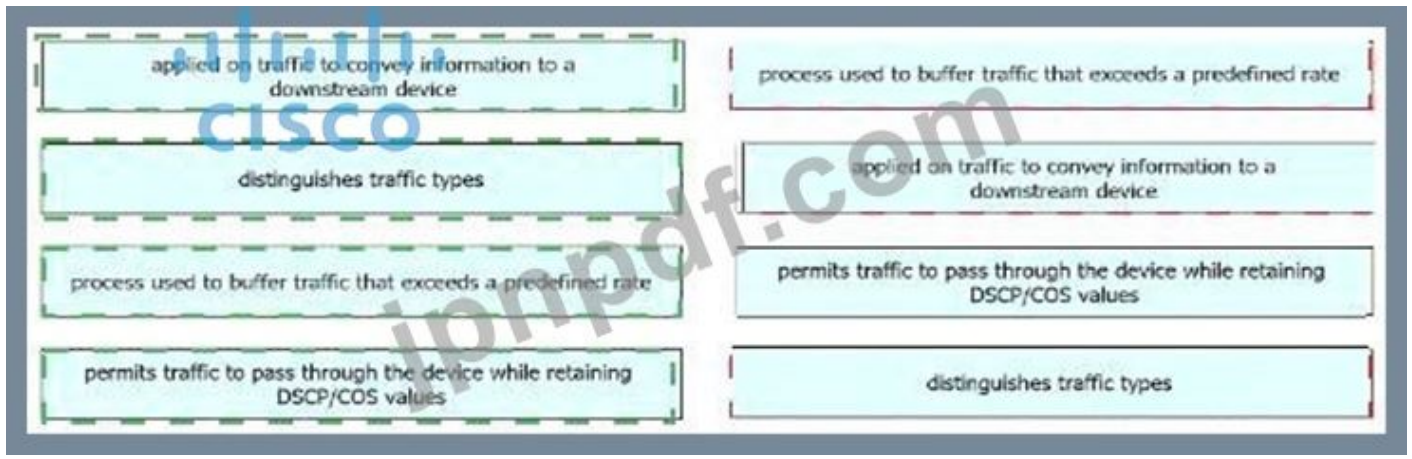
Answer: D (メーッセージを残す**)**

最新問題**: 248**

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。

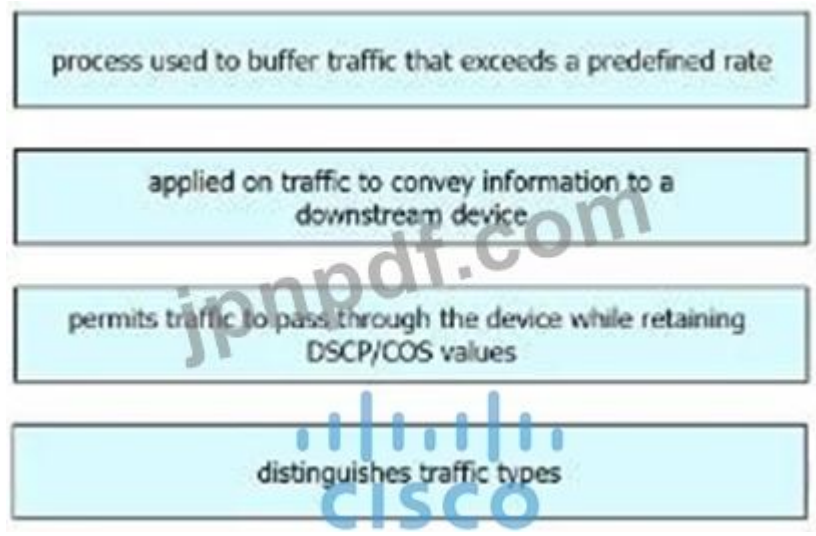


Answer:



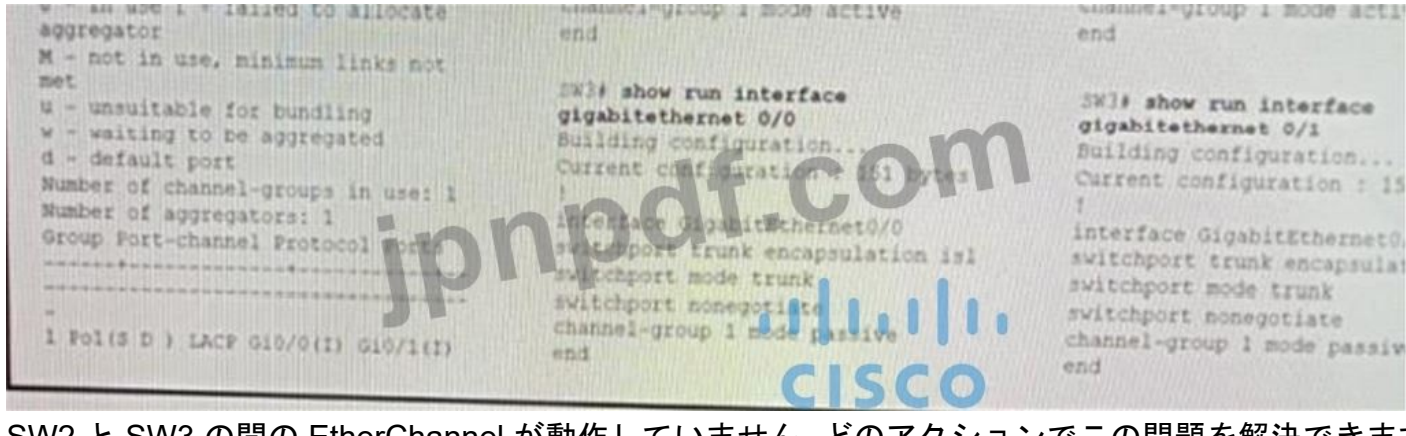
説明

グラフィカル ユーザー インターフェイス、テキスト、アプリケーション、電子メール 説明が自動的に生成される



最新問題: **249**

展示を参照してください。



SW2 と SW3 の間の EtherChannel が動作していません。どのアクションでこの問題を解決できますか?

A. SW2 Gi0/1 および Gi0/1 のチャネル グループ モードをオンに構成します。

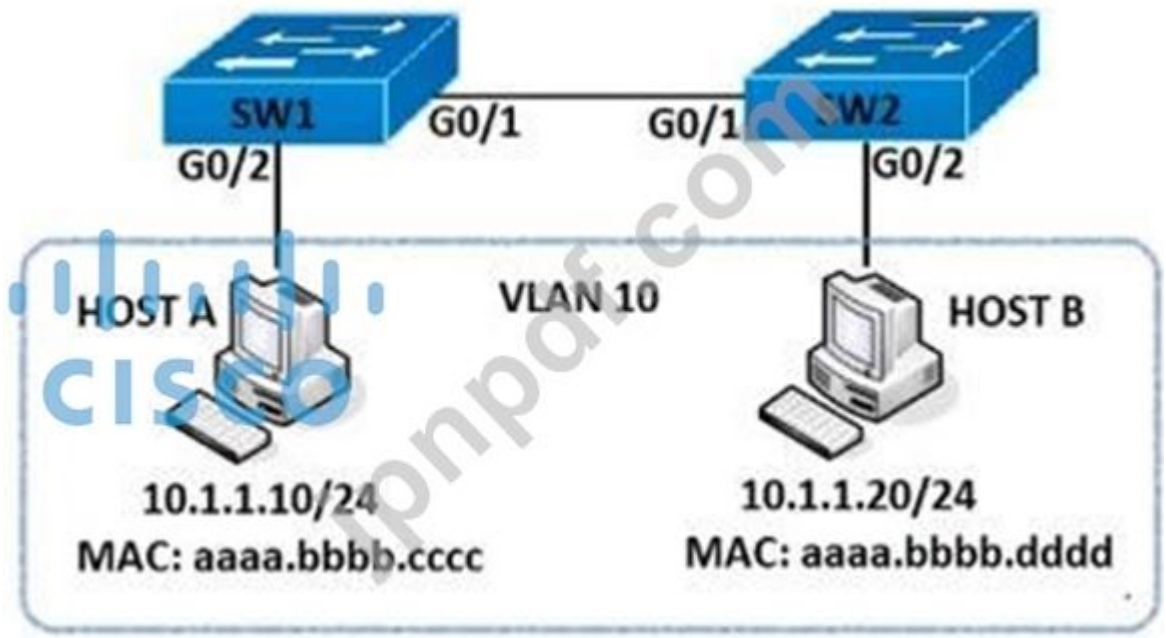
B. SW2 Gi0/0 のモードをトランクに構成します。

C. アクセスする SW2 Gi0/1 のモードを構成します。

D. SW3 Gi0/1 のチャネル グループ モードをアクティブに構成します。

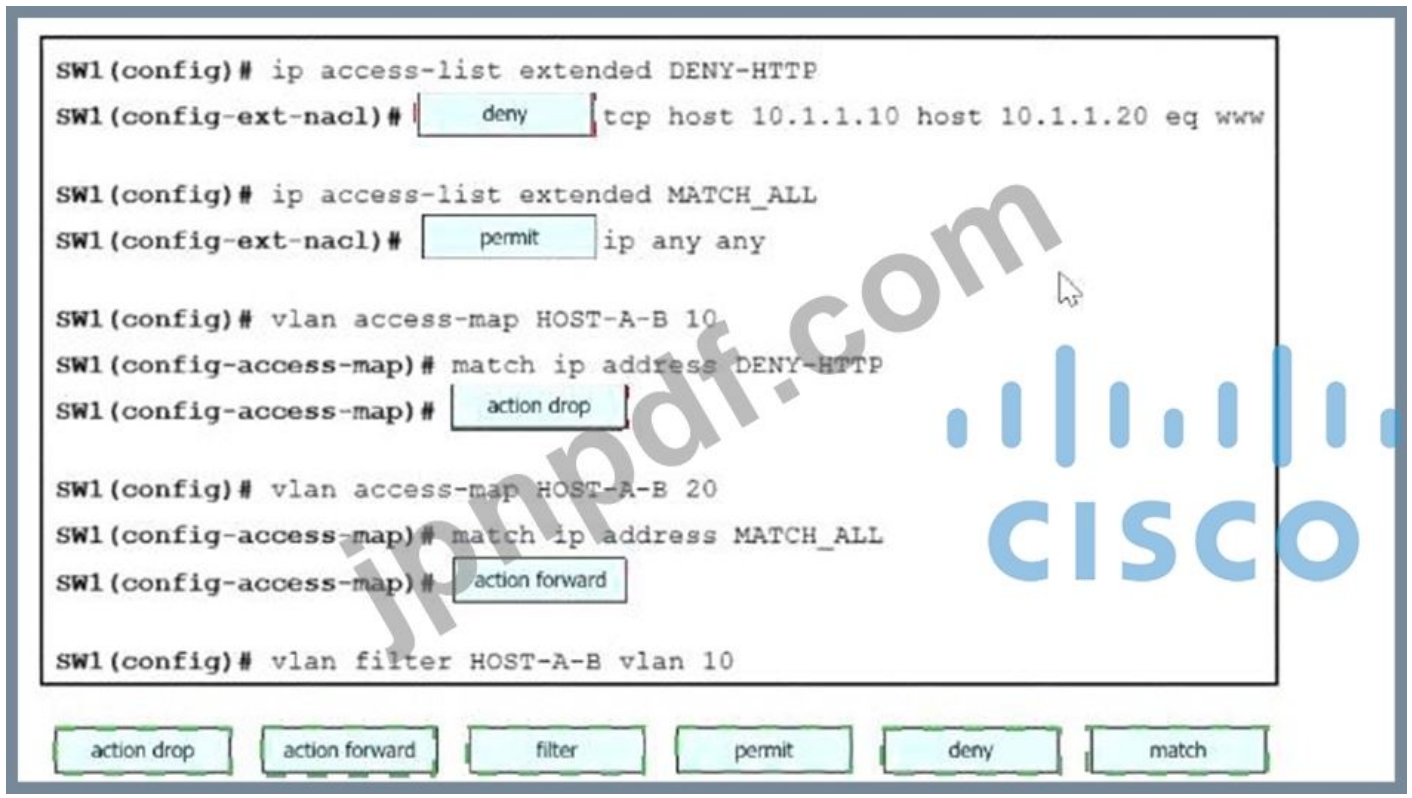
Answer: B (メーッセージを残す**)**

最新問題: **250**
展示を参照してください。



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する必要があります。これらの結果を得るには、コマンドを構成にドラッグ アンド ドロップします。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:



説明

拒否

許可

アクションドロップ

アクションフォワード

最新問題: **251**

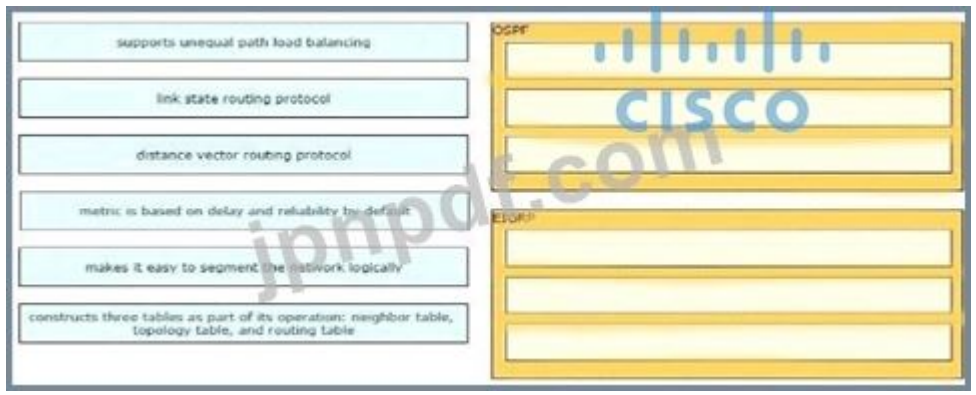
展示を参照してください。

Link1 は銅線接続で、Link2 はファイバー接続です。ファイバー ポートは、すべての転送のプライマリ ポートである必要があります。SW2 での show spanning-tree コマンドの出力は、ファイバ ポートがスパニング ツリーによってブロックされていることを示しています。エンジニアが SW2 の GO/1

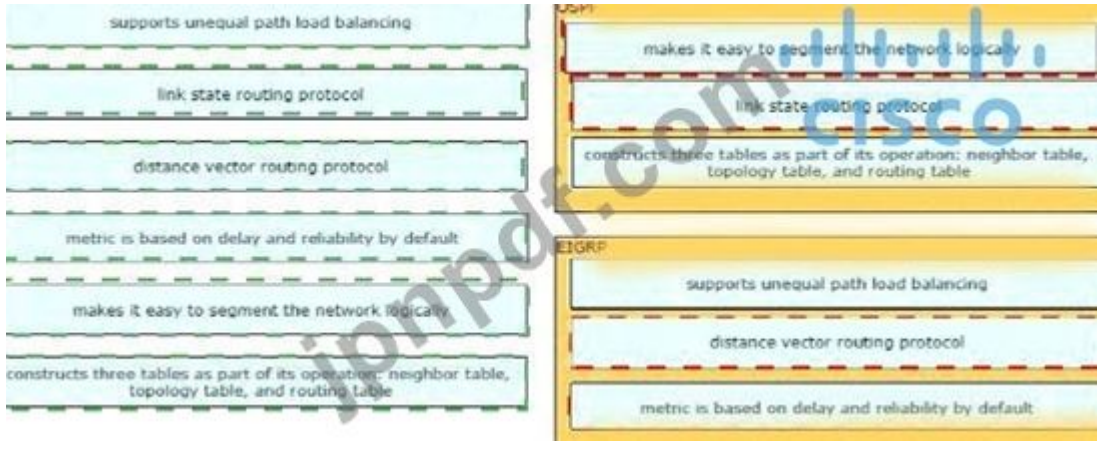
で spanning-tree port-priority 32 コマンドを入力しますが、ポートはブロックされたままです。問題を解決するには、Link2 に接続されているポートでどのコマンドを入力する必要がありますか?

A. SW1 でスパニング ツリー ポート プライオリティ 32 を入力します。
B. SW1 でスパニング ツリー ポート プライオリティ 224 を入力します。
C. SW2 でスパニング ツリー ポート プライオリティ 64 を入力します。
D. SW2 でスパニング ツリー ポート プライオリティ 4 を入力します。
Answer: (解答を表示する**)**

最新問題**: 252**
左側の特性を右側の正しいルーティング プロトコル タイプにドラッグ アンド ドロップします。



Answer:



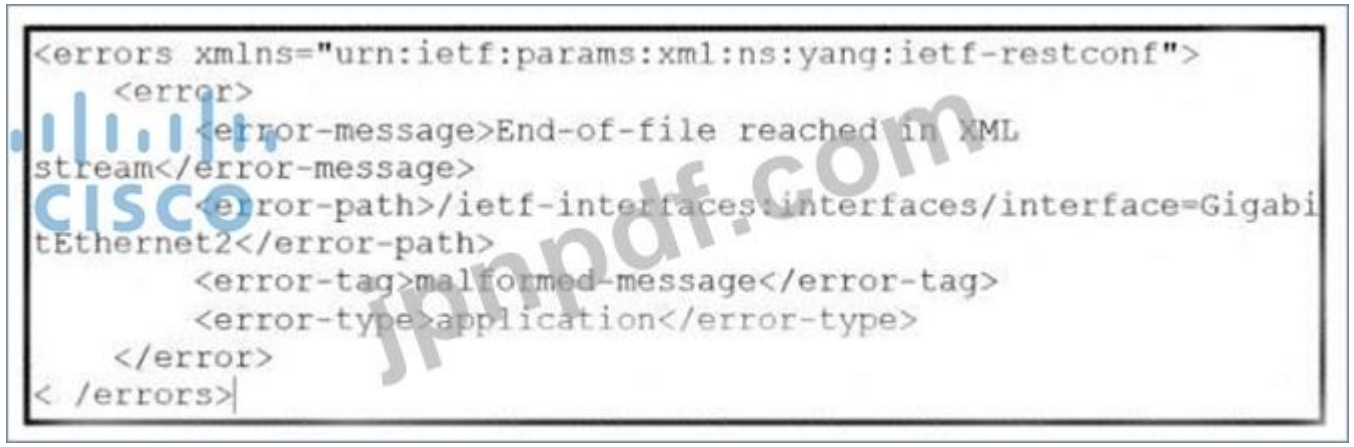
説明
OSPF: セグメント、リンク状態、テーブル
EIGRP: 不等パス、距離ベクトル、メトリック

最新問題**: 253**
クライアント デバイスはエンタープライズ SSID を認識できませんが、他のデバイスはそれに接続されています。この問題の原因は何ですか?

A. クライアントには、構成された非表示の SSID に対して誤った資格情報が保存されています。
B. クライアントには、構成されたブロードキャスト SSID に対して誤った資格情報が保存されています。
C. クライアントでブロードキャスト SSID が手動で構成されていません。
D. 非表示の SSID がクライアントで手動で構成されていません。
Answer: D (メーッセージを残す**)**

最新問題: **254**
Cisco DNA Center で設計ワークフローが使用されるのはいつですか?
A. 既存のインフラストラクチャを持たないグリーンフィールド展開
B. グリーンフィールドまたはブラウンフィールドの展開で、既存のデータを一掃する
C. ブラウンフィールド展開で、ネットワーク内の既存のデバイスの構成を変更するため
D. ブラウンフィールド展開で、新しいネットワーク デバイスをプロビジョニングしてオンボードするため
Answer: A (メーッセージを残す)
設計領域では、ネットワーク全体のデバイスに適用できる物理トポロジ、ネットワーク設定、デバイス タイプ プロファイルなど、ネットワークの構造とフレームワークを作成します。既存のインフラストラクチャがまだない場合は、設計ワークフローを使用します。既存のインフラストラクチャがある場合は、検出機能を使用します。
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/b_cisco_dna_center_ug_2_1_1_chapter_0110. html
参照: https://synoptek.com/insights/it-blogs/greenfield-vs-brownfield-software-development/ グリーンフィールド開発とは、まったく新しい環境向けのシステムを開発することを指し、白紙の状態から開発する必要があります。レガシー コードは必要ありません。これは、制限や依存関係がなく、新たに始めるときに使用されるアプローチです。」

最新問題: **255**



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。要求を送信した後、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ますか?
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: A (メーッセージを残す)
説明
Accept と Content-type はどちらも、クライアント (ブラウザー) からサービスに送信されるヘッダーです。Accept ヘッダーは、クライアントが期待する応答コンテンツのメディア タイプを指定する方法であり、Content-type は、クライアントからサーバーに送信される要求のメディア タイプを指定する方法です。
応答は XML で送信されたため、送信された Accept ヘッダーは application/xml であると言えます。

最新問題: **256**

ルーターが 100 kbps を受け入れる SSH の量を制限する構成はどれですか?

A)

B)

ハ）

D)

A. オプション C

B. オプション A

C. オプション B

D. オプション D

Answer: A (メーッセージを残す**)**

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**36130%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **257**
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?
A)

```
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
```

B)

```
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
```

ハ)

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

D)

E)

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

最新問題**: 258**
Cisco SDWAN 導入における vBond の機能は何ですか?
A. SD-WAN ルーターからのテレメトリ データの収集
B. SD-WAN オーバーレイへの SDWAN ルーターのオンボーディング
C. SD-WAN ルーターとの接続を自動的に開始する
D. SD-WAN ルーターへの構成のプッシュ
Answer: C (メーッセージを残す**)**

最新問題**: 259**
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 エンジニアが 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るでしょうか?

A. ギガビット Ethernet0/0 および GigabitEthemet0/1

B. GigabitEthemet0/1およびGigabitEthernet0/1.40

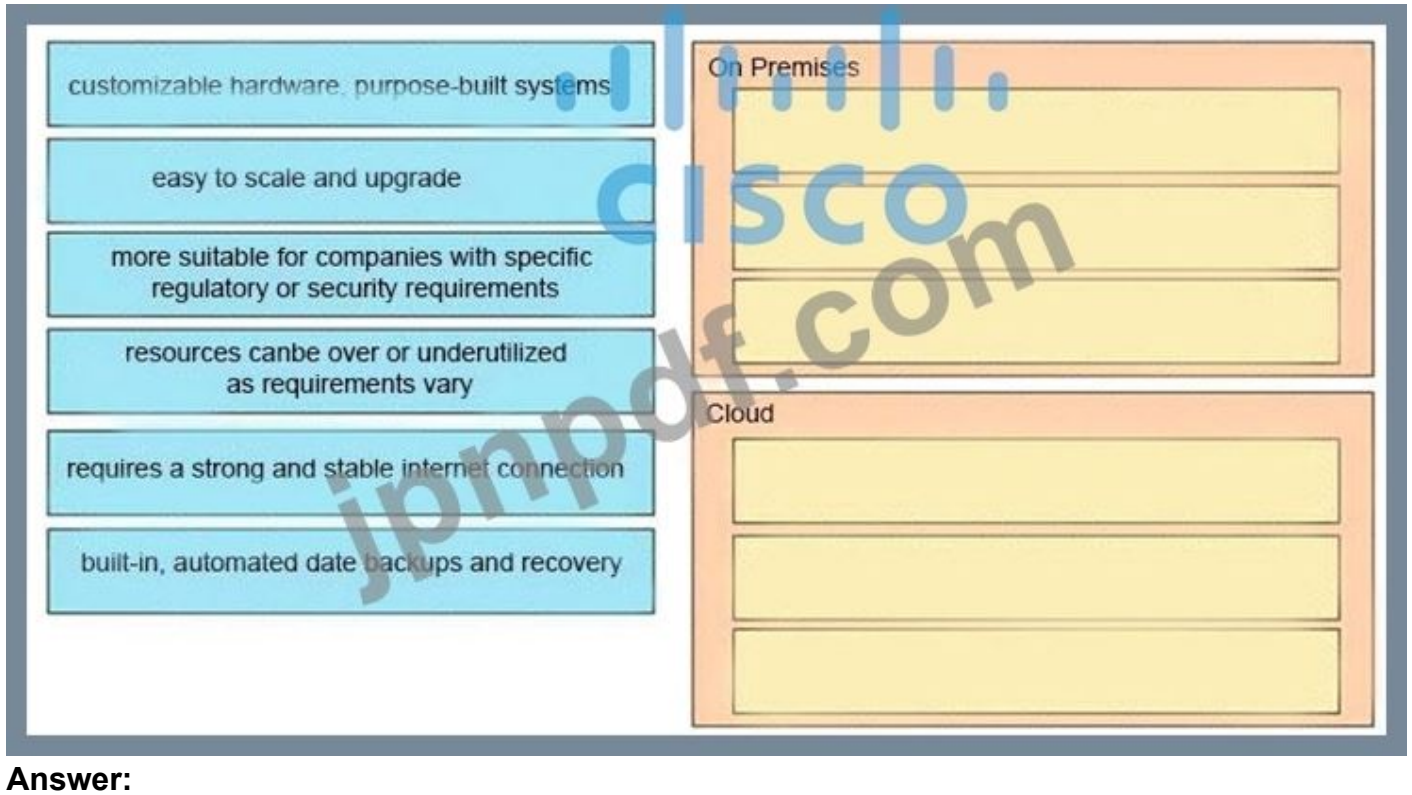
C. GigabttEthernet0/0 のみ

D. GigabitEthernet0/1のみ

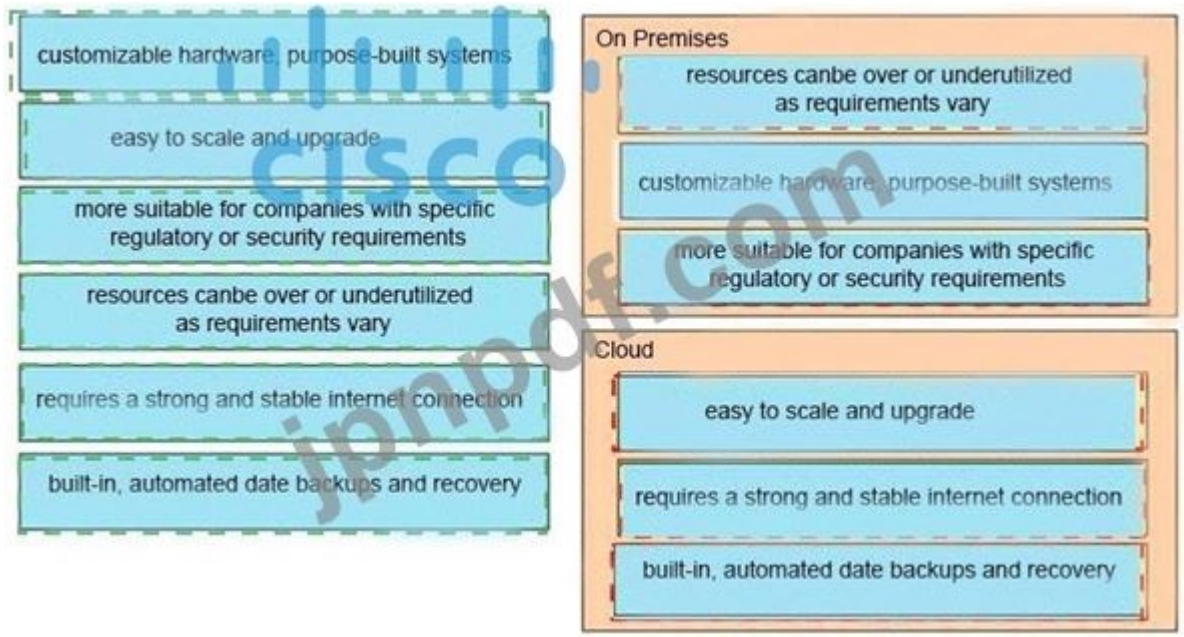
Answer: (解答を表示する**)**

最新問題**: 260**

特性を左側から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:

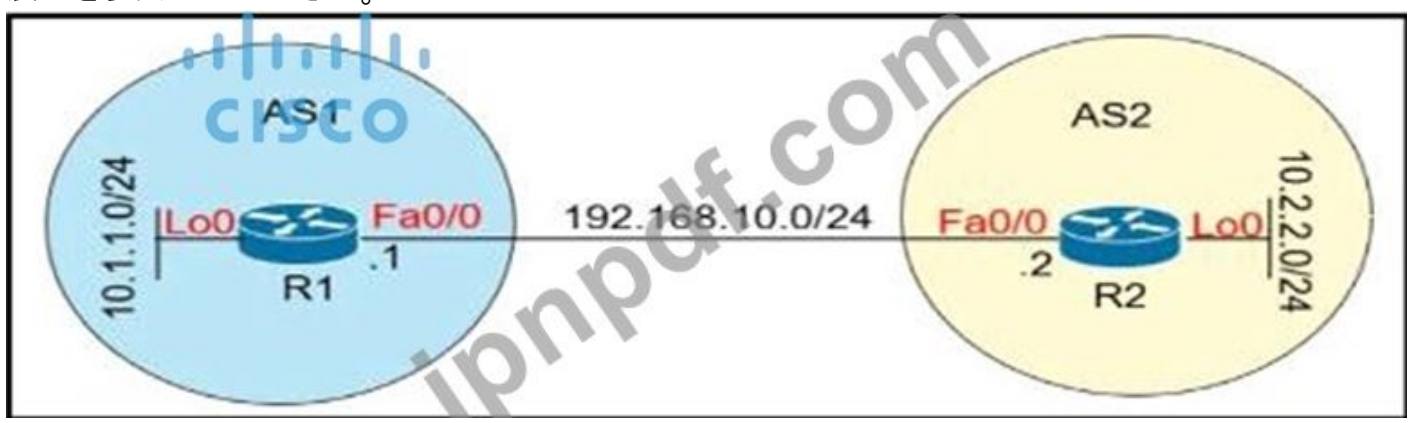


説明

オンプレミス:+ 要件が異なると、リソースが過剰に使用されたり、十分に活用されなかったりする可能性があります+ カスタマイズ可能なハードウェア、専用システム+ 特定の規制またはセキュリティ要件を持つ企業により適していますクラウド:+ 拡張とアップグレードが容易です+ 強力で安定したインターネット接続が必要です+ 組み込みの自動化されたデータバックアップとリカバリ 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**: 261**

展示を参照してください。



これら 2 つの直接接続されたネイバー間に EBGP ネイバーシップを確立し、BGP を介して 2 つのルーターのループバック 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
```

ハ)

```
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、「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 のネットワーク 10.1.1.0/24 と R2 のネットワーク 10.2.2.0/24)。BGP は非常に厳格です。
ルーティング広告。つまり、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れると、または
「network x.0.0.0 mask 255.0.0.0」または「network xxxx mask 255.255.255.255」の場合、BGP は
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、いつ何が必要か見てみましょう
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つ必要です
コマンド:
+ R1 のコマンド「neighbor 10.1.1.1 ebgp-multihop 2」と「neighbor 10.2.2.2 ebgpmultihop
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。
+ Answer '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 (構成) #router bgp 2
R2 (config-router) #neighbor 192.168.10.1 remote-as 1
R2 (config-router) #network 10.2.2.0 マスク 255.255.255.0
クイック ワイヤレス サマリー
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。
+ 自律的: 自給自足でスタンドアロン。小規模なワイヤレス ネットワークに使用されます。
+ Lightweight: Cisco Lightweight AP (LAP) が機能するには、ワイヤレス LAN コントローラ (WLC) に参加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
次の違いを除く LWAPP:
+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
+ 以前はハイブリッド リモート エッジ AP (H-REAP) と呼ばれていた FlexConnect モード: データ トラフィックを許可
ローカルで切り替えられ、コントローラには戻りません。FlexConnect AP はスタンドアロンで実行できます
WLC に接続されていない場合でも、クライアント認証とローカルでの VLAN トラフィックの切り替え (ローカル
切り替えました)。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 (CAPWAP 経由で) トンネリングすることもできます。
集中型 WLC (Central Switched)。
+ 監視モード: クライアントとインフラストラクチャ間のデータ トラフィックを処理しません。それはのように機能します
ロケーションベース サービス (LBS)、不正 AP 検出、および IDS 用のセンサー
+ Rogue Detector モード: 不正 AP を監視します。データをまったく処理しません。
+ スニファ モード: スニファとして実行し、特定のチャネル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) を使用してデータを確認できるリモート マシン
パケットと診断の問題。トラブルシューティングの目的で厳密に使用されます。
+ ブリッジ モード: WLAN と有線インフラストラクチャを一緒にブリッジします。
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、小規模から中規模の、またはマルチサイト ブランチの場所にのみ適しています。
専用の WLC に投資したくない場合があります。Mobility Express WLC は最大 100 個の AP をサポートできます

最新問題: **262**
展示を参照してください。

Edge-01 は現在、プライオリティ 110 の HSRP プライマリとして動作しています。Edge-01 がダウンしている場合、Edge-02 で転送の役割を引き継ぐコマンドはどれですか?

A. スタンバイ 10 タイマー
B. スタンバイ 10 トラック
C. スタンバイ 10 プリエンプト
D. スタンバイ10優先
Answer: D (メーッセージを残す)

最新問題**: 263**
ネットワーク エンジニアは、R1 と R2 の間で BGP を構成します。どちらのルーターも BGP ピア グループ CORP を使用し、MD5 認証を使用するように設定されています。このメッセージは、ルーター R1 のコンソールに記録されます。

```
*May 5 39:85:86.070: %TCP-6-BADAUTH" Invalid MD5 digest from 10.10.10.1 (29832) to 10.120.10.1 (179) tebleid -0
```

Which two configurations allow a peering session to form between R1 and R2? (Choose two.)
R1 と R2 の間からのピアリング セッションを許可する 2 つの構成はどれですか? 2 つ選んでください。) A)

```
R2(config-router)#neighbor 10.10.10.1 peer-group CORP
R2(config-router)#neighbor PEER password Cisco
```

B)

```
R2(config-router)#neighbor 10.10.10.1 peer-group CORP
R2(config-router)#neighbor CORP password Cisco
```

ハ)

```
R1(config-router)#neighbor 10.10.10.1 peer-group CORP
R1(config-router)#neighbor CORP password Cisco
```

D)

```
R1(config-router)#neighbor 10.120.10.1 peer-group CORP
R1(config-router)#neighbor CORP password Cisco
```

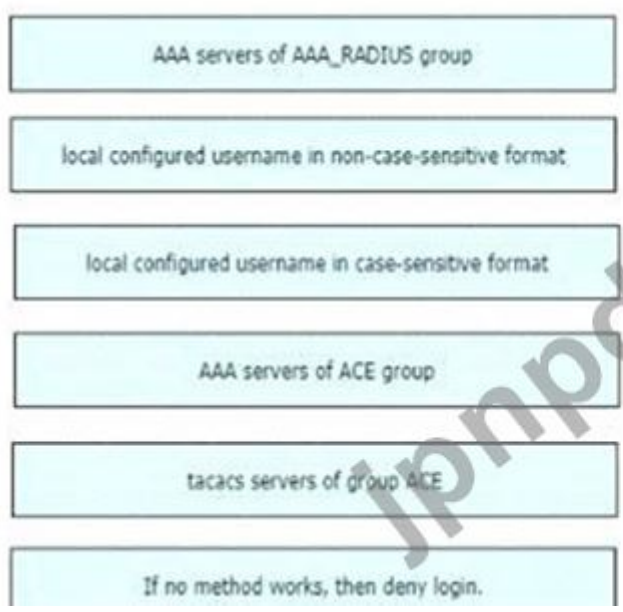
E)

```
R2(config-router)#neighbor 10.120.10.1 peer-group CORP
R2(config-router)#neighbor CORP password Cisco
```

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
E. オプション E
Answer: D,E (メーッセージを残す)

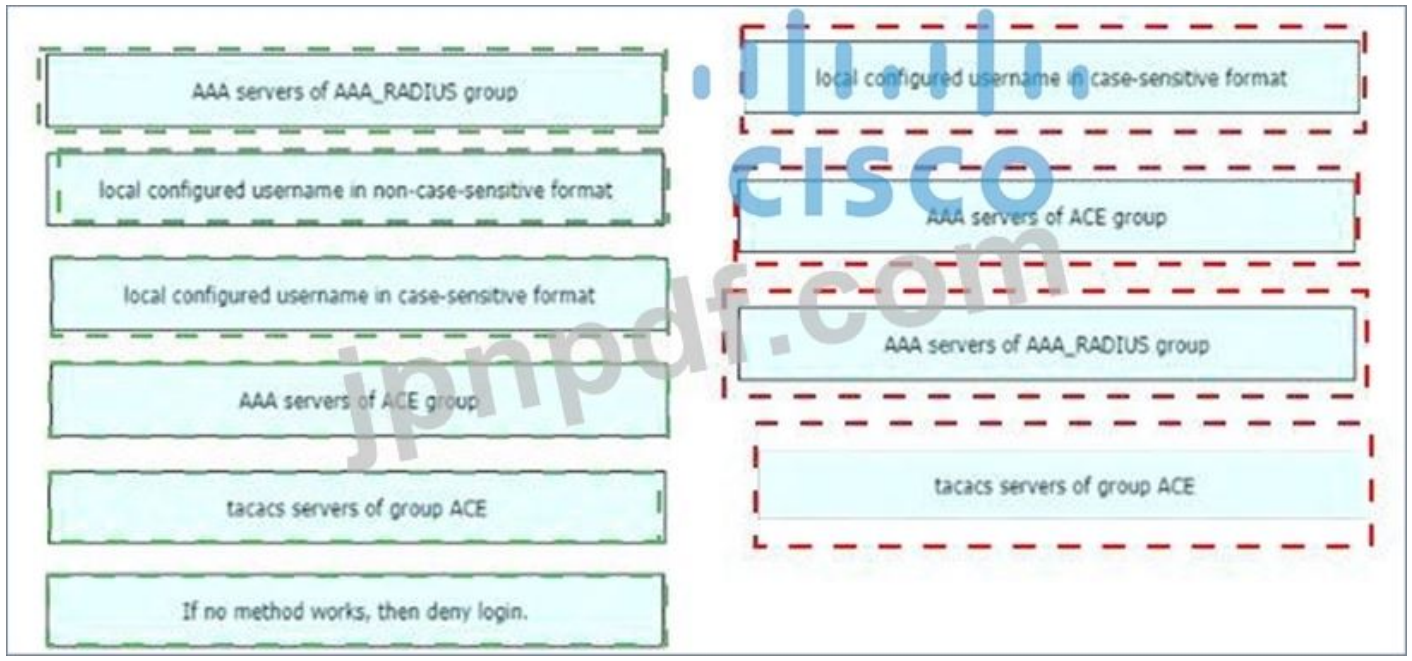
最新問題**: 264**
エンジニアが以下の構成を作成します。認証方法を左から右の優先順にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。

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

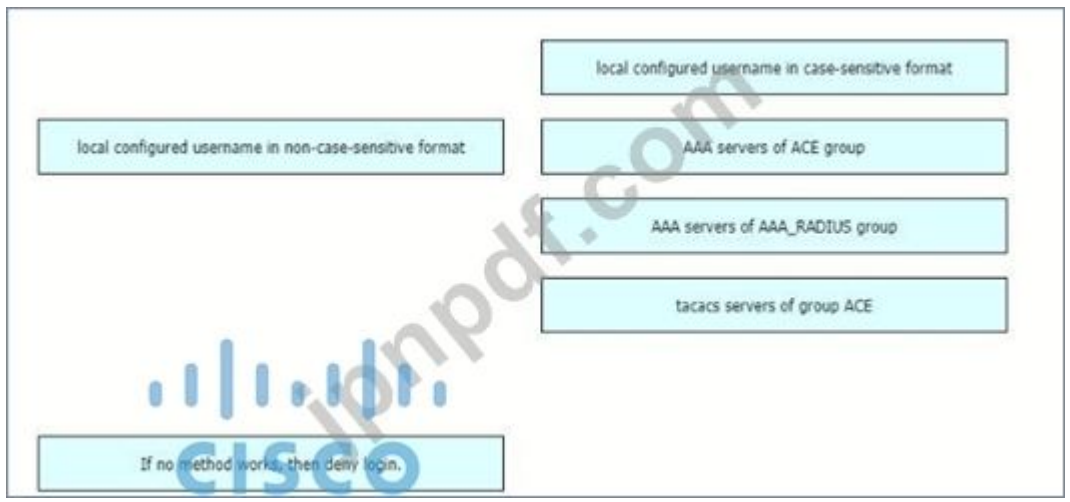


jpnpdf.com

Answer:

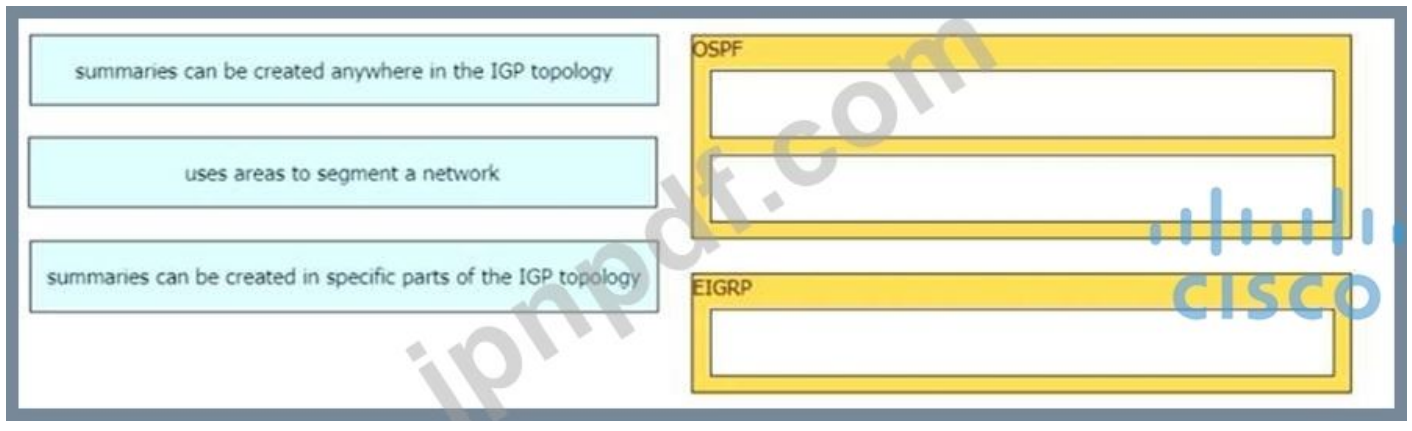


説明

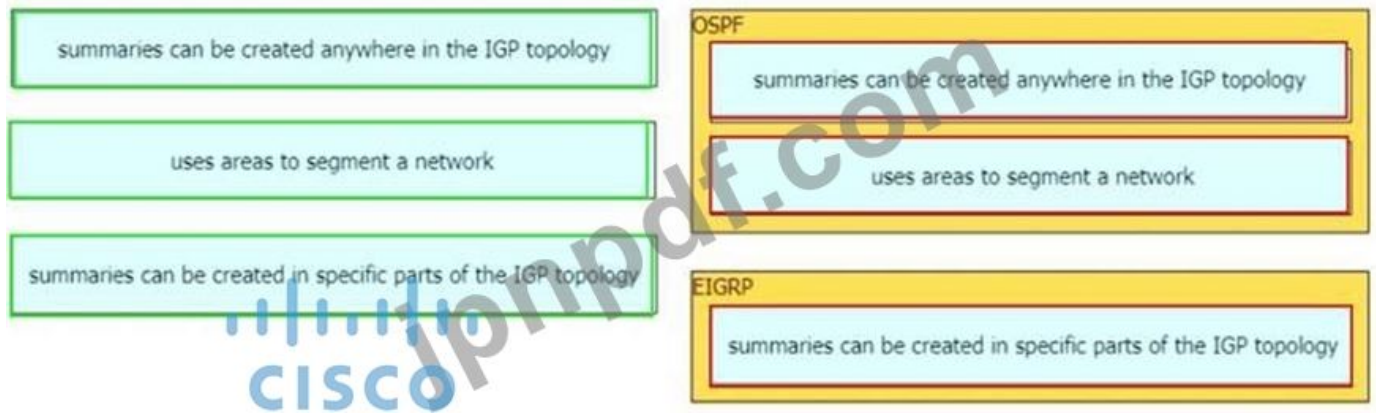


最新問題**: 265**

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**: 266**

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. Make":'Gocar, "Model': "Zoom", "Features": ["Power Windows", "Manual Dnve", "Auto AC"]}

B. 'Make ": "Gocar1, "Model": "Zoom", "Features": ["Power Windows", "Manual Drive", "Auto AC"]

C. {"メーカー": Gocar、"モデル": Zoom、"機能": パワー ウィンドウ、マニュアル ドライブ、オート AC}

D. ("メーカー":["Gocar", "型式": "Zoom"], 機能": ["パワーウィンドウ", "手動駆動", "オートエアコン"]}

Answer: A (メーッセージを残す**)**

説明

JSON 構文構造: + 中かっこ {} を使用してオブジェクトを保持し、角かっこ [] を使用して配列を保持 + JSON データはキー/値のペアとして記述されます + キー/値のペアはキーで構成されます (二重引用符で囲まれた文字列である必要があります) "") の後にコロン : が続き、その後に値が続きます。例: "name":"John" + 各キーは一意である必要があります + 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 + オブジェクト内の複数のキー/値はカンマで区切ります。JSON では配列を使用できます. 配列は、1 つの変数に複数の値を格納するために使用されます。例えば :

{

"名前":"ジョン",

"年齢":30,

"cars":["フォード"、"BMW"、"フィアット"]

}

上記の例では、 Cars」は Ford」、 BMW」、 Fiat」の 3 つの値を含む配列です。

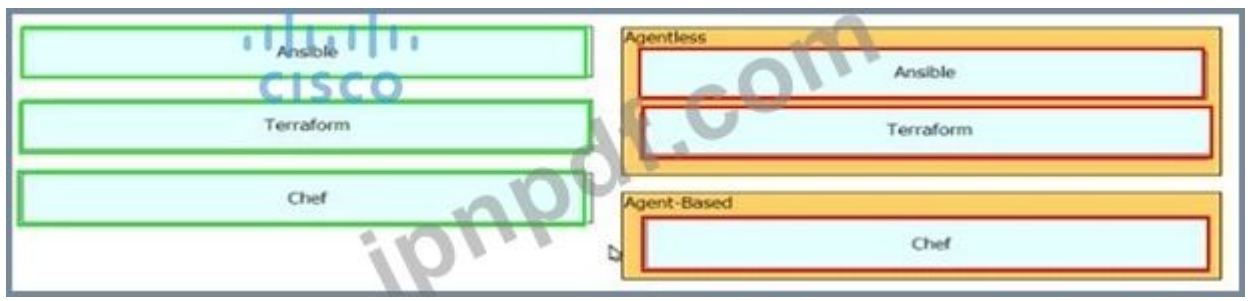
注: 上記の正解には、オブジェクトを保持するための中括弧がありませんが、それでもここでは最良の選択です。

Results

Valid JSON

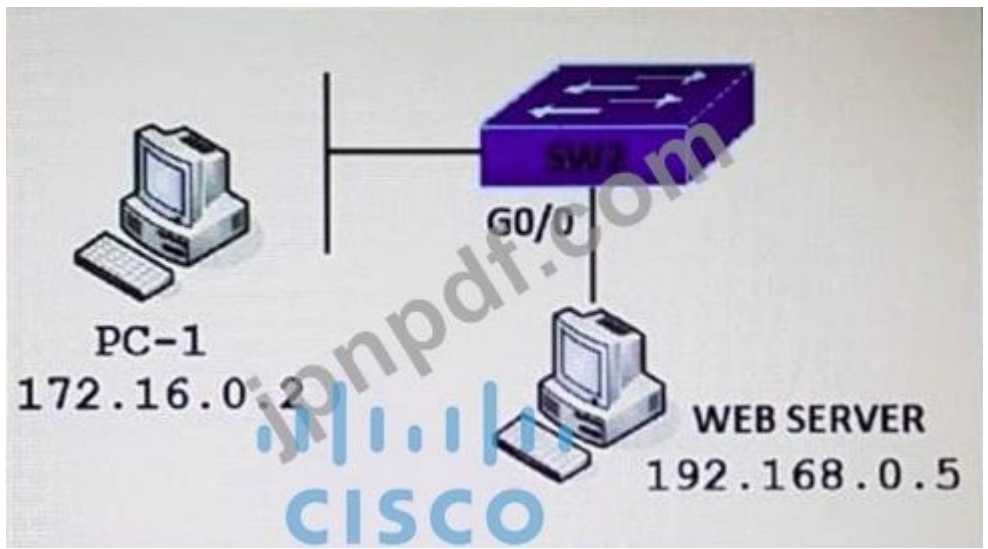
最新問題: **267**
左側のツールを右側のエージェント タイプにドラッグ アンド ドロップします。

Answer:



最新問題: **268**
ファブリック アクセス ポイントはネットワークにどのように適合しますか?
A. ローカル モードであり、ファブリック ボーダー ノードに直接接続する必要があります。
B. FlexConnect モードであり、ファブリック ボーダー ノードに直接接続する必要があります。
C. ローカル モードであり、ファブリック エッジ スイッチに直接接続する必要があります。
D. FlexConnect モードであり、ファブリック エッジ スイッチに直接接続する必要があります。
Answer: (解答を表示する**)**
ファブリック モード AP は、従来の AP がサポートするのと同じワイヤレス メディア サービスを引き続きサポートします。AVC、サービス品質 (QoS)、およびその他のワイヤレス ポリシーを適用します。CAPWAP コントロール プレーンをファブリック WLC に確立します。ファブリック AP はローカル モード AP として参加し、ファブリック エッジ ノード スイッチに直接接続して、ファブリック WLC を介した RLOC 割り当てなどのファブリック登録イベントを有効にする必要があります。ファブリック エッジ ノードは、CDP を使用して AP を特別な有線ホストとして認識し、特別なポート構成を適用して、ファブリック全体の共通 EID スペース内の一意のオーバーレイ ネットワークに AP を割り当てます。この割り当てにより、単一のサブネットを使用してファブリック サイトの AP インフラストラクチャをカバーすることで、管理を簡素化できます。

最新問題: **269**
展示を参照してください。



展示を参照してください。PC-1 はポート 8080 で Web サーバーにアクセスする必要があります。このトラフィックを許可するには、インバウンド方向の SW2 ポート G0/0 に適用されるアクセス制御リストに追加する必要があるステートメントはどれですか?

A. ホスト 192.168.0.5 を許可 8080 ホスト 172.16.0.2

B. ホスト 192.168.0.5 ホスト 172.16.0.2 eq 8080 を許可

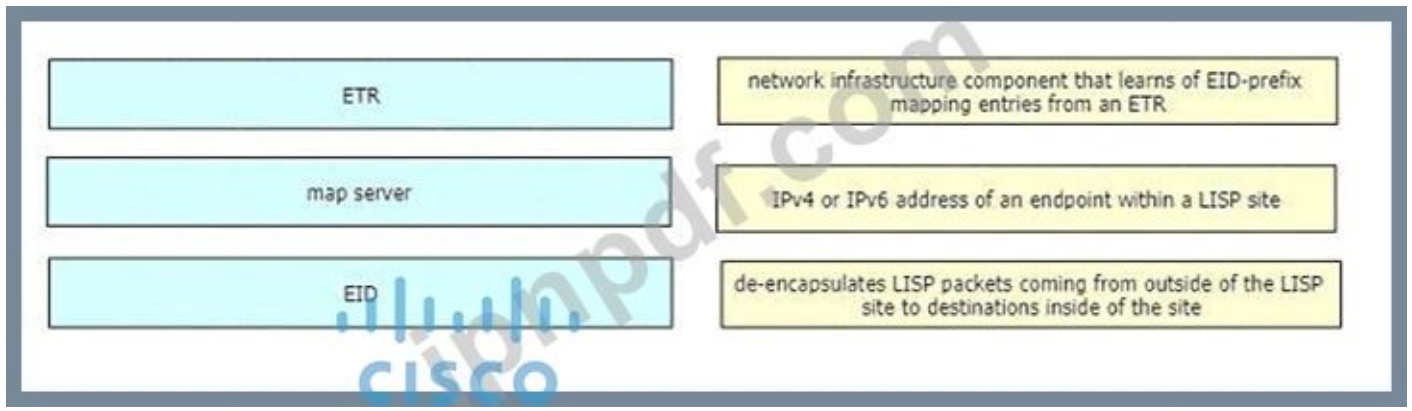
C. ホスト 172.16.0.2 ホスト 192.168.0.5 eq 8080 を許可

D. ホスト 192.168.0.5 eq 8080 ホスト 172.16.0.2 を許可

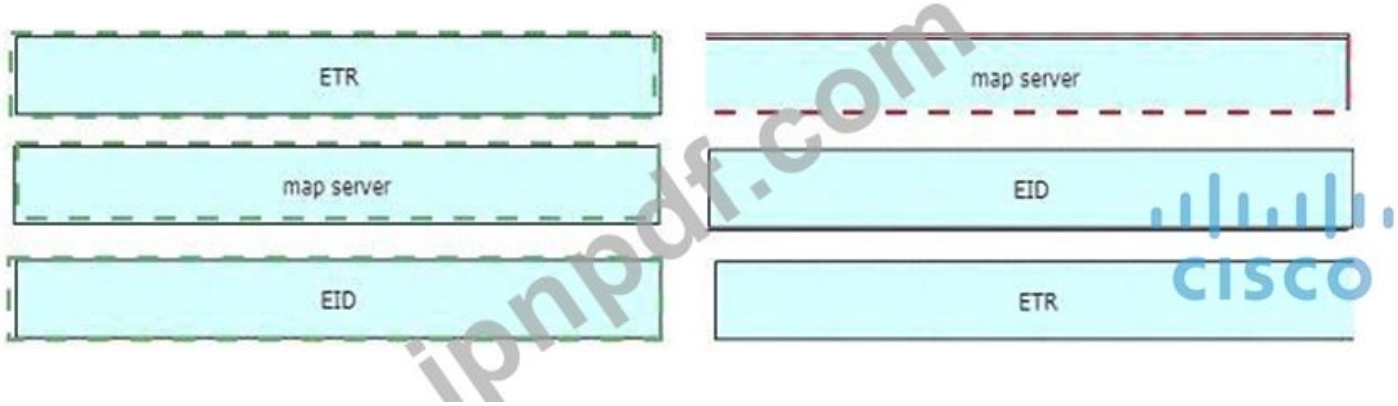
Answer: D (メーッセージを残す)

最新問題: **270**

左側の LISP コンポーネント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

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irloverview.h

最新問題**: 271**

展示を参照してください。Cisco DNA Center からのネットワーク デバイスのリストを表示する Python スクリプトが機能するコードはどれですか?

```
login = dnac_login(dnac["host"], dnac["username"], dnac["password"])

network_device_list(dnac, login)
for item in dnac_devices:
   print(dnac_devices.item)
```

```
login = dnac_login(dnac["host"], dnac["username"], dnac["password"])
network_device_list(dnac, login)
print(dnac_devices)
```

```
network_device_list(dnac["host"], dnac["username"],dnac["password"])
login = dnac_login(dnac)
print(dnac_devices)
```

```
network_device_list(dnac["host"], dnac["username"],dnac["password"])
login = dnac_login(dnac)
for item in dnac_devices:
   print(dnac_devices.item)
```

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**)**

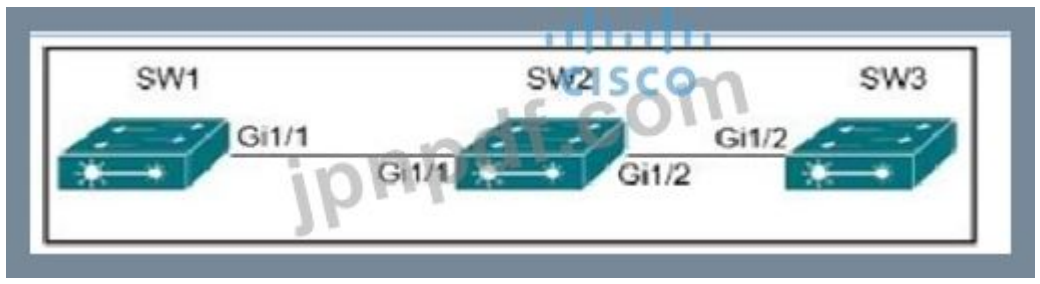
有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 272**

ログイン方法は、これらのパラメータを使用してルータの VTY 回線で設定されます。
* 最初の認証方法は TACACS です
* TACACS が利用できない場合、提供された資格情報なしでログインが許可されます。このタスクを実行する構成はどれですか?
A. R1#sh 実行 | aaaを含む
aaa ニューモデル
aaa 認証 ログイン VTY グループ tacacs+ なし
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
パスワード 7 0202039485748
R1#sh 実行 | ユーザー名を含める
R1#
B. R1#sh 実行 | aaaを含む
aaa ニューモデル
aaa authentication login telnet group tacacs+ none
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
R1#sh 実行 | ユーザー名を含める
R1#
C. R1#sh 実行 | aaaを含む
aaa ニューモデル
AAA 認証ログイン デフォルト グループ tacacs+ なし
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
パスワード 7 0202039485748
D. R1#sh 実行 | aaaを含む
aaa ニューモデル
AAA 認証ログイン デフォルト グループ tacacs+
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
トランスポート入力なし
R1#
Answer: (解答を表示する**)**
説明
要件 (最初に TACACS+ を使用し、次に認証なしでログインを許可する) に従って、AAA コマンドに「aaa authentication login ...」を使用する必要があります。

次に確認することは、「aaa authentication login」または「aaa authentication login list-name」が使用されているかどうかです。「default」キーワードは、すべてのログイン接続 (tty、vty、console、aux など) に適用することを意味します。このキーワードを使用する場合、tty、vty、および aux ラインの下で他に何も構成する必要はありません。このキーワードを使用しない場合は、認証機能を適用する行を指定する必要があります。
上記の情報から、答え 'R1#sh run | ' を見つけることができます。include aaa aaa new-model aaa authentication login default group tacacs+ none aaa session-id common R1#sh run | section vty line vty 0 4 password 7 0202039485748 AAA 設定の詳細については、AAA TACACS+ および RADIUS チュートリアル - パート 2 をお読みください。
参考までに、「R1#sh run |」と答えてください。aaaを含む
aaa ニューモデル
aaa authentication login telnet group tacacs+ none
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
R1#sh 実行 | ユーザー名を含める
vty 行 (「line vty 0 4」) の下に次のコマンドを追加すると、R1# は正しくなります: 「login authentication telnet」(「telnet」は上記の AAA リストの名前です)

最新問題**: 273**



会社のポリシーにより、VLAN 10 は SW1 と SW2 でのみ許可されるように制限されています。他のすべての VLAN は、3 つのスイッチすべてに配置できます。管理者は、VLAN 10 が SW3 に伝播したことに気付きました。問題を修正する構成はどれですか?
A)

```
SW1(config)#int gi1/1
SW1(config)#switchport trunk allowed vlan 1-9,11-4094
```

B)

```
SW2(config)#int gi1/2
SW2(config)#switchport trunk allowed vlan 10
```

ハ)

```
SW2(config)#int gi1/2
SW2(config)#switchport trunk allowed vlan 1-9,11-4094
```

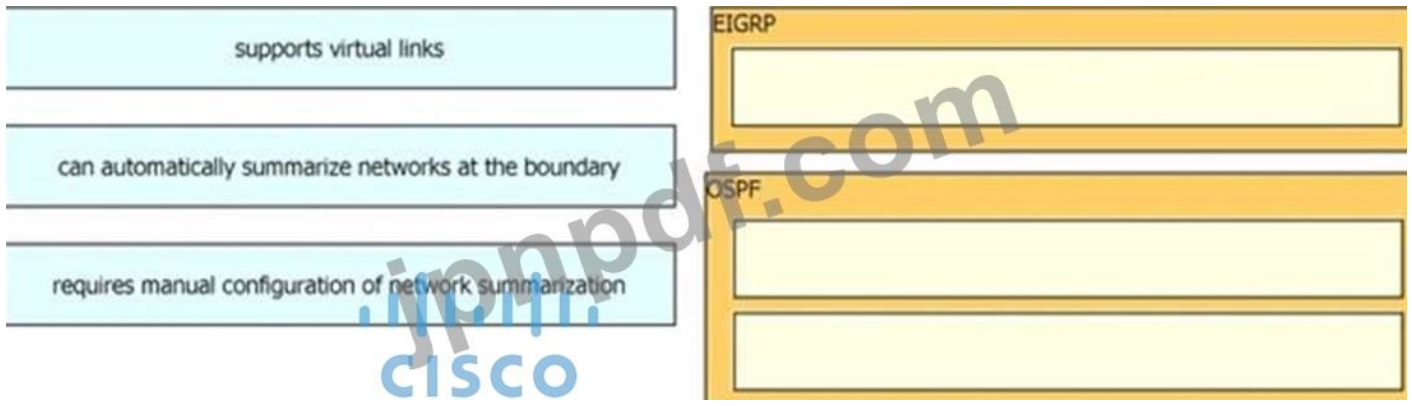
D)

```
SW1(config)#int gi1/1
SW1(config)#switchport trunk allowed vlan 10
```

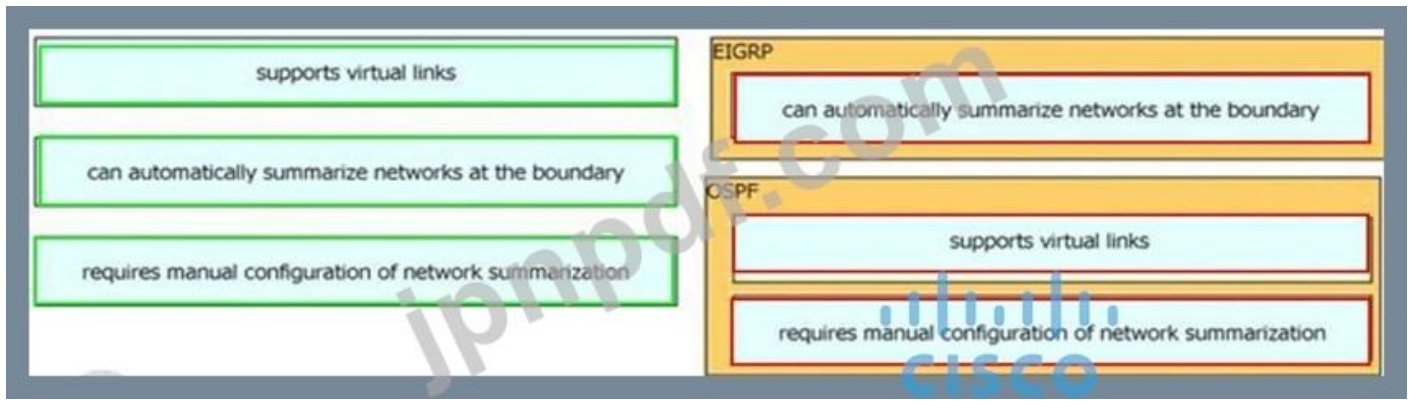
A. オプション C

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

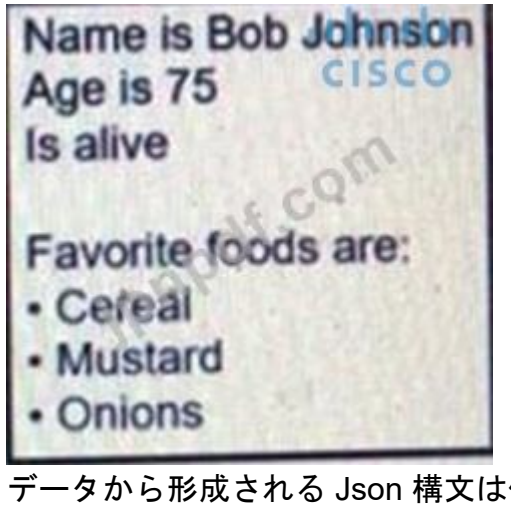
最新問題**: 274**
左側の特性を、右側に記述されているルーティング プロトコルにドラッグ アンド ドロップします。



Answer:



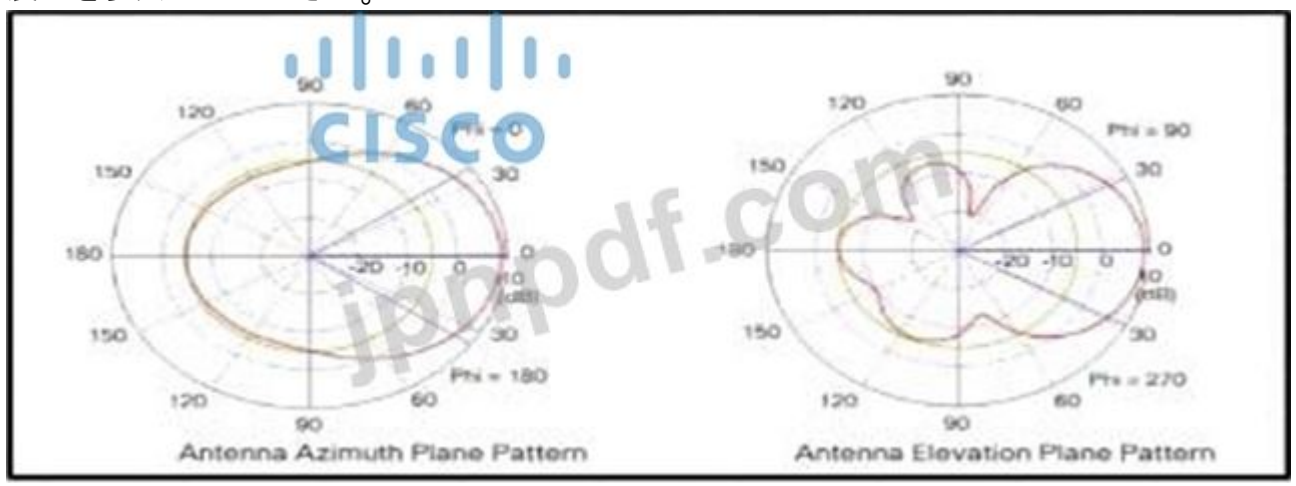
最新問題**: 275**
展示を参照してください。



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、タマネギ]}
B. 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 オニオン

C. 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]}
D. 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、タマネギ]}
Answer: (解答を表示する**)**

最新問題**: 276**
展示を参照してください。



放射パターンはどのタイプのアンテナを示していますか?
A. 双極子
B. 無指向性
C. パッチ
D. 八木
Answer: C (メーッセージを残す**)**

最新問題**: 277**
展示を参照してください。

放射パターンに示されているアンテナのタイプはどれですか?

A. 双極子

B. 八木

C. パッチ

D. 無指向性

Answer: A (メーッセージを残す)

説明

ダイポール アンテナは、最も一般的には半波長 (/2) ダイポールを指します。物理的なアンテナ (アンテナが入っているパッケージではありません) は、意図した動作周波数で長さを合わせた長さが波長の約半分になる導電性要素で構成されています。これは、エネルギーを地平線に向かって (アンテナに対して垂直に) 放射する単純なアンテナです。示されているパターンは、z 軸に沿って垂直に配向された 2 つの細いワイヤで形成された完全な双極子から生じるものです。

参照：
https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900a

最新問題**: 278**

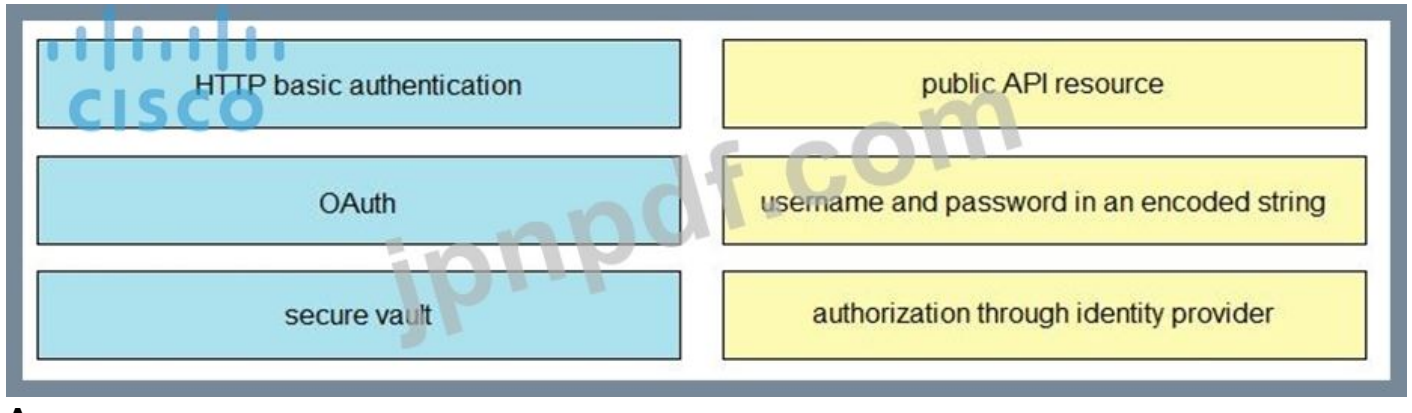
展示を参照してください。

ネットワーク管理者は、すべての RADIUS サーバーに到達できない場合に構成の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に、すべてのコマンドを許可できる構成はどれですか?

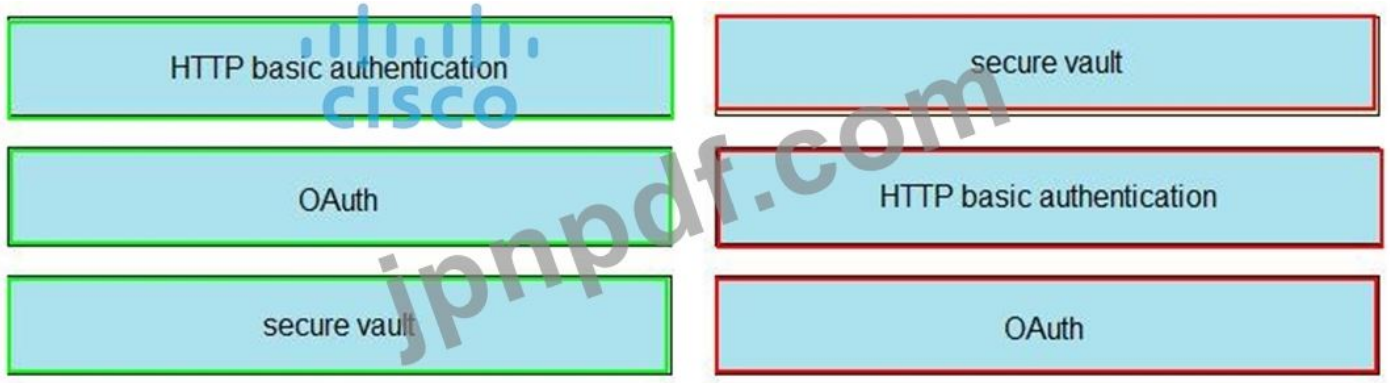
A. aaa 承認 exec デフォルト グループ 半径 なし
B. aaa 認可 exec デフォルト グループ 半径
C. aaa 承認 exec デフォルト グループ 半径 if-authenticated
D. aaa 認証ログイン デフォルト グループ 半径 ローカル なし
Answer: C (メーッセージを残す)

最新問題: **279**
Cisco Trustsec は、どのようにしてダイナミック ネットワーキング環境やデータ センターのアクセス制御を強化しますか?
A. 高度なアプリケーション認識に基づいてトラフィックを分類します
B. Flexible NetFlow を使用
C. 正しい IP アドレスではなく、エンドポイントのコンテキスト ID に基づいてトラフィックを分類します。
D. エンドポイントに VLAN を割り当てます
Answer: C (メーッセージを残す)
Cisco TrustSec ソリューションは、ソフトウェア定義のセグメンテーションを使用してネットワーク トラフィックを分類し、より柔軟なアクセス コントロールのポリシーを適用することで、ネットワーク アクセス コントロールのプロビジョニングと管理を簡素化します。トラフィックの分類は、IP アドレスではなくエンドポイントの ID に基づいているため、ネットワークを再設計することなくポリシーを変更できます。
参照：
DC_Access_Control_Using_TrustSec_Deployment_April2016.pd

最新問題: **280**
REST API 認証方法を左側から右側の説明にドラッグ アンド ドロップします。



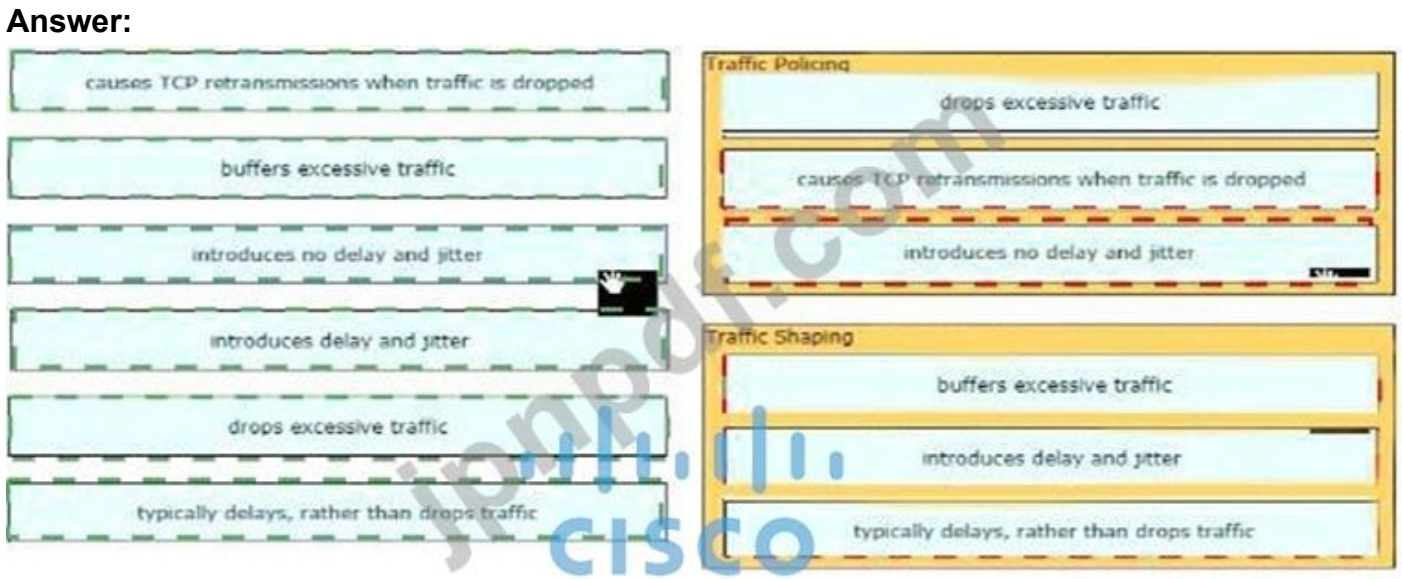
Answer:



最新問題: **281**

左側の説明を右側の正しい QoS コンポーネントにドラッグ アンド ドロップします。

Answer:



説明

トラフィック ポリシング: 過剰なトラフィックをドロップし、TCP 再送信を引き起こし、遅延/ジッターを導入しません

最新問題: **282**

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説明はどれですか?

A. 出力には、ルーター R1 がインターフェイス 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、ルーター R1 がすべてのインターフェー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、ルーター R1 が送信した OSPF hello メッセージがインターフェイス Fa0/1 で受信されたことが表示されます。

D. 出力には、ルーター R1 が送受信した OSPF の hello および LSACK メッセージが表示されます。

Answer: C (メーッセージを残す**)**

説明

このコマンドの組み合わせは 条件付きデバッグ」と呼ばれ、条件に基づいてデバッグ出力をフィルタリングします。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: **283**
EEM に登録され、オンデマンドまたは手動で実行される EEM アプレット ポリシーを作成する方法はどれですか?
A. イベント マネージャ アプレット オンデマンド
イベント登録
action 1.0 syslog priority critical msg 「これはオンデマンドからのメッセージです」
B. イベント マネージャ アプレット オンデマンド
イベントマニュアル
action 1.0 syslog priority critical msg 「これはオンデマンドからのメッセージです」
C. イベント マネージャ アプレット オンデマンド
イベントなし
action 1.0 syslog priority critical msg 「これはオンデマンドからのメッセージです」
D. イベント マネージャ アプレット オンデマンド
action 1.0 syslog priority critical msg 「これはオンデマンドからのメッセージです」
Answer: (解答を表示する**)**
EEM ポリシーは、イベントと、そのイベントが発生したとき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、アプレットまたはスクリプトの 2 種類があります。アプレットは、CLI 構成内で定義される単純な形式のポリシーです。answer 'event manager applet ondemand event register action 1.0 syslog priority critical msg 'This is a message from ondemand'
<="" p="" style="box-sizing: border-box;">
EEM ポリシーを手動で実行するには、2 つの方法があります。EEM は通常、ポリシー自体に含まれるイベント仕様に基づいてポリシーをスケジュールし、実行します。event none コマンドを使用すると、EEM は手動でトリガーできる EEM ポリシーを識別できます。ポリシーを実行するには、アプレット コンフィギュレーション モードで action policy コマンドを使用するか、特権 EXEC モードで event manager run コマンドを使用します。
参照：
3s-book/eem-policy-cli.html

最新問題: **284**
Linux を実行するサーバーは、中小企業向けの DNS および DHCP サービスと共に仮想マシンのサポートを提供しています。これはどの技術を表していますか?
A. コンテナー
B. タイプ 1 ハイパーバイザー
C. ハードウェア パススルー
D. タイプ 2 ハイパーバイザー
Answer: D (メーッセージを残す**)**
説明
タイプ 1 ハイパーバイザーとは対照的に、タイプ 2 ハイパーバイザー (またはホスト型ハイパーバイザー) は、物理ハードウェアではなく、オペレーティング システム上で実行されます。タイプ 2 ハイパーバイザーの大きな利点は、管理コンソール ソフトウェアが必要ないことです。タイプ 2 ハイパーバイザーの例としては、VMware Workstation (Windows、Mac、および Linux で実行可能) または Microsoft Virtual PC (Windows でのみ実行) があります。

最新問題: **285**

Cisco DNA Center が SD-Access ファブリック内のデバイスへの接続を失った場合に発生する 2 つの結果はどれですか? (2つ選択)

A. ユーザーが接続を失う

B. 既に接続しているユーザーは影響を受けませんが、新しいユーザーは接続できません

C. ユーザー接続は影響を受けません。

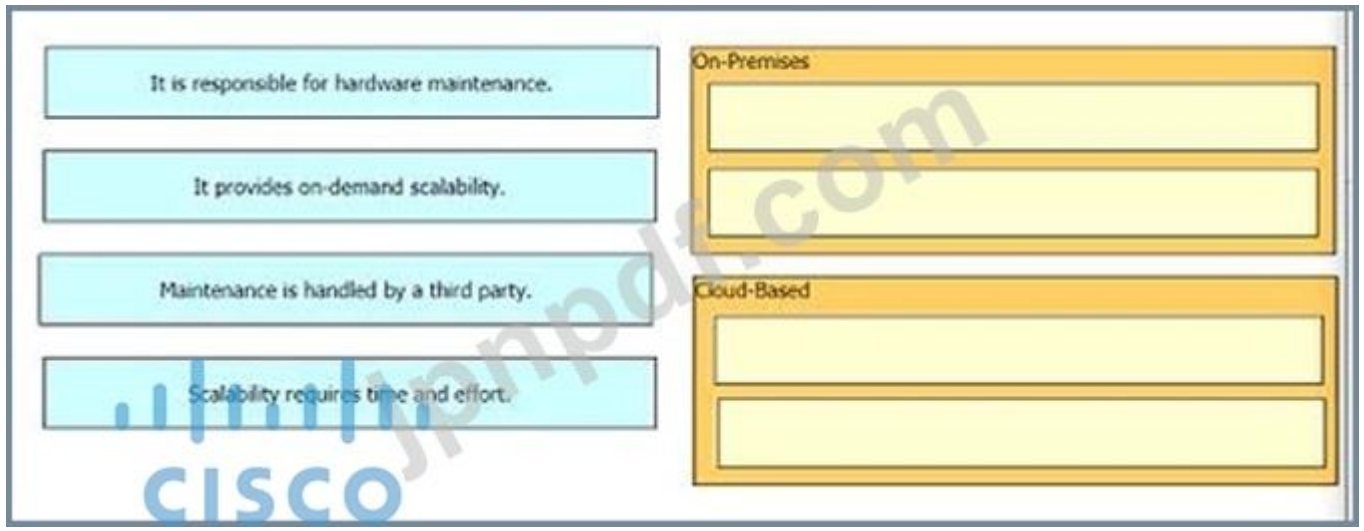
D. Cisco DNA Center への接続が失われたことを検出した後、すべてのデバイスがリロードします

E. Cisco DNA Center は保証でモニタリング データを収集できません。

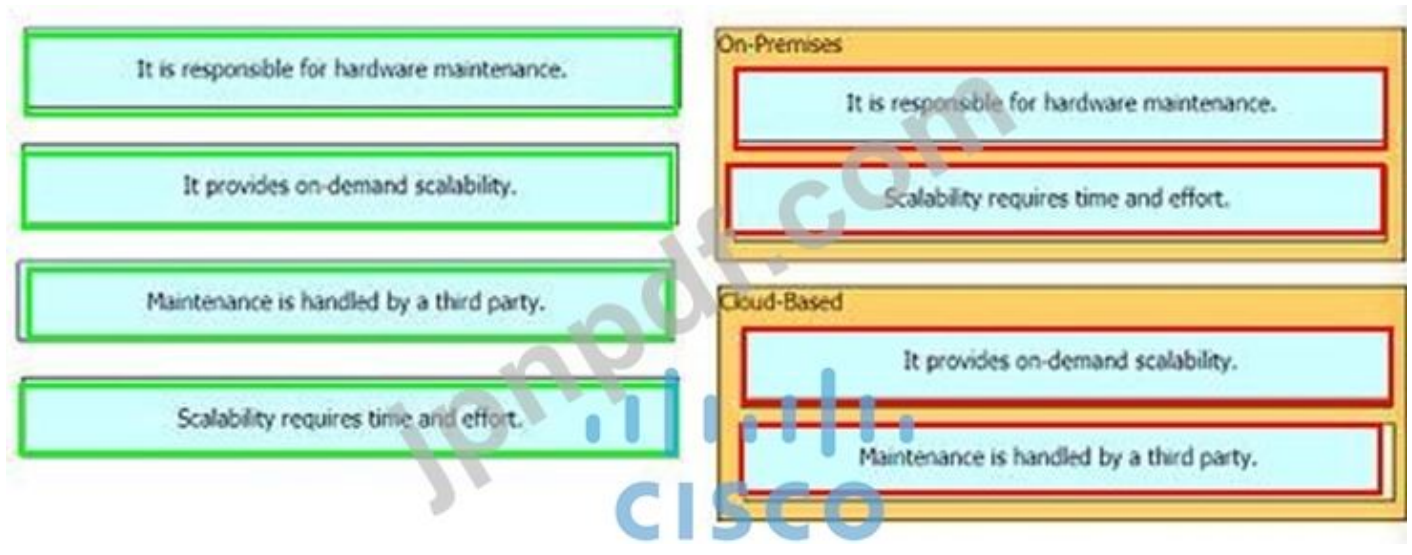
Answer: (解答を表示する**)**

最新問題**: 286**

左側の特性を右側の展開タイプにドラッグ アンド ドロップします。



Answer:

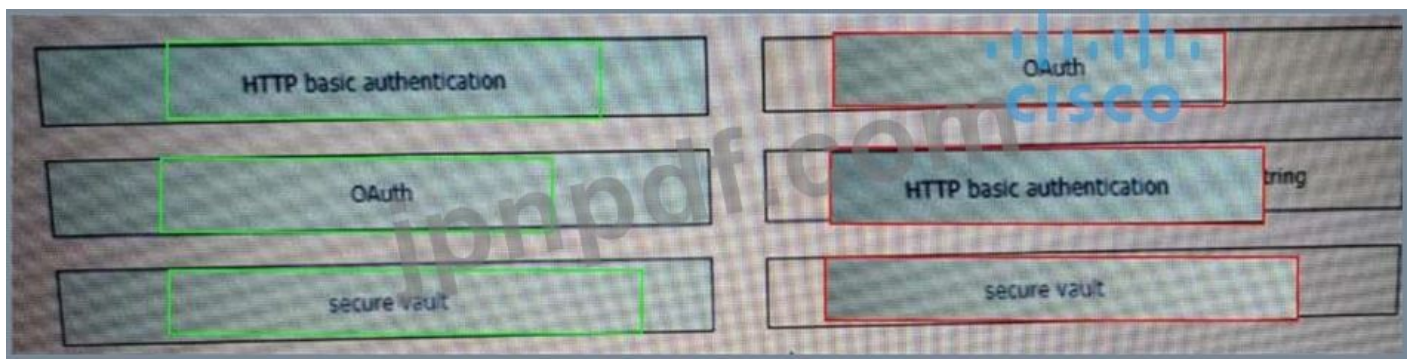


有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **287**
ネットワークは、デュアルスタック アプローチを使用して IPV4 から IPV6 に移行されています。ネットワーク管理では、すでに 100% IPV6 が有効になっています。2 つのデュアルスタック NetFlow コレクションを持つデュアルスタック ネットワークでは、柔軟な NetFlow 構成のネットワーク デバイスごとにいくつのフロー エクスポータが必要ですか?
A. 1
B. 2
C. 4
D. 8
Answer: B (メーッセージを残す**)**

最新問題: **288**
REST API 認証方法を左側から右側の説明にドラッグ アンド ドロップします。

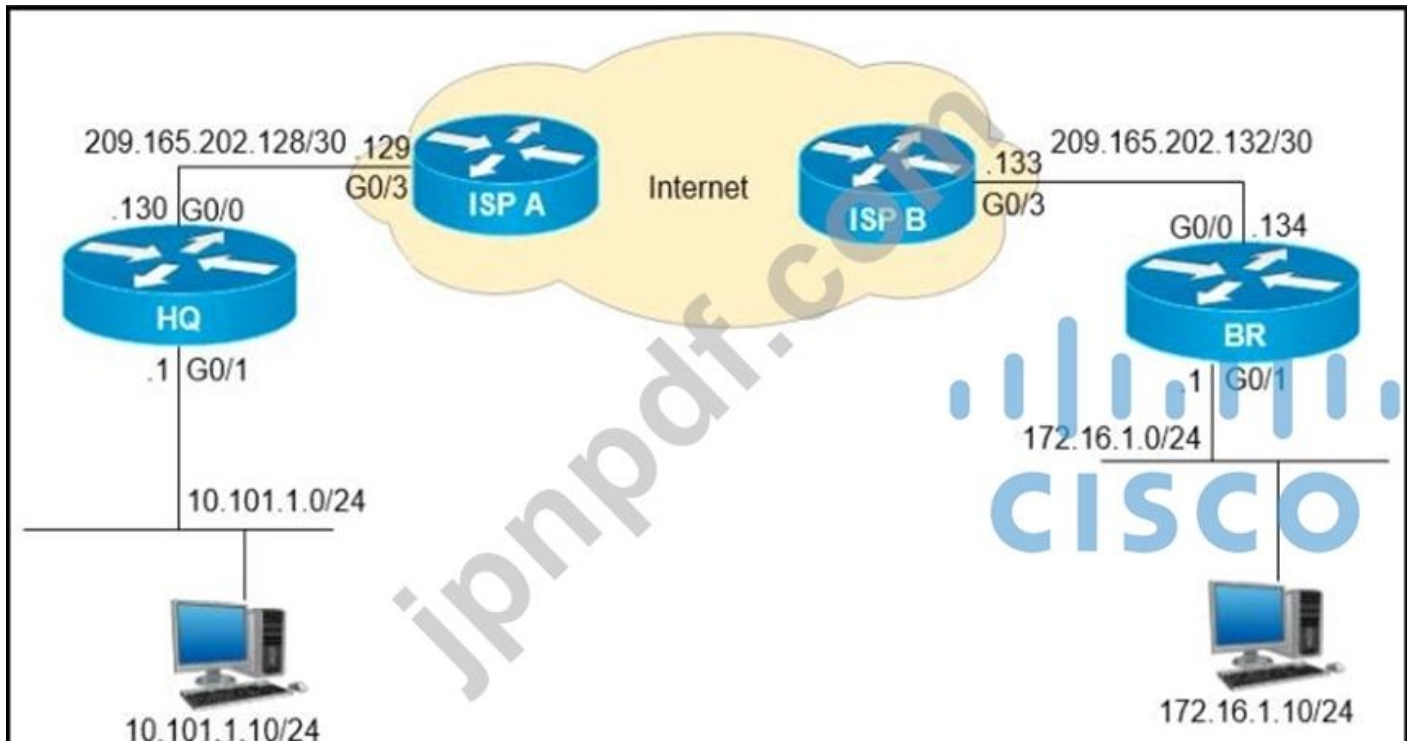
Answer:



最新問題: **289**
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 Stratum レベルですか?
A. ストラタム 0
B. 層 1
C. Stratum 14
D. Stratum 15
Answer: B (メーッセージを残す**)**

参照：
figuration/guide/bsm/16-6-1/b-bsm-xe-16-6-1-asr920/bsm-timecalendar-set.html

最新問題: **290**
展示を参照してください。



HQ ルーターと BR ルーターの間に GRE トンネルを設定するには、HQ ルーターにどの構成を適用する必要がありますか?

```
interface Tunnel1
 ip address 209.165.202.130 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.133
```

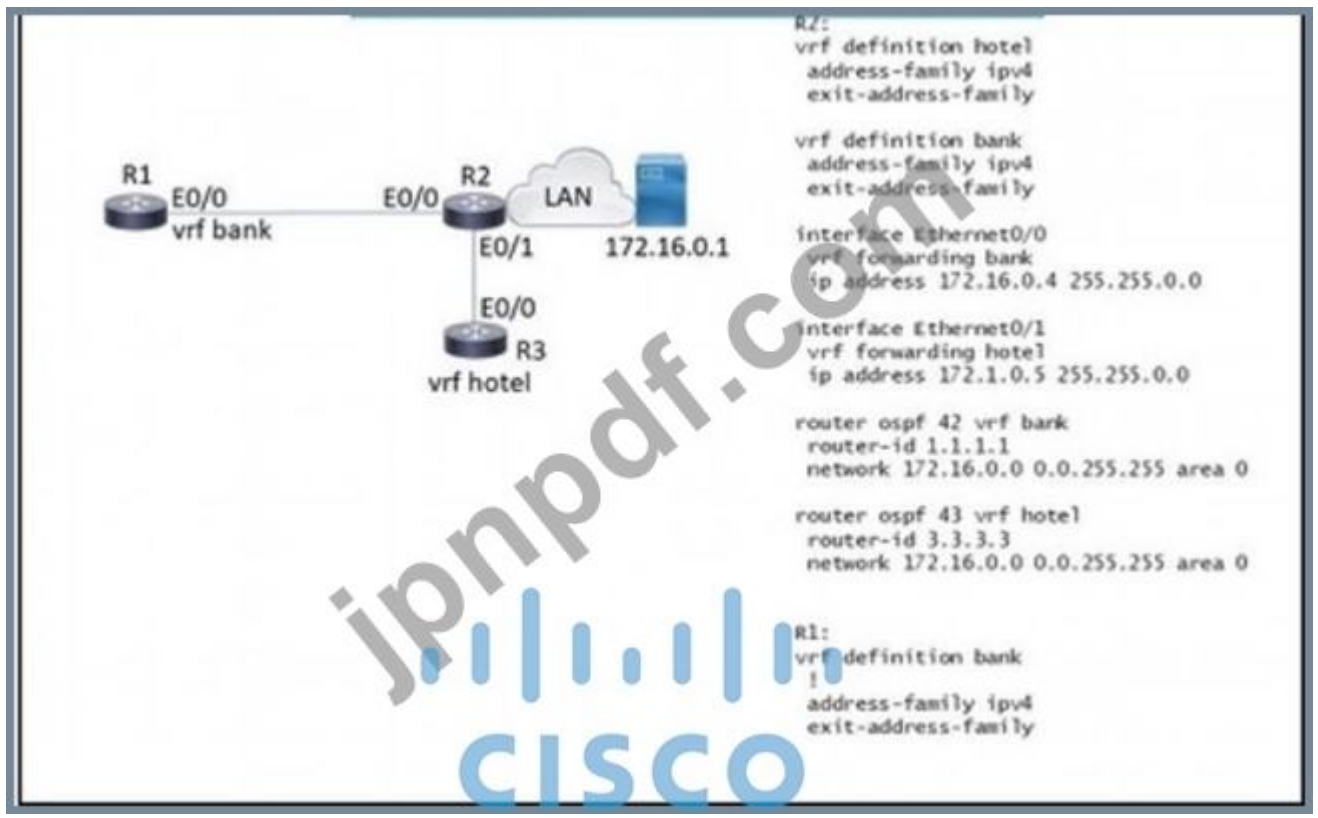
```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.134
```

A. オプション A

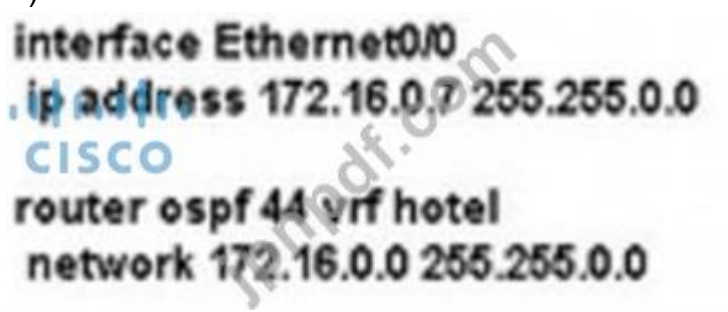
B. オプション B
C. オプション C
D. オプション D
Answer: (解答を表示する**)**
https://community.cisco.com/t5/networking-documents/how-to-configure-a-gre-tunnel/ta-p/3131970#toc-hId--1446104265

最新問題**: 291**
ぜ



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、R にどの構成を適用する必要がありますか?
A)

B)



ハ）

```
interface Ethernet0/0
ip address 172.16.0.7 255.255.0.0

router ospf 44 vrf bank
 network 172.16.0.0 255.255.0.0
```

D)

```
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
```

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

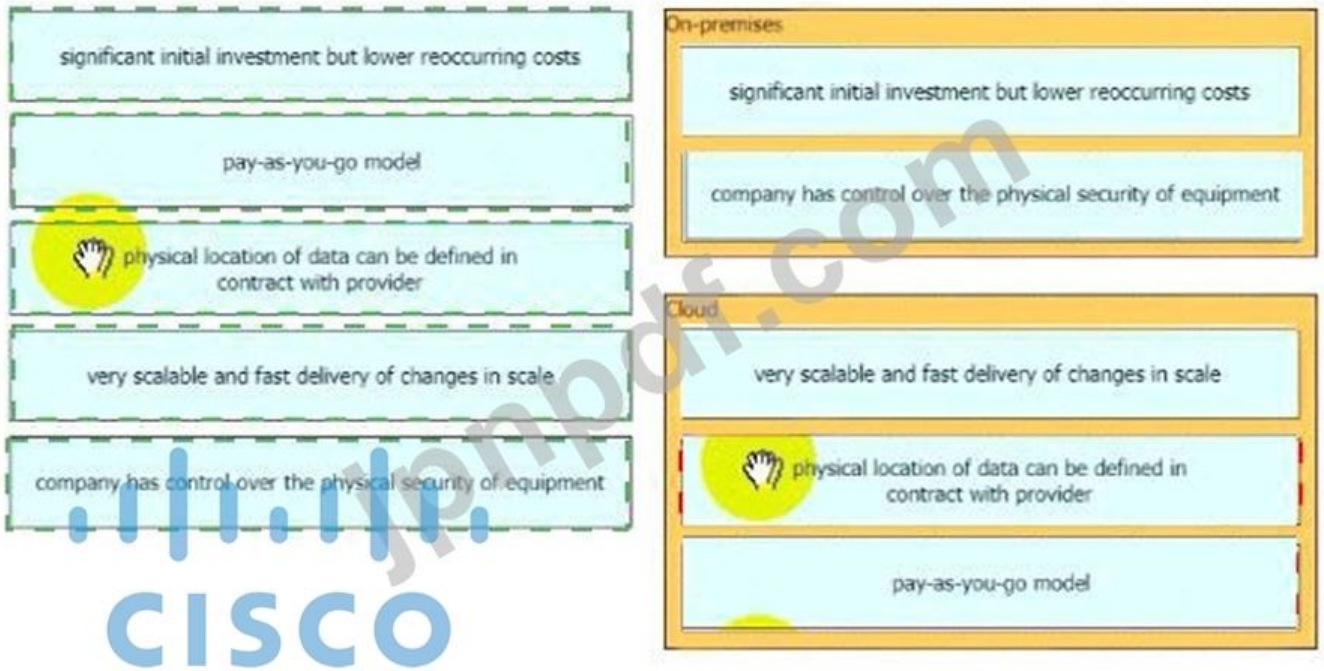
最新問題**: 292**
クラウド展開はオンプレミス展開とどう違うのですか?
A. クラウド展開では、オンプレミス展開よりも頻繁にアップグレードする必要がありません。
B. クラウド展開は、オンプレミス展開よりも初期費用が低くなります。
C. クラウド展開は、オンプレミス展開よりも実装に時間がかかります
D. クラウド展開は、オンプレミス展開よりもカスタマイズ可能です。
Answer: D (メーッセージを残す**)**

最新問題**: 293**
音声ネットワークの最小 SNR を満たす信号強度とノイズ値はどれですか?
A. 信号強度 -68 dBm、ノイズ 89 dBm
B. 信号強度 -67 dBm、ノイズ 91 dBm
C. 信号強度 -66 dBm、ノイズ 90 dBm
D. 信号強度 -69 dBm、ノイズ 94 dBm
Answer: B (メーッセージを残す**)**

最新問題**: 294**

特性を左側から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:

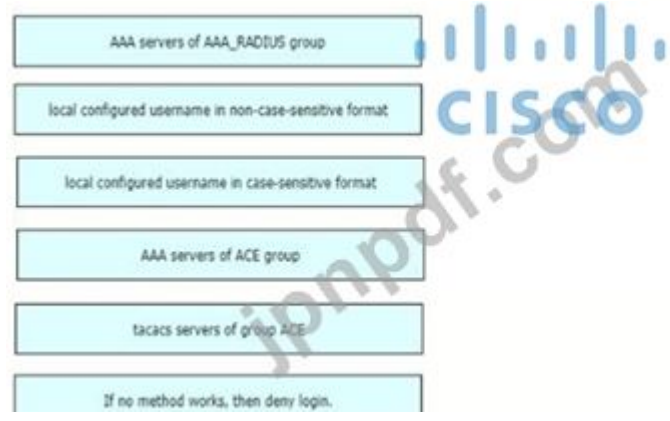


jpnpdf.com

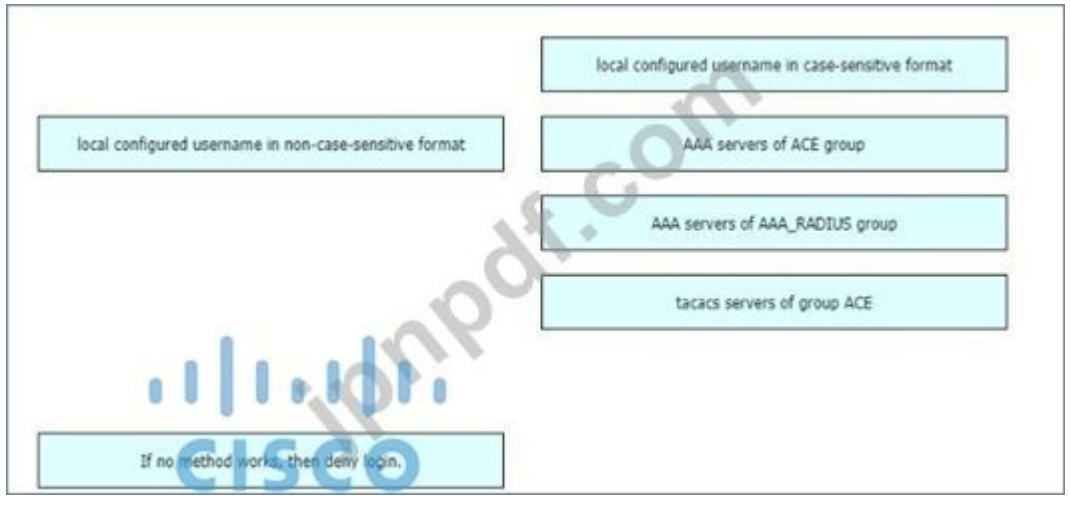
最新問題: **295**

エンジニアが以下の構成を作成します。認証方法を左から右の優先順にドラッグ 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#
```



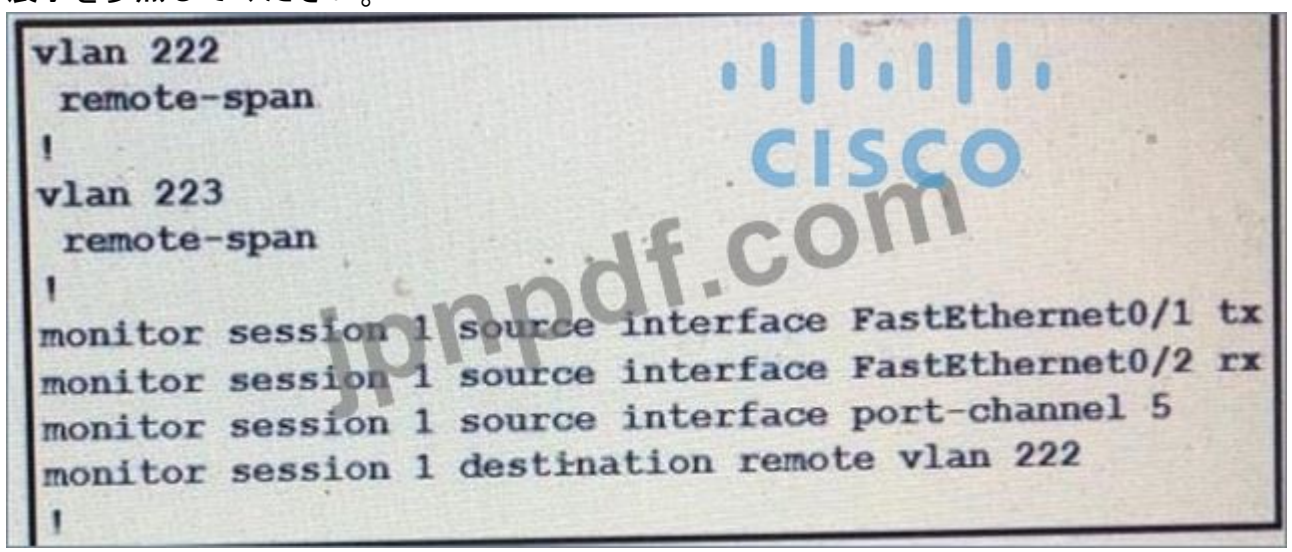
Answer:



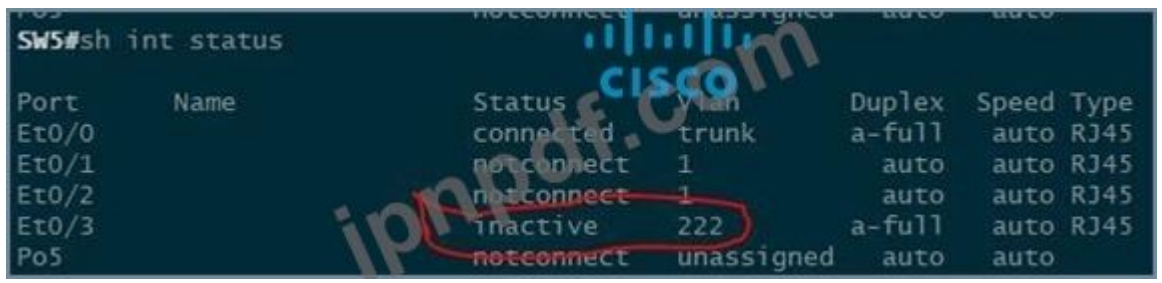
最新問題: **296**

saltstack と ansible の違いは何ですか?
A. SaltStack は SSH を使用して Cisco デバイスとやり取りしますが、Ansible はイベント バスを使用します。
B. SaltStack はボックスで Ansible エージェントを使用しますが、Ansible はボックスで Telnet サーバーを使用します。
C. SaltStack は API プロキシ エージェントを使用して Cisco ボックスをエージェント モードでプログラムしますが、Ansible は Telnet 接続を使用します。
D. SaltStack は minion で構築され、Ansible は YAML で構築されます。
Answer: D (メーッセージを残す)

最新問題**: 297**
展示を参照してください。



VLAN 222 が割り当てられているアクセス インターフェイスはどうなりますか?
A. STP BPDU ガードが有効
B. RSPAN」の記述を追加
C. 非アクティブ状態に置かれます
D. PoE を提供できない
Answer: C (メーッセージを残す)
説明

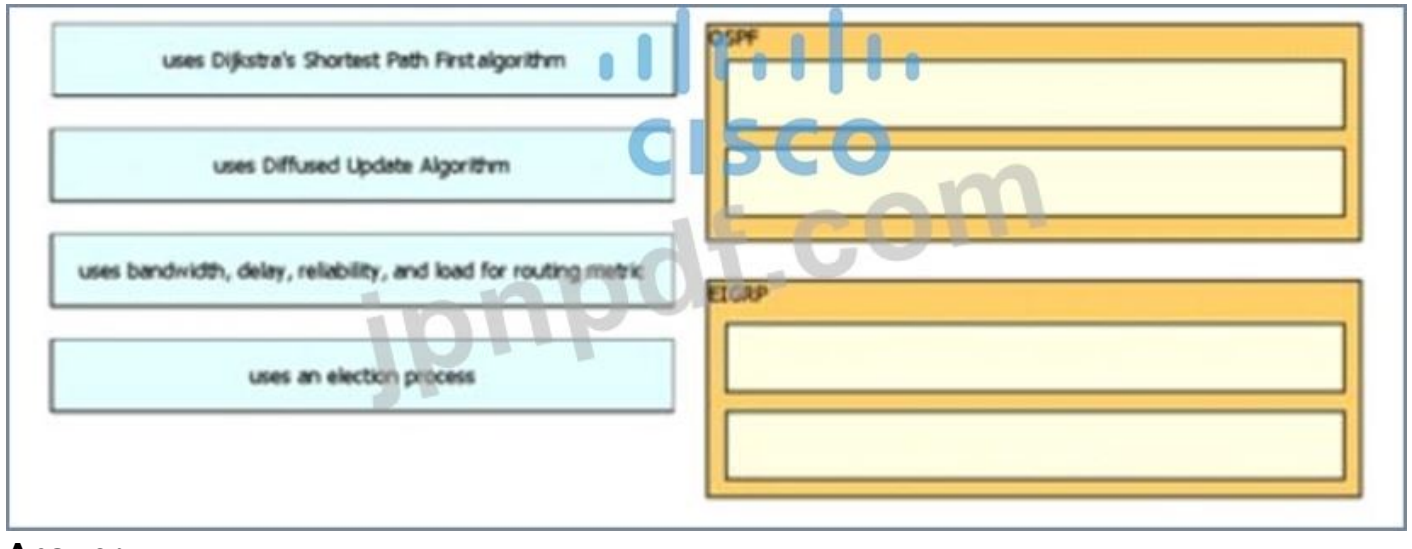


RSPAN VLAN 上のアクセス ポート（音声VLAN ポートを含む）は非アクティブ ステートになります。
参照：
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configura

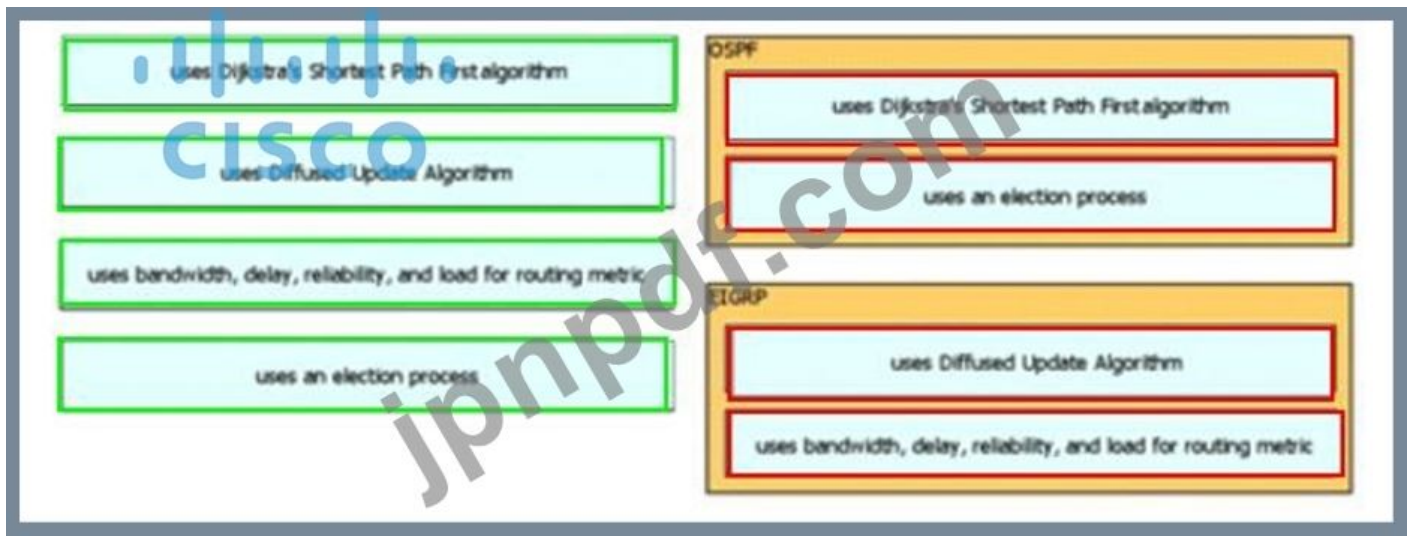
最新問題**: 298**
IP パケット ヘッダーの ToS フィールドの IP Precedence ビットを使用して、トラフィックを異なる優先度レベルに分割する QoS 機能はどれですか?

A. マーキング
B. 分類
C. 整形
D. ポリシング
Answer: (解答を表示する)

最新問題: **299**
左側の特性を、右側の適用対象のプロトコルにドラッグ アンド ドロップしますか?



Answer:



最新問題: **300**
展示を参照してください。

WLC のインターフェイスが RADIUS サーバと同じサブネットにない場合、WLC はどのインターフェイスをすべての RADIUS 関連トラフィックの送信元として使用しますか?

A. WLC で設定された任意のインターフェイス

B. コントローラの仮想インターフェイス

C. WLAN 構成で指定されたインターフェース

D. コントローラー管理インターフェース

Answer: C (メーッセージを残す**)**

最新問題**: 301**

Cisco DNA Center が提供する Intent API を定義する 2 つの特徴はどれですか? (2つ選んでください。)

A. ノースバウンド API

B. ビジネス成果志向

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

The Intent API is a *Northbound* REST API that exposes specific capabilities of the Cisco DNA Center platform.
The Intent API provides policy-based abstraction of business intent, allowing focus on an outcome rather than struggling with individual mechanisms steps.

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 302**

展示を参照してください。

管理者は、err-disabled に移行し続ける EtherChannel をトラブルシューティングします。問題を解決するために実行する必要がある 2 つのアクションはどれですか? 2つ選んでください。）

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 および 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することを確認します。

D. 隣接スイッチの対応するポート 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 と Gi/0/3 の隣接インターフェイスが同じ EtherChannel のメンバーとして構成されていることを確認します。

Answer: B,E (メーッセージを残す**)**

説明

Errdisable の原因 この機能は、スイッチがポート上で過剰またはレイト コリジョンを検出した特殊なコリジョン状況を処理するために最初に実装されました。スイッチが連続して 16 回のコリジョンに遭遇するため、フレームがドロップされると過剰なコリジョンが発生します。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で発生します。これらの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、タイプが間違っている、または欠陥がある)
* 不良のネットワーク 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)
* ポート デュプレックスの設定ミス

ポートのデュプレックス構成の誤りは、2 つの直接接続されたデバイス (たとえば、スイッチに接続する 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、エラーの一般的な原因です。LAN で衝突が発生するのは、半二重接続だけです。イーサネットの Carrier Sense Multiple Access (CSMA) の性質により、衝突がトラフィックのわずかな割合を超えない限り、衝突は半二重では正常です。

最新問題**: 303**

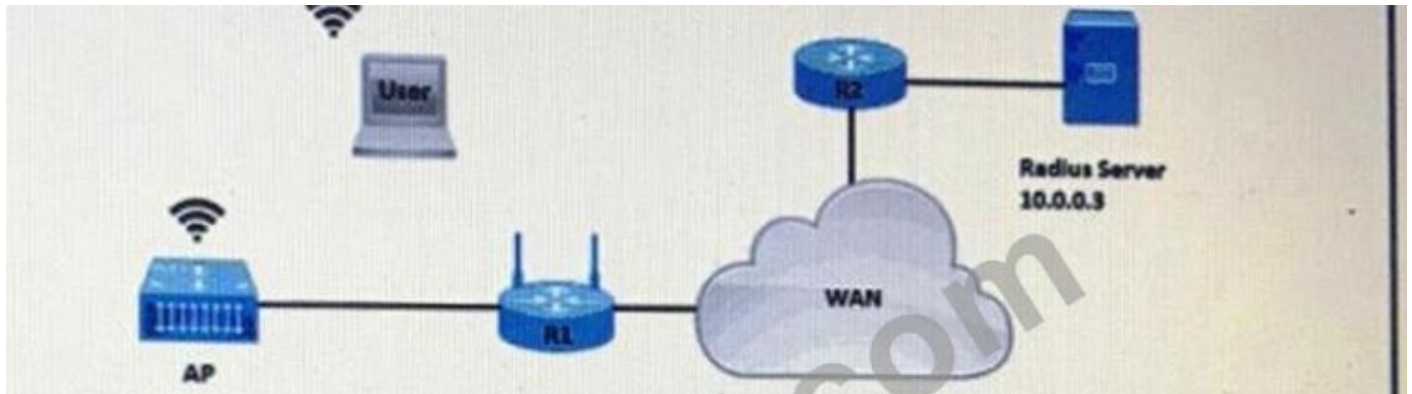
展示を参照してください。Link1 は銅線接続で、Link2 はファイバー接続です。ファイバー ポートは、すべての転送のプライマリ ポートである必要があります。SW2 での show spanning-tree コマンドの出力は、ファイバ ポートがスパニング ツリーによってブロックされていることを示しています。エンジニアは、SW2 の GO/1 で spanning-tree port-priority 32 コマンドを入力します。しかし、ポートはブロックされたままです。

問題を解決するには、Lmk2 に接続されているポートでどのコマンドを入力する必要がありますか?

A. SW1 でスパニング ツリー ポート プライオリティ 32 を入力します。
B. SW1 でスパニング ツリー ポート プライオリティ 224 を入力します。
C. SW2 でスパニング ツリー ポート プライオリティ 4 を入力します。
D. SW2 でスパニング ツリー ポート プライオリティ 64 を入力します。
Answer: A (メーッセージを残す)
SW1 は、2 つのスイッチ間のブリッジング ループを回避するために、SW2 へのポートの 1 つをブロックする必要があります。
残念ながら、ファイバー ポート Link2 がブロックされました。しかし、SW2 はブロックされたポートをどのように選択するのでしょうか? その答えは、SW1 から受信した BPDU に基づいています。次の場合、BPDU は他のものよりも優れています。
1. 低いルート ブリッジ ID
2. ルートへのより低いパス コスト
3. 低い送信ブリッジ ID
4. 低い送信ポート ID
これらの 4 つのパラメーターは、順番に調べられます。この特定のケースでは、SW1 によって送信されたすべての BPDU は、同じルート ブリッジ ID、ルートへの同じパス コスト、および同じ送信ブリッジ ID を持ちます。
最適なものを選択するために残された唯一のパラメーターは、送信ポート ID (ポート ID = ポート優先度 + ポート インデックス) です。また、Gi0/0 のポート インデックスは Gi0/1 のポート インデックスよりも小さいため、リンク 1 がプライマリ リンクとして選択されています。
したがって、プライマリ リンクを変更するには、ポート プライオリティを変更する必要があります。ポート プライオリティの数値が小さいほど、そのポートのプライオリティは高くなります。つまり、SW1 の Gi0/1 (SW2 の Gi0/1 ではなく) のポート プライオリティを、Gi0/0 のポート プライオリティよりも低い値に変更する必要があります。

最新問題**: 304**

展示を参照してください。




```
AP(config)# aaa group server radius rad_auth
AP(config-sg-radius)# server 10.0.0.3 auth-port 1645 acct-port 1646
AP(config)# aaa new-model
AP(config)# aaa authentication login eap_methods group rad_auth
AP(config)# radius-server host 10.0.0.3 auth-port 1645 acct-port 1646 key
labap1200
AP(config)# interface dot11radio 0
AP(config-if)# ssid labap1200
AP(config-if-ssid)# encryption mode wep mandatory
```

ある会社では、すべてのワイヤレス ユーザーが動的なキー生成を使用して認証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. AP(config-if-ssid)# authentication open eap eap_methods

B. AP(config-if-ssid)# authentication dynamic open wep_dynamic

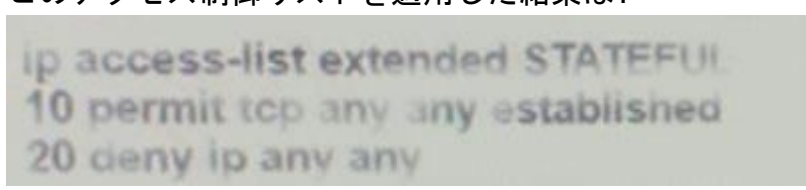
C. AP(config-if-ssid)# authentication dynamic wep wep_methods

D. AP(config-if-ssid)# authentication open wep wep_methods

Answer: A (メーッセージを残す**)**

最新問題**: 305**

このアクセス制御リストを適用した結果は?



A. URG ビットが設定された TCP トラフィックが許可されます

B. SYN ビットが設定された TCP トラフィックが許可されます

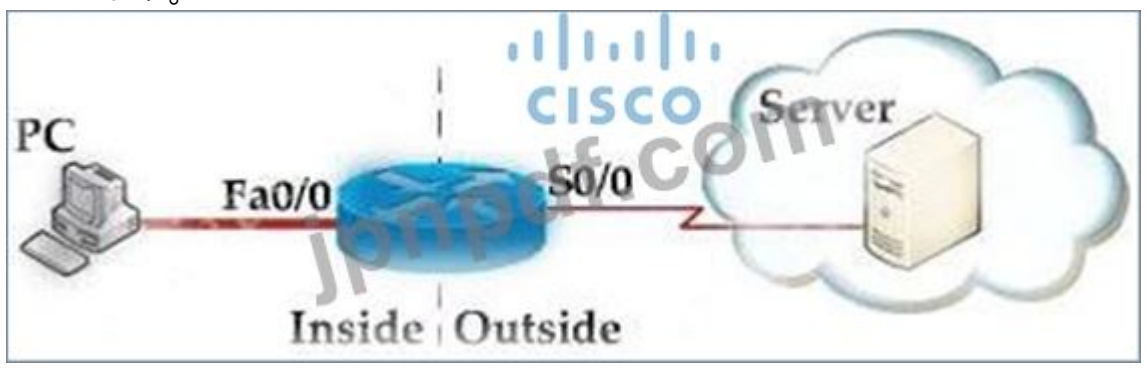
C. ACK ビットが設定された TCP トラフィックが許可されます

D. DF ビットが設定された TCP トラフィックが許可されます

Answer: C (メーッセージを残す**)**

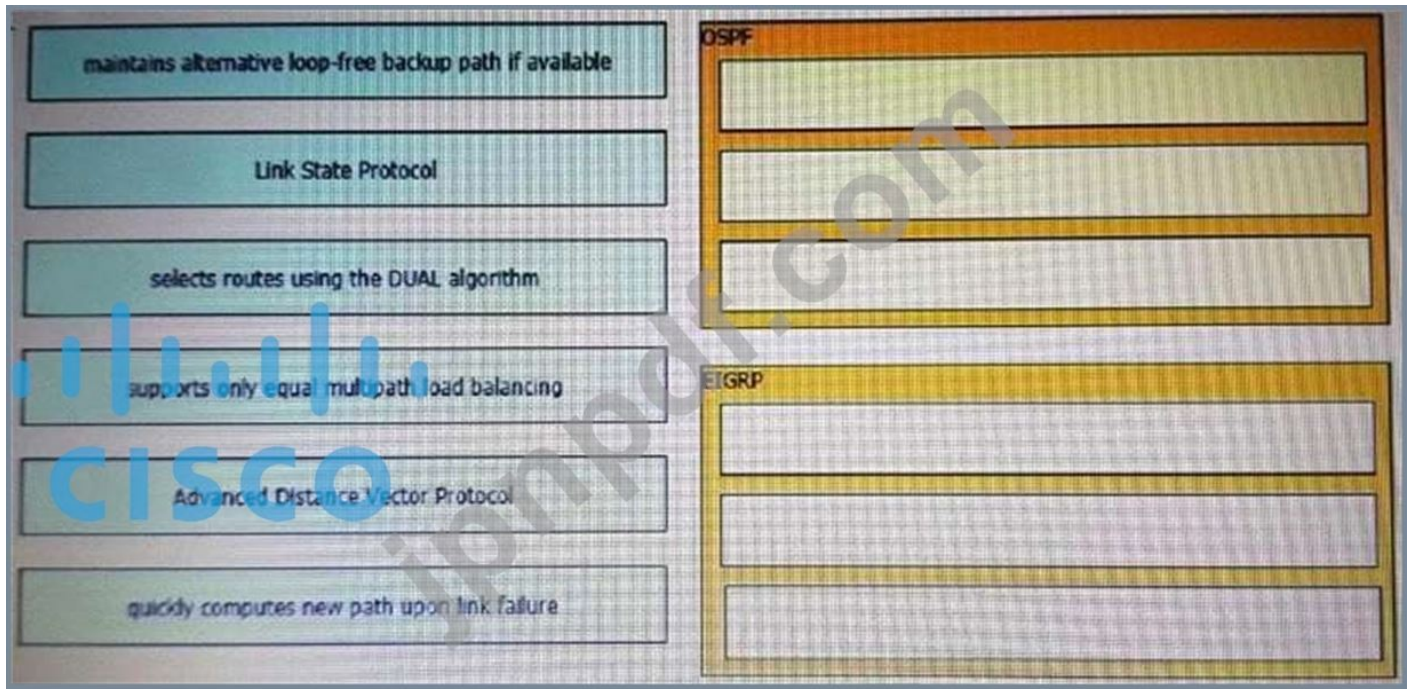
説明

確立されたキーワードは、ACK および/または RST 制御ビットが設定された TCP セグメントに一致する TCP アクセス リスト エントリにのみ適用されます（送信元ポートと宛先ポートに関係なく）。これは、TCP 接続が一方向のみですでに確立されていることを前提としています。. 以下の例を見てみましょう。

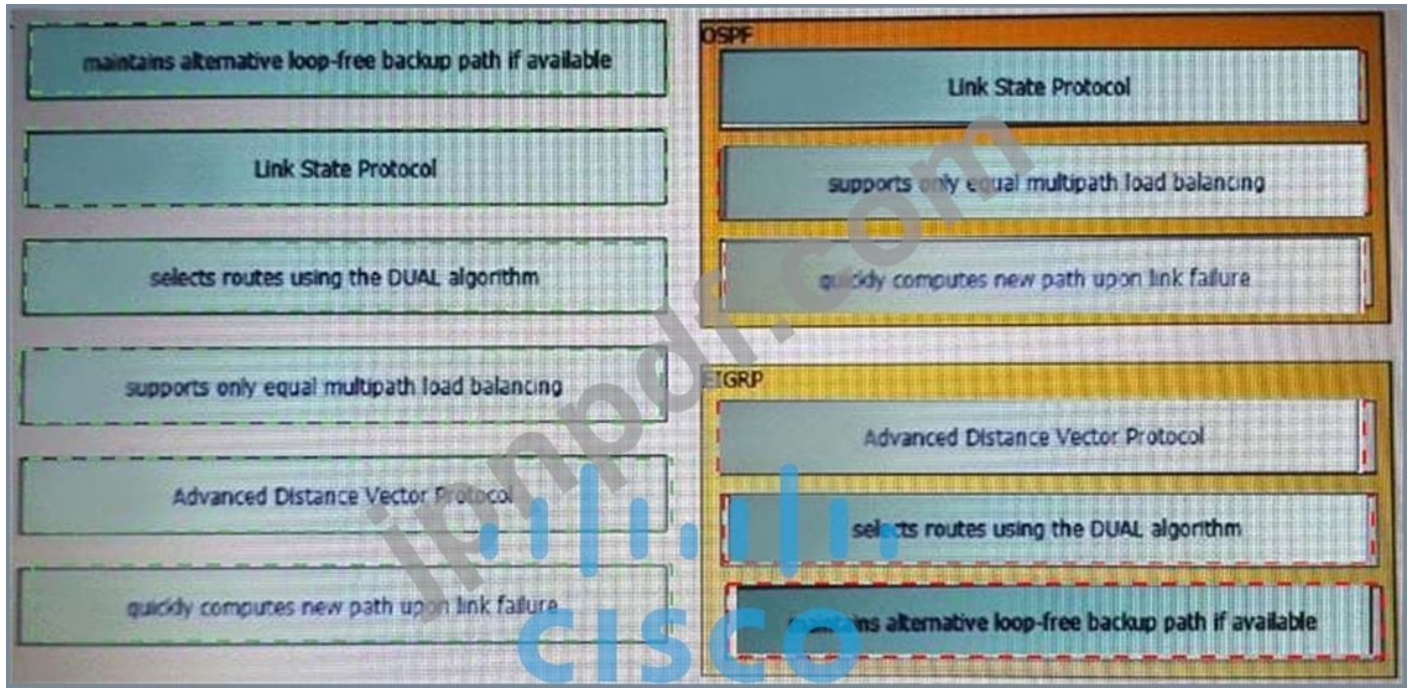


社内のホストに外部サーバーへの telnet を許可したいだけで、その逆は許可したくない場合は、次のように 確立された」アクセス リストを使用できます。tcp any any eq telnet ! インターフェイス S0/0 ip access-group 100 in ip access-group 101 out

最新問題: **306**
左側の特性を、右側に記述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

EIGRP は、フィジブル サクセサを介してループのない代替バックアップを維持します。フィージブル サクセサとしての資格を得るには、ルータのアドバタイズ ディスタンス (AD) が現在のサクセサ ルートのフィージブル ディスタンス (FD) よりも小さい必要があります。
アドバタイズド ディスタンス (AD): ネイバーから宛先までのコスト。フィージブル ディスタンス (FD): AD と、ローカル ルーターとネクスト ホップ ルーター間のコストの合計

最新問題: **307**
エンジニアが YANG を使用する理由
A. JSON を同等の XML 構文に変換します。
B. SNMP を使用してデータにアクセスする
C. コントローラとネットワーク デバイス間でデータを転送する
D. NETCONF のモデル データへ
Answer: D (メーッセージを残す)

最新問題: **308**
展示を参照してください。

```
------------------------------------------------------------------------------
------------------------------------------------------------------------------
------
vsmart  dtls 4.4.4.70        100        1       192.168.100.80
12446 10.10.20.70                               12446 default        No    up
0:02:24:09  0
vbond   dtls 0.0.0.0         0          0       192.168.100.81
12346 10.10.20.80                               12346 default        -     up
0:02:24:10  0
vmanage dtls 4.4.4.90        100        0       192.168.100.82
12446 10.10.20.90                               12446 default
```

認証の問題を解決するには、どの手順を実行しますか?

A. vsmart ホストを再起動します。
B. 基本認証を使用
C. ポートを 12446 に変更します
D. URI のターゲット 192 168 100 82
Answer: (解答を表示する**)**

最新問題: **309**
RESTCONF を使用してネットワーク デバイスに構成を書き込む場合、TLS について正しい記述はどれですか?

A. プロキシ Web サーバーとして機能する NGINX を使用して提供されます。
B. Cisco デバイスではサポートされていません。
C. 認証に証明書が必要でした。
D. HTTP および HTTPS リクエストに使用されます。
Answer: (解答を表示する**)**

デバイスがスタートアップ コンフィギュレーションで起動すると、nginx プロセスが実行されます。NGINX は、プロキシ Web サーバーとして機能する内部 Web サーバーです。Transport Layer Security (TLS) ベースの HTTPS を提供します。HTTPS 経由で送信された RESTCONF リクエストは、最初に NGINX プロキシ Web サーバーによって受信され、さらに構文/セマンティクス チェックのために confd Web サーバーに転送されます。
参照：

ios/prog/configuration/168/b_168_programmability_cg/RESTCONF.html
ステートレス プロトコルである https ベースのプロトコル RESTCONF (RFC 8040) は、安全な HTTP メソッドを使用して、YANG 定義のデータを含む概念的なデータストアで CREATE、READ、UPDATE、および DELETE (CRUD) 操作を提供します -> RESTCONF は HTTP のみを使用します.

最新問題: **310**
脅威防御ソリューションを左側から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: **311**
展示を参照してください。

このデータから派生した JSON 構文はどれですか?

({['First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}

{'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Reading'}]}

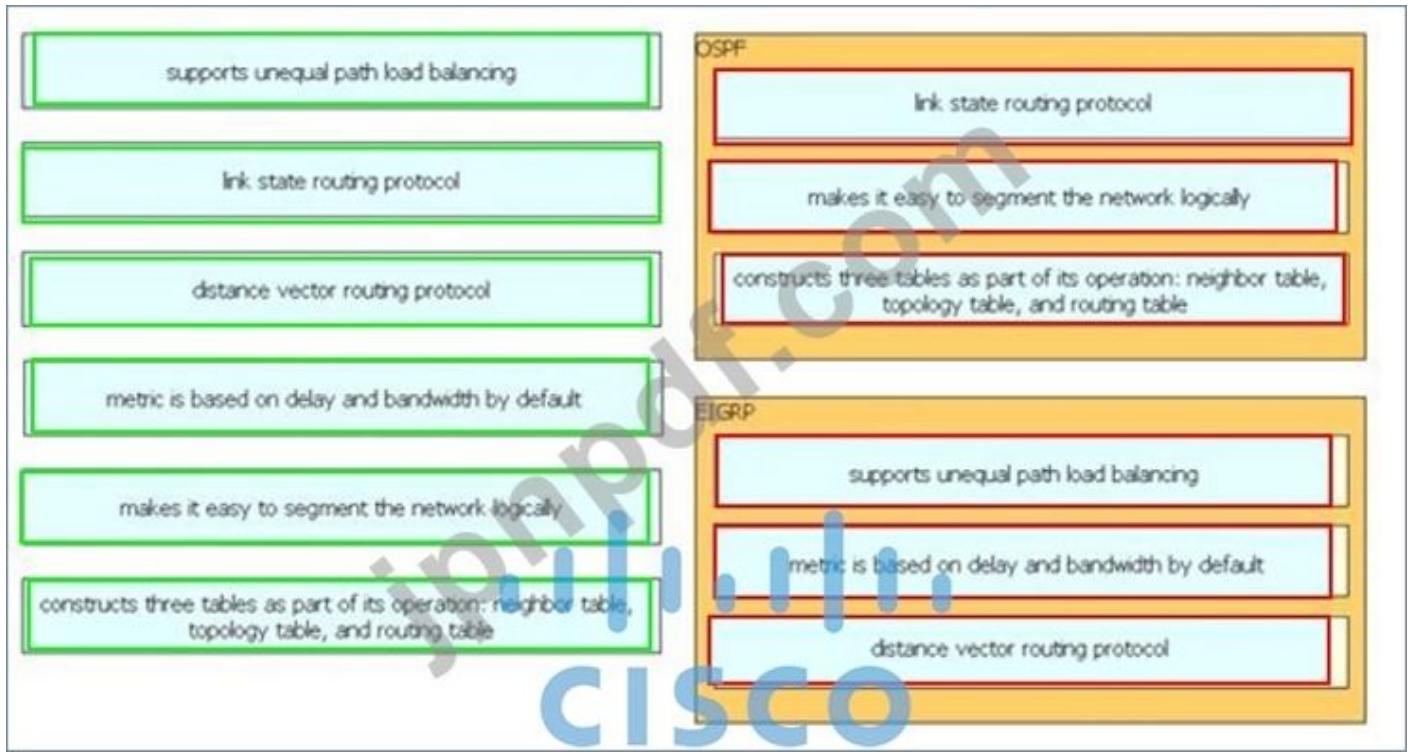
({['First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Hobbies': 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Hobbies': 'Reading'}]}

{'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}

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**: 312**
左側の特性を、右側に記述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。

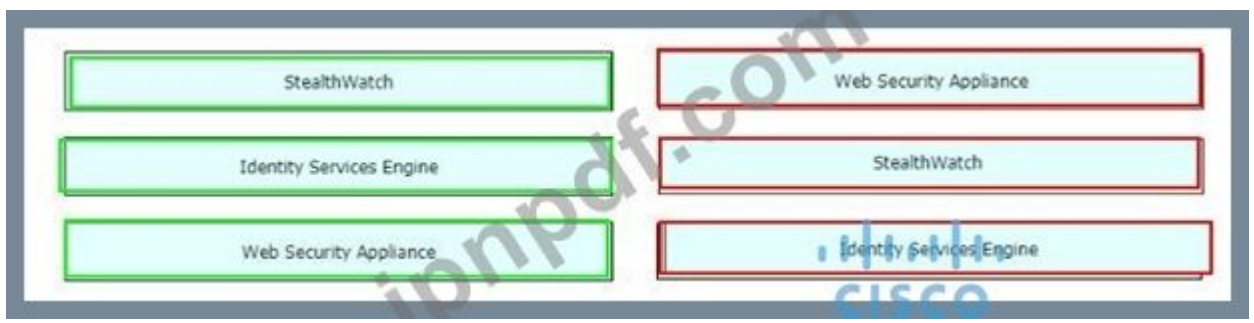
Answer:



最新問題**: 313**

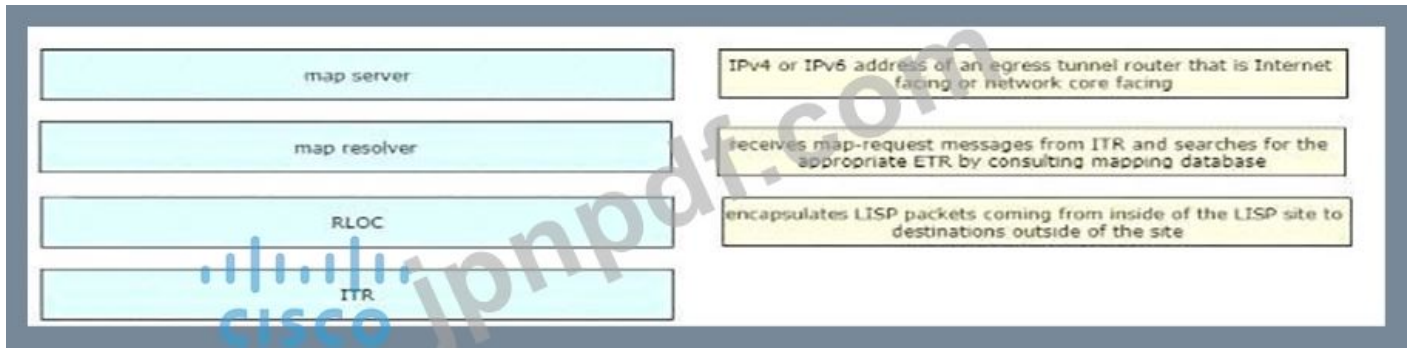
Cisco Cyber Threat Defense を構成するソリューションを、左から右の達成目標にドラッグ アンド ドロップします。

Answer:

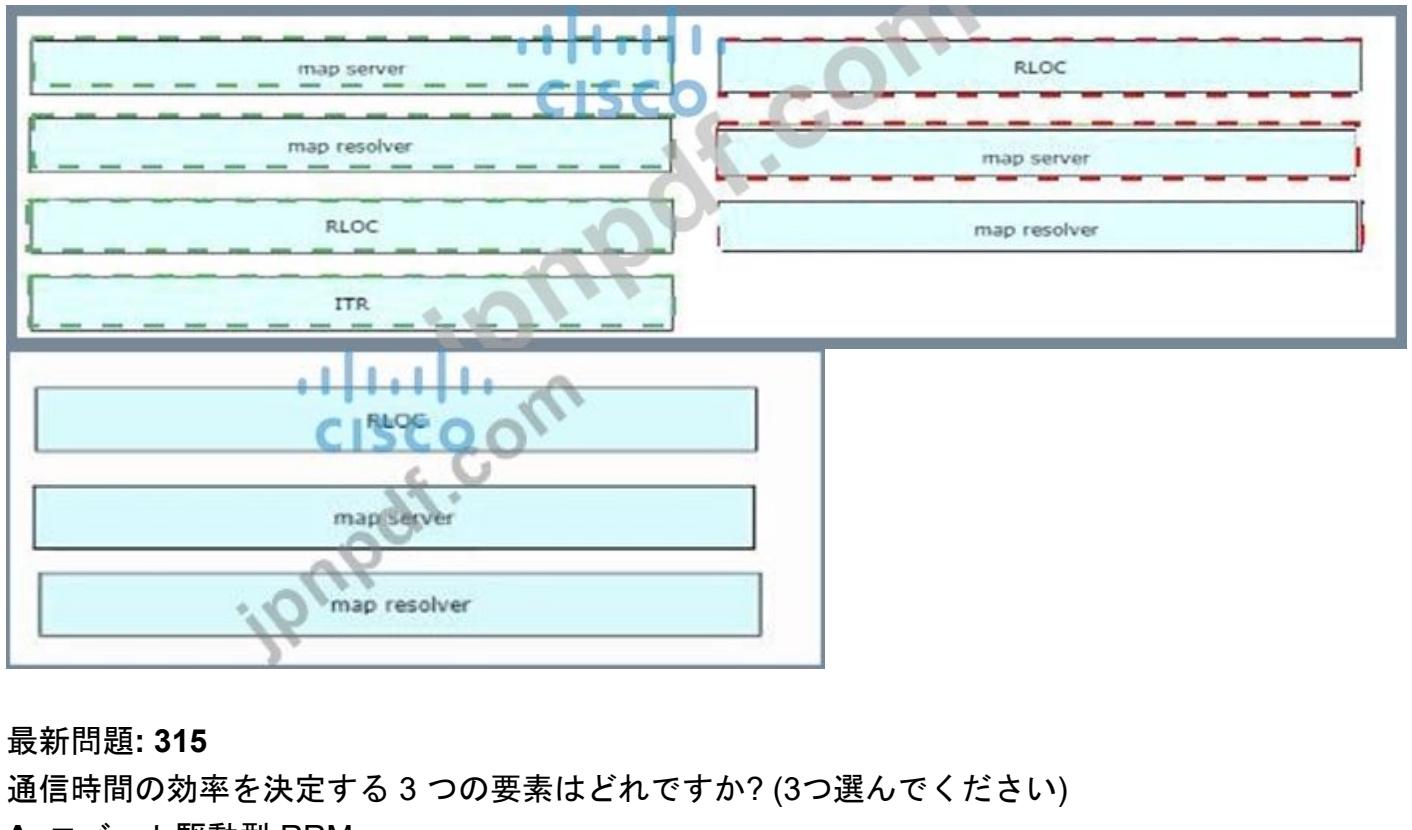


最新問題**: 314**

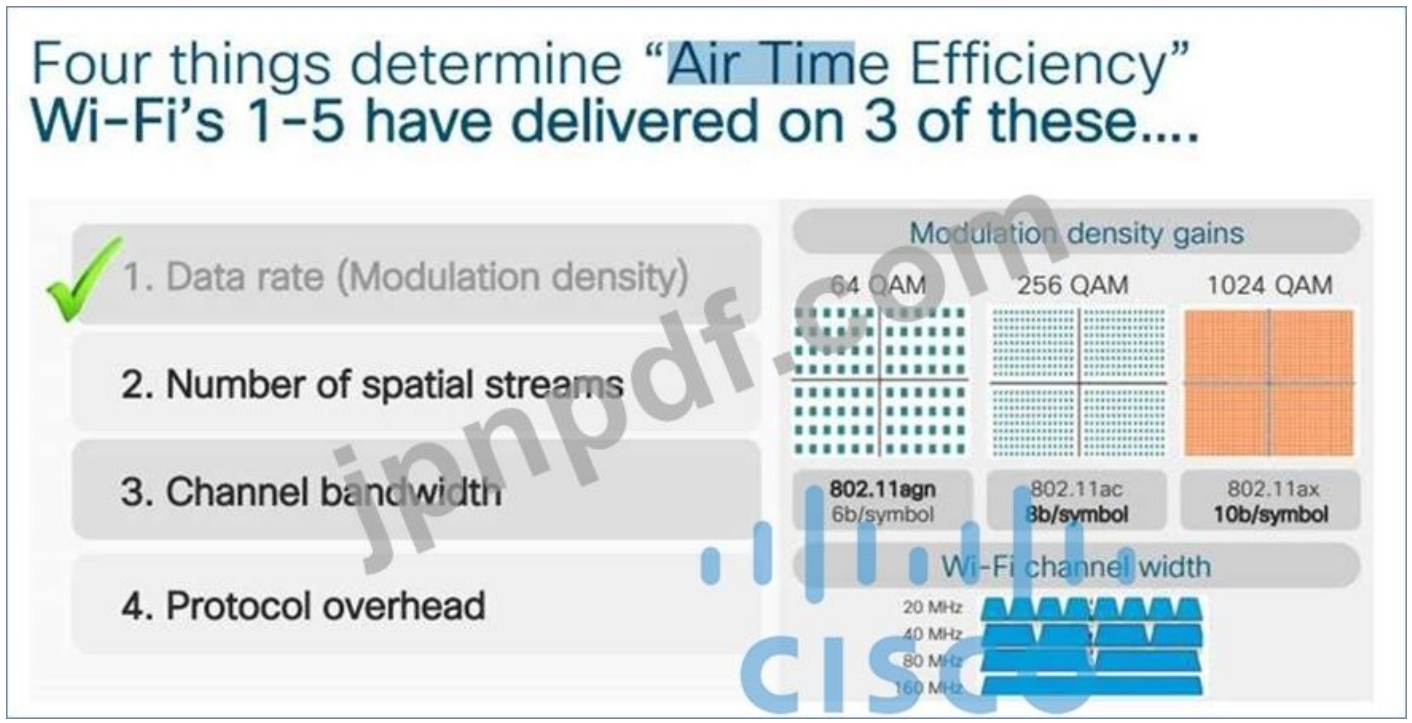
左側の LISP コンポーネントを右側の説明にドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。



Answer:



最新問題: **315**
通信時間の効率を決定する 3 つの要素はどれですか? (3つ選んでください)
A. エバート駆動型 RRM
B. データ レート (変調密度) または QAM
C. チャネル帯域幅
D. 空間ストリーム数と空間再利用
E. RF グループ リーダー
F. 動的チャネル割り当て
Answer: B,C,D (メーッセージを残す**)**
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKEWN-3010.pdf



最新問題**: 316**
通信チャネルを保護するために REST API が依存するプロトコルはどれですか?
A. TCP
B. HTTPS
C. SSH
D. HTTP
Answer: B (メーッセージを残す**)**
REST API は、HTTP (デフォルトでは無効) または HTTPS メッセージを受け入れて返します。
JavaScript Object Notation (JSON) または Extensible Markup Language (XML) ドキュメント。使用できます
メッセージと JSON または XML ドキュメントを生成するための任意のプログラミング言語
API メソッドまたは管理対象オブジェクト (MO) の説明が含まれています。
参照：
x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Config
uration_Guide_chapter_01.html

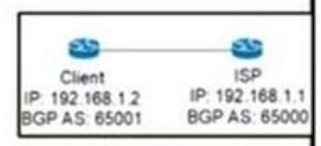
有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら:
https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 317**
OSI モデルのレイヤ 2 ですべてのトラフィックに安全な通信チャネルを提供するテクノロジはどれですか?
A. MACsec
B. IPsec

C. SSL
D. Cisco Trustsec
Answer: (解答を表示する**)**
説明
802.1AE で定義された MACsec は、暗号化キーイングに帯域外方式を使用して、有線ネットワーク上で MAC 層の暗号化を提供します。MACsec Key Agreement (MKA) プロトコルは、必要なセッション キーを提供し、必要な暗号化キーを管理します。MKA と MACsec は、802.1x Extensible Authentication Protocol (EAP-TLS) または Pre Shared Key (PSK) フレームワークを使用して認証が成功した後に実装されます。
MACsec を使用するスイッチは、MKA ピアに関連付けられたポリシーに応じて、MACsec または非 MACsec フレームのいずれかを受け入れます。MACsec フレームは暗号化され、整合性チェック値 (ICV) で保護されます。スイッチは、MKA ピアからフレームを受信すると、フレームを復号化し、MKA から提供されたセッション キーを使用して正しい ICV を計算します。スイッチは、その ICV をフレーム内の ICV と比較します。それらが同一でない場合、フレームはドロップされます。スイッチはまた、現在のセッション キーを使用して、セキュア ポート セキュア MAC サービスを MKA ピアに提供するために使用されるアクセス ポイント）を介して送信されるすべてのフレームに ICV を暗号化し、追加します。
参照: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/sec/b_169_sec_9300_cg/macsec_encryption.html
注: Cisco Trustsec は、MACsec を含むソリューションです。

最新問題**: 318**
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、トポロジに従って BGP を構成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なく、一部のオプションは 2 回使用される場合があります。

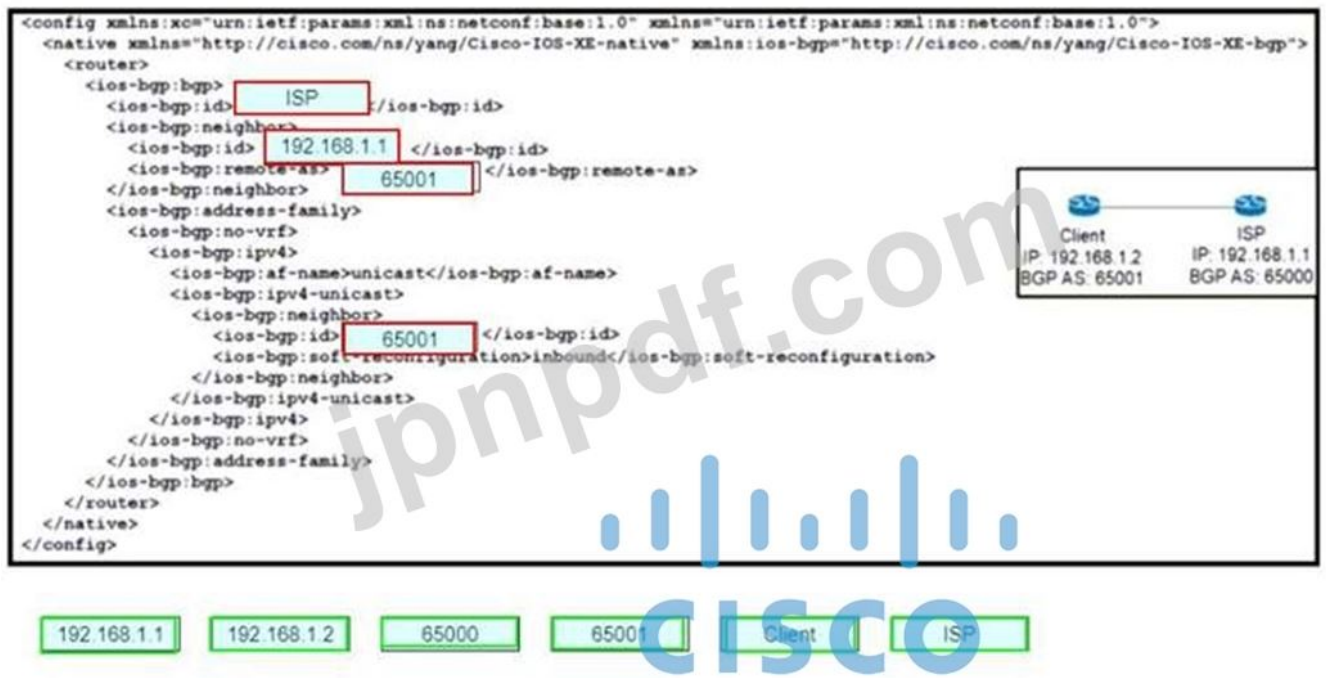
```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native" xmlns:ios-bgp="http://cisco.com/ns/yang/Cisco-IOS-XE-bgp">
    <router>
      <ios-bgp:bgp>
        <ios-bgp:id>                </ios-bgp:id>
        <ios-bgp:neighbor>
          <ios-bgp:id>              </ios-bgp:id>
          <ios-bgp:remote-as>       </ios-bgp:remote-as>
        </ios-bgp:neighbor>
        <ios-bgp:address-family>
          <ios-bgp:no-vrf>
            <ios-bgp:ipv4>
              <ios-bgp:af-name>unicast</ios-bgp:af-name>
              <ios-bgp:ipv4-unicast>
                <ios-bgp:neighbor>
                  <ios-bgp:id>          </ios-bgp:id>
                  <ios-bgp:soft-reconfiguration>inbound</ios-bgp:soft-reconfiguration>
                </ios-bgp:neighbor>
              </ios-bgp:ipv4-unicast>
            </ios-bgp:ipv4>
          </ios-bgp:no-vrf>
        </ios-bgp:address-family>
      </ios-bgp:bgp>
    </router>
  </native>
</config>
```



192.168.1.1　192.168.1.2　65000　65001　Client　ISP

Answer:

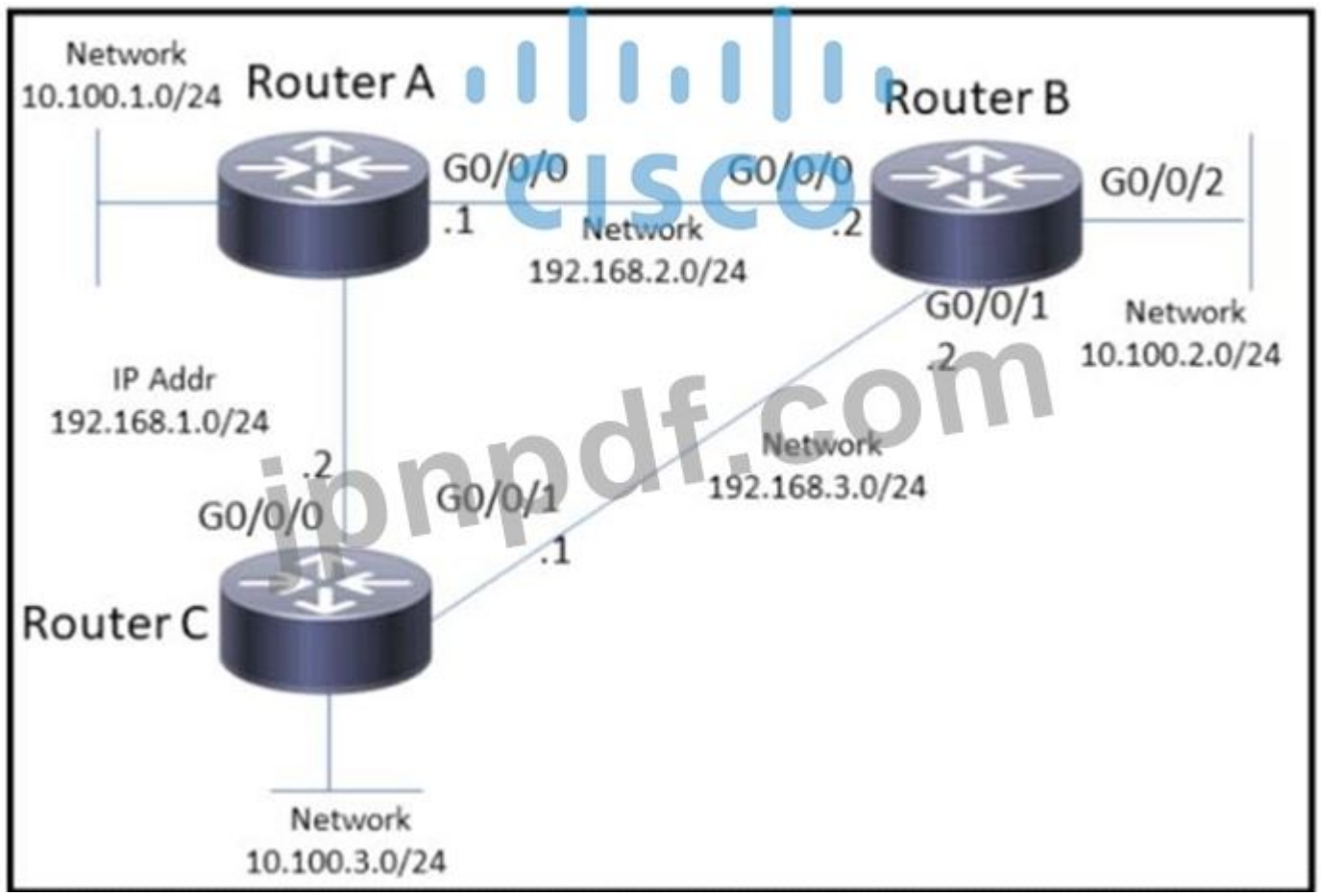
cisco
ipnpdf.com



最新問題**: 319**
SD-Access 展開でファブリック エッジ ノードが実行する機能はどれですか?
A. 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
B. ファブリック アンダーレイのボーダー ノード間の到達可能性を提供します。
C. エンドユーザーのデータ トラフィックを LISP にカプセル化します。
D. 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ー 3 ネットワークに接続します。
Answer: (解答を表示する**)**

最新問題**: 320**
EIGRP メトリックは OSPF メトリックとどのように異なりますか?
A. EIGRP メトリックは、帯域幅のみに基づいて計算されます。OSPF メトリックは遅延のみで計算されます。
B. EIGRP メトリックは、遅延のみに基づいて計算されます。OSPF メトリックは、帯域幅と遅延で計算されます。
C. EIGRP メトリックは、帯域幅と遅延に基づいて計算されます。OSPF メトリックは、帯域幅のみで計算されます。
D. EIGRP メトリックは、ホップ カウントと帯域幅に基づいて計算されます。OSPF メトリックは、帯域幅と遅延で計算されます。
Answer: C (メーッセージを残す**)**
デフォルトでは、EIGRP メトリックが計算されます。
メトリック = 帯域幅 + 遅延
OSPF は次のように計算されます。
OSPF メトリック = 参照帯域幅 / インターフェイス帯域幅 (bps)
(または、Cisco は参照帯域幅として 100Mbps (108) 帯域幅を使用します。この帯域幅を使用すると、方程式は次のようになります。
コスト = 108/インターフェイス帯域幅 (bps)

最新問題**: 321**
展示を参照してください。ネットワーク エンジニアは、10.100 2.248 ～ 10.100.2 255 の範囲のホストからネットワーク 10.100.3.0 への Telnet トラフィックをブロックし、それ以外はすべて許可する必要があります。エンジニアはどの構成を適用する必要がありますか?



A)

```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 22
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

B)

```
RouterB(config)# access-list 101 deny icmp 10.100.2.0 0.0.0.248 10.100.2.0 0.0.0.248
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

```
RouterB(config)# access-list 101 deny tcp 10.100.2.0 0.0.0.248 10.100.3.0 0.0.0.255 eq 23
RouterB(config)# access-list 101 permit any any
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

```
RouterB(config)# access-list 101 permit tcp 10.100.2.0 0.0.0.252 10.100.3.0 0.0.0.255
RouterB(config)# int g0/0/2
RouterB(config-if)# ip access-group 101 in
```

A. オプション C

B. オプション D

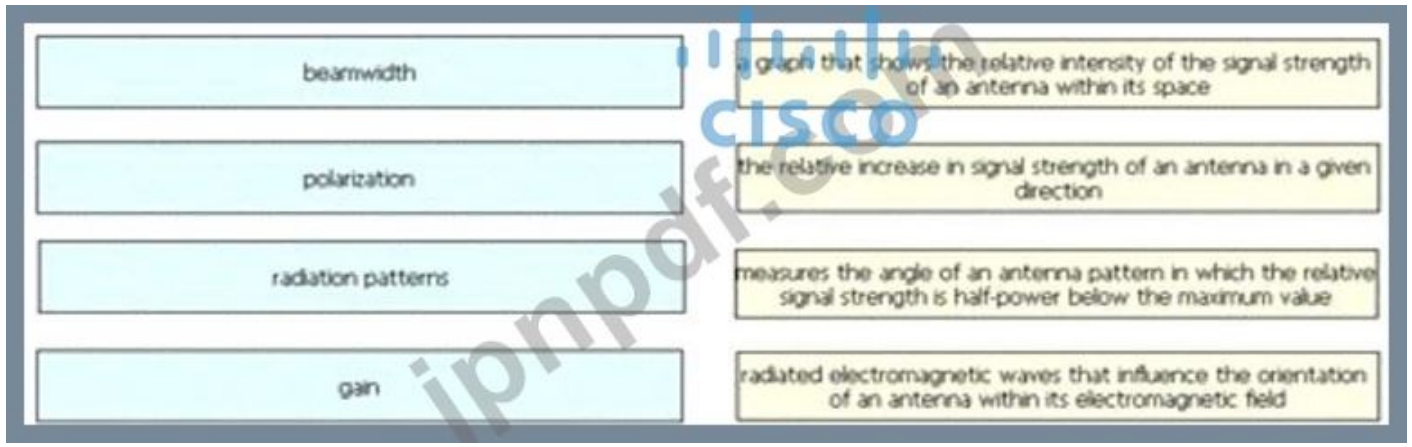
C. オプション A

D. オプション B

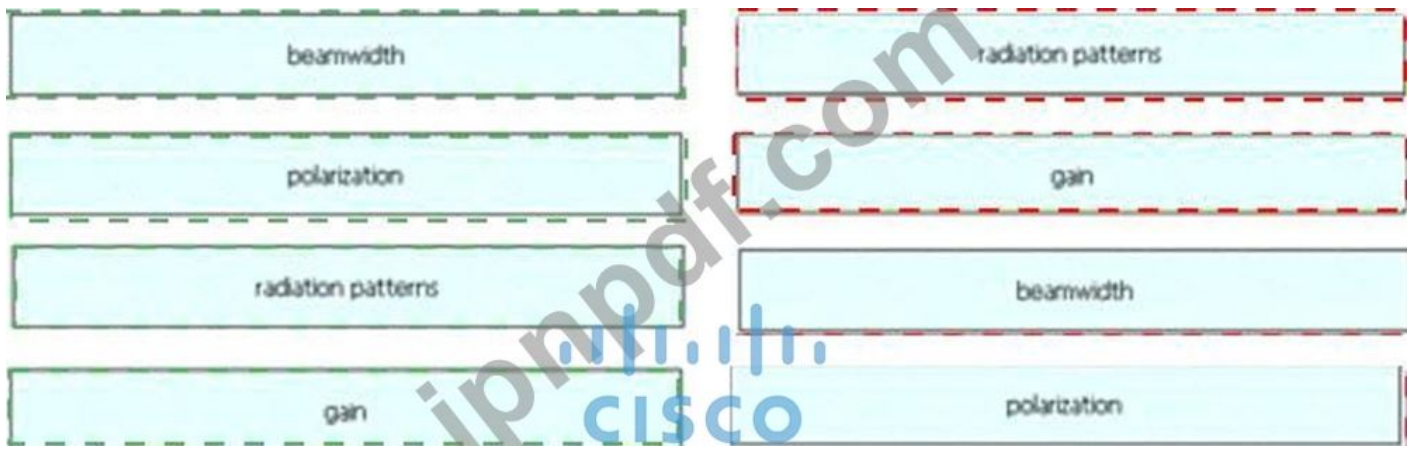
Answer: (解答を表示する**)**

最新問題: **322**

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。

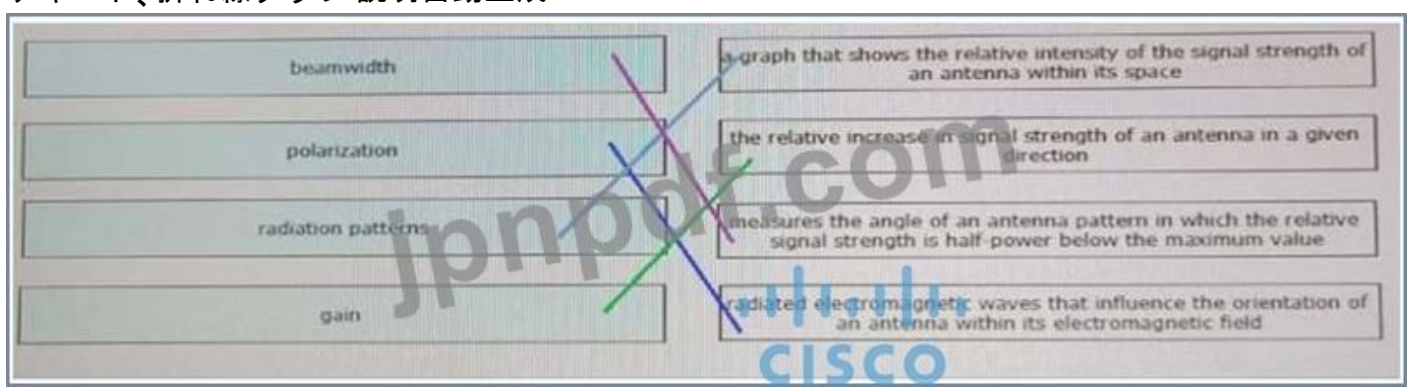


Answer:



説明

チャート、折れ線グラフ 説明自動生成



最新問題: **323**

展示を参照してください。

https://mydevice.mycompany.com/getstuff?queryName=errors&queryResults=yes

展示で使用されているネットワーク スクリプト自動化オプションまたはツールはどれですか?

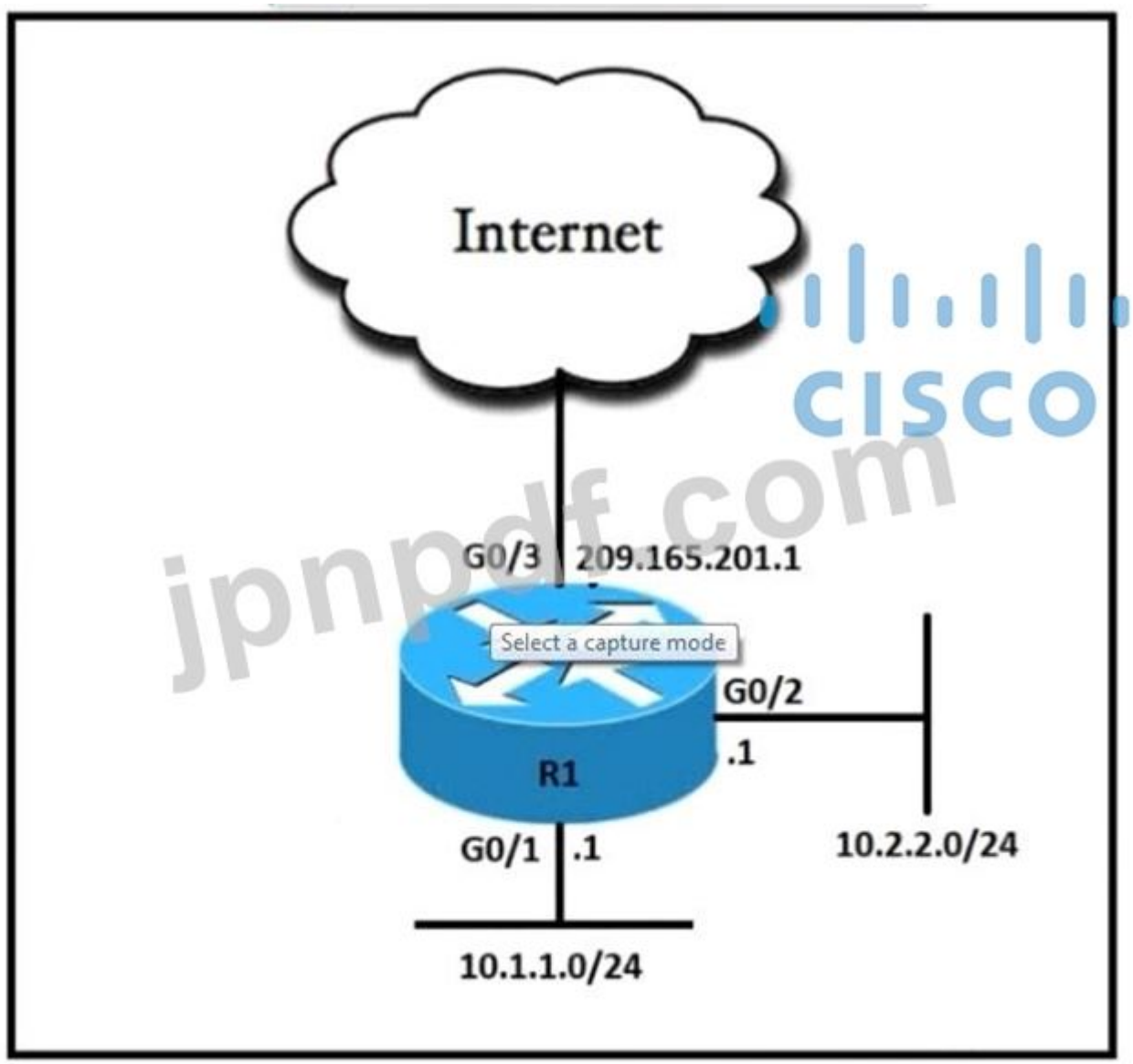
A. Bash スクリプト

B. REST 正しい

C. EEM

D. パイソン
E. ネットコンフ
Answer: B (メーッセージを残す**)**

最新問題: **324**
参照する
展示品。



エンジニアは、10.2.2.0/24 サブネット内のすべてのユーザーがインターネットにアクセスできるようにする必要があります。アドレス空間を節約するために、209.165.201.1 のパブリック インターフェイス アドレスをすべての外部通信に使用する必要があります。これらの要件を満たすコマンド セットはどれですか?

A)

```
access-list 10 permit 10.2.2.0 0.0.0.255

interface G0/3
ip nat outside

interface G0/2
ip nat inside

ip nat inside source list 10 interface G0/2 overload
```

B)

ハ)

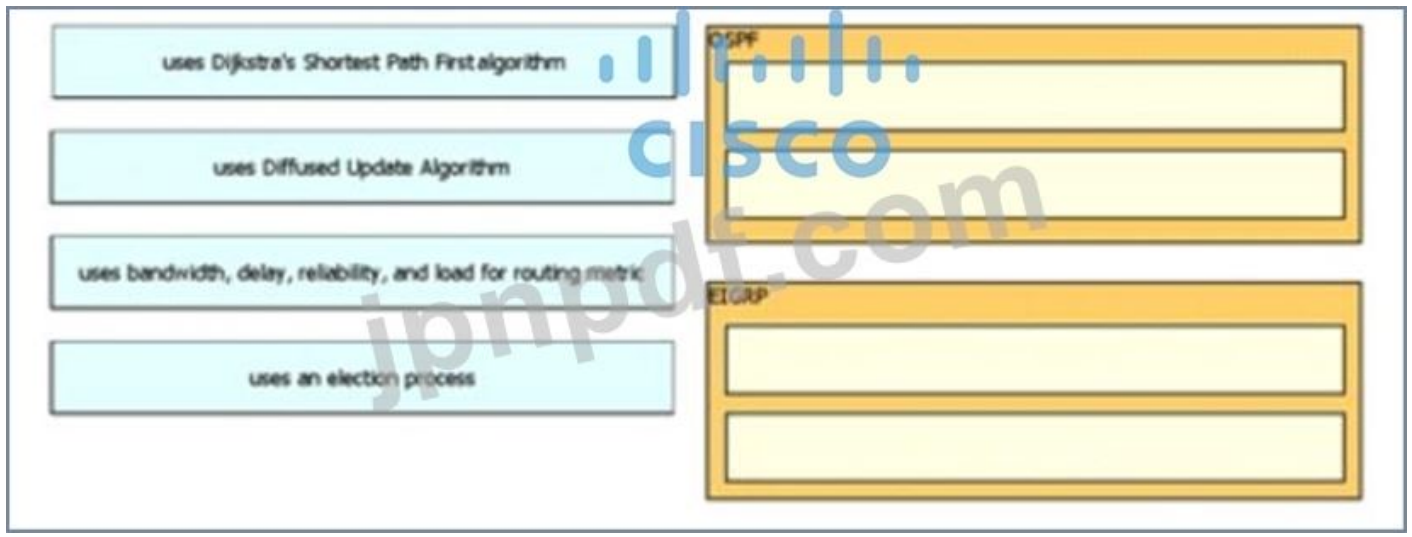
D)

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: (解答を表示する**)**

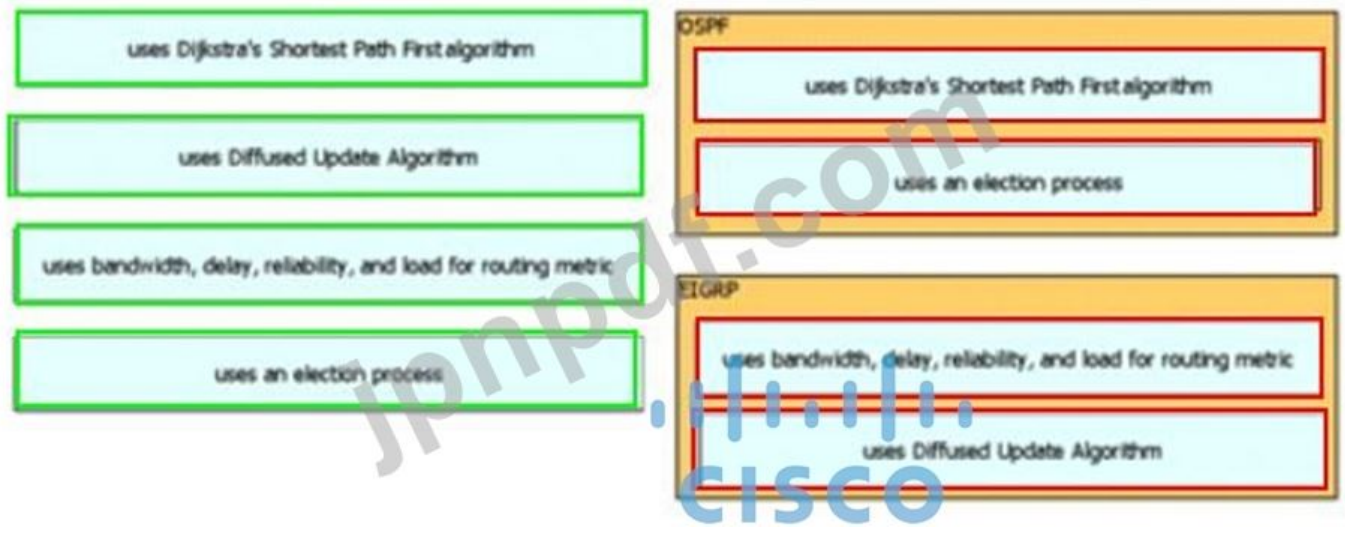
最新問題**: 325**
Cisco DNA サウスバウンド API は何を提供しますか?
A. コントローラとネットワーク デバイス間のインターフェイス
B. オーケストレーション通信用の NETCONF API インターフェイス
C. オーケストレーター通信用の RESful API インターフェイス
D. コントローラとコンシューマ間のインターフェース
Answer: A (メーッセージを残す**)**
説明
Southbound API は、ネットワーク デバイスとの通信に使用されます。

最新問題: **326**

左側の特性を、右側の適用対象のプロトコルにドラッグ アンド ドロップしますか?



Answer:



最新問題: **327**

正しくないパスワードが REST API セッションに適用された要求に対する正しい応答は、どの HHTP 状態コードですか?

A. HTTP ステータス コード 200

B. HTTP ステータス コード 302

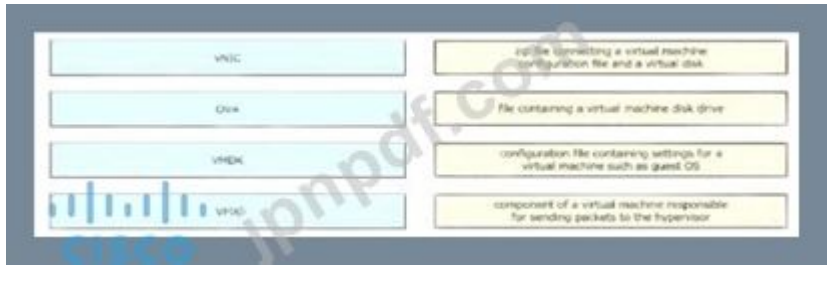
C. HTTP ステータス コード 401

D. HTTP ステータス コード: 504
Answer: (解答を表示する**)**
401 エラー応答は、クライアントが適切な承認を提供せずに保護されたリソースを操作しようとしたことを示します。間違った資格情報を提供したか、まったく提供しなかった可能性があります。
注: HTTP ステータス コード 200」に回答してください。4xx コードは クライアント エラー」を示し、5xx コードは サーバー エラー」を示します。

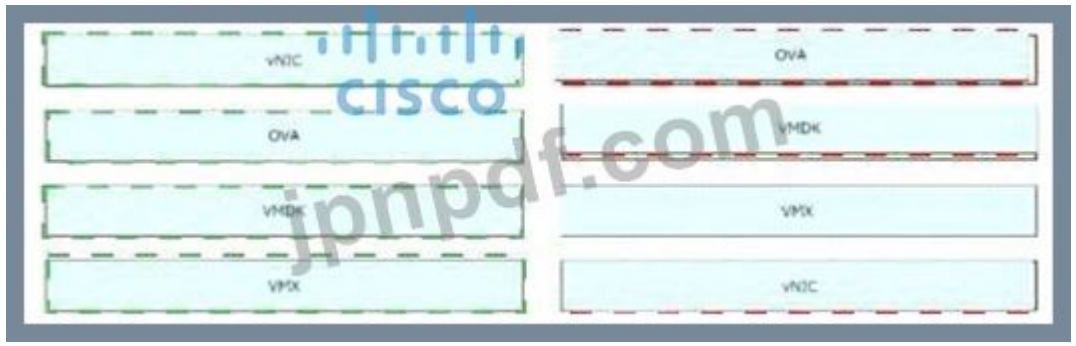
最新問題**: 328**
展示を参照してください。

VTY ユーザーに割り当てられる権限レベルは?
A. 7
B. 1
C. 15
D. 13
Answer: C (メーッセージを残す**)**

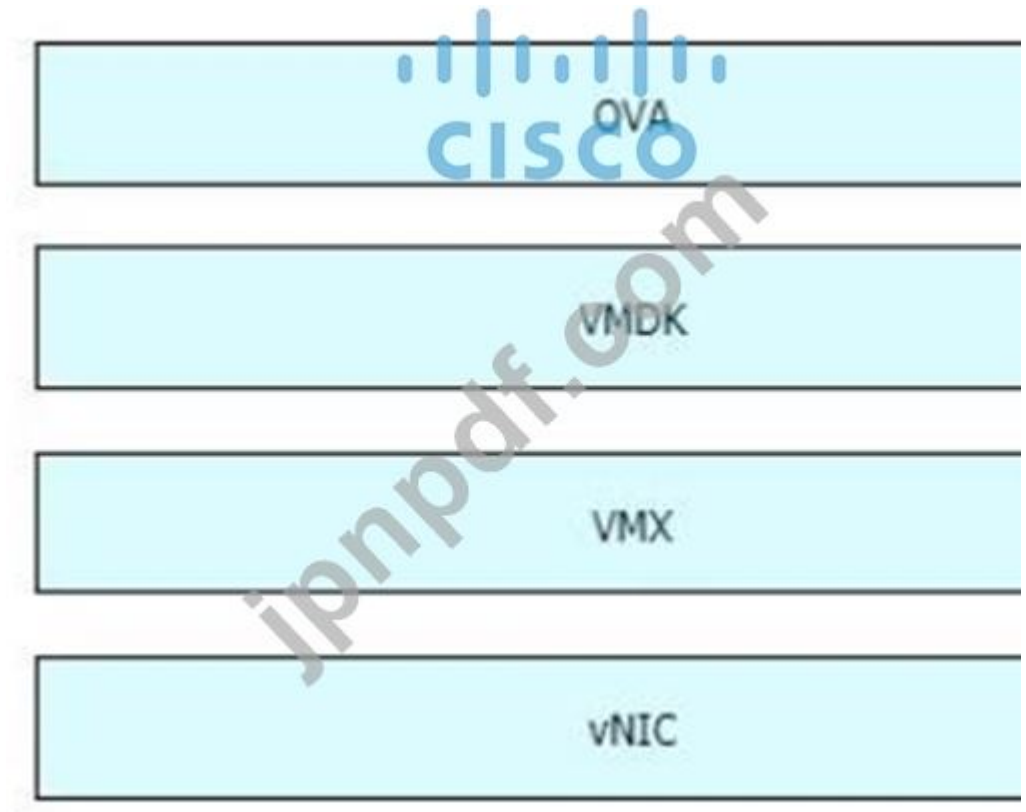
最新問題**: 329**
仮想コンポーネントを左側から右側の欺瞞にドラッグ アンド ドロップします。



Answer:



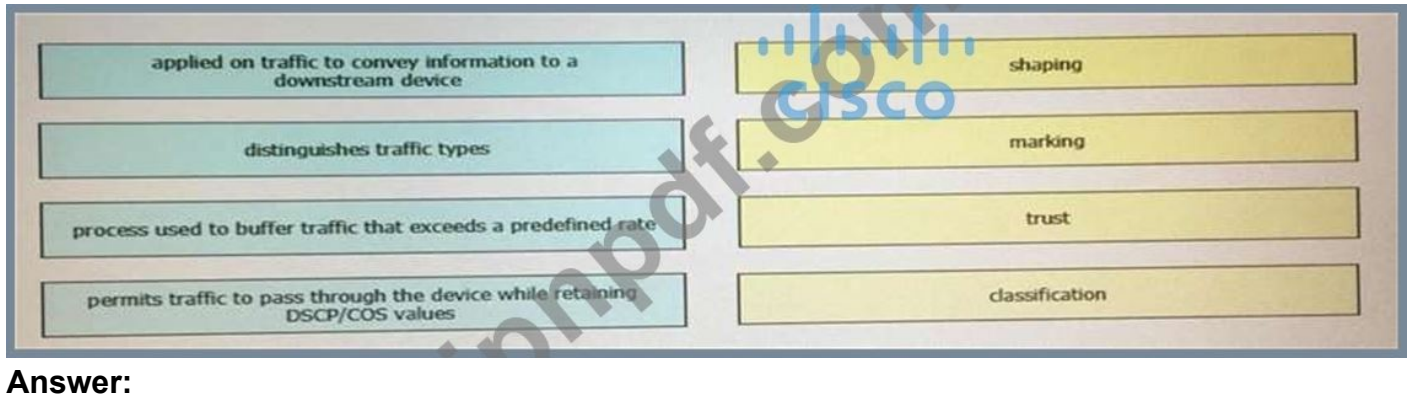
説明



自動生成されたテーブルの説明

最新問題**: 330**

左側の特性を、右側に記述されている QoS コンポーネントにドラッグ アンド ドロップします。

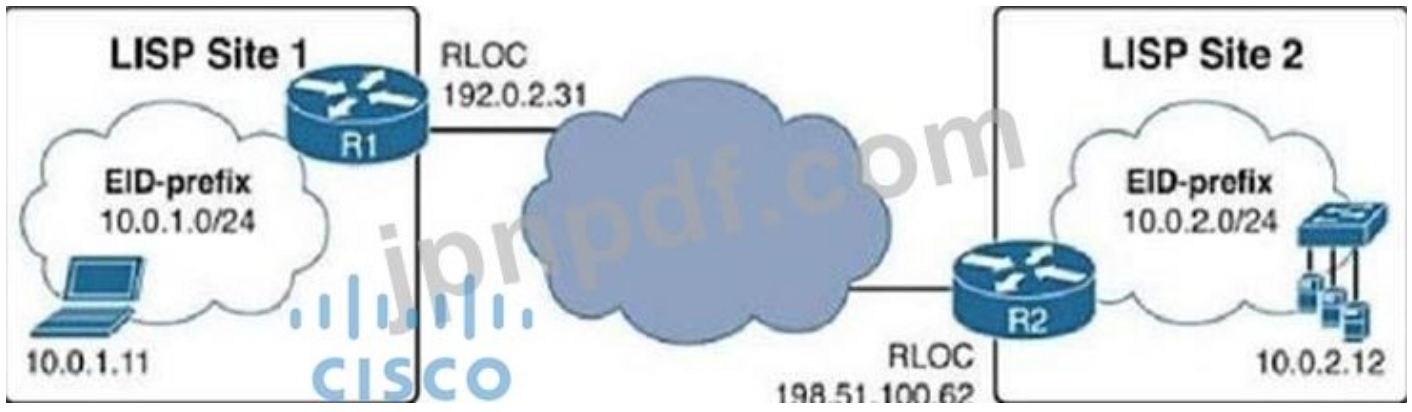


Answer:

説明

マーキング = ダウンストリーム デバイスに情報を伝達するためにトラフィックに適用されます。分類 = トラフィック タイプを区別します。信頼 = DSCP/COS 値を保持しながらデバイスを通過するトラフィックを許可します。

最新問題: **331**
EIGRP OTP 実装における LISP カプセル化について正しいのはどれですか?
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近隣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 Over the Top ソリューションを使用して、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に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) デバイス間のルートを配布するために使用され、WAN アーキテクチャを介して転送されるトラフィックは LISP 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、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、OTP がダイナミック 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は言えません。これには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です。「OTP はダイナミック 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 プロトコルの代わりとして機能します (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 はネクスト ホップを学習する」という回答は正しくありません)。ネイティブの LISP マッピング サービスで動的な EID から RLOC への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 プロバイダーから提供された 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。例を見てみましょう：



R1 と R2 が互いに OTP を実行した場合、R1 は EIGRP を介して 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 を介してネットワーク 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。両方のルーターで、この情報を使用して LISP マッピング テーブルを設定します。
10.0.1.0/24 から 10.0.2.0/24 へのパケットが R1 に到着するときはいつでも、通常の LISP と同様にその LISP マッピング テーブルを使用して、パケットが LISP でカプセル化され、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、ネイティブの LISP マッピングおよび解決メカニズムは EIGRP に置き換えられています。
参照: CCIE Routing and Switching V5.0 公式認定ガイド、第 1 巻、第 5 版

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **332**
ローカル ルーターは、アクティブ状態の EBGP ネイバーを示しています。ローカル ルーターについて正しい説明はどれですか?
A. ローカル ルーターは隣接ルーターとの TCP セッションを開こうとしています。
B. ローカル ルーターには、隣接ルーター用に構成された BGP パッシブ モードがあります。
C. ローカル ルーターは隣接ルーターからプレフィックスを受信し、それらを RIB-IN に追加しています。
D. ローカル ルーターには、隣接ルーターからの転送テーブルにアクティブなプレフィックスがあります。
Answer: A (メーッセージを残す**)**

最新問題: **333**
展示を参照してください。

ネットワーク アーキテクトは、静的 NAT を部分的に構成しました。構成を完了するためにどのコマンドを要求する必要がありますか?
A. R1(config)#interface GigabitEthernet0/0 R1(config)#ip pat inside
R1(config)#interface GigabitEthernet0/1 R1(config)#ip pat outside
B. R1(config)#interface GigabitEthernet0/0 R1(config)#ip pat outside
R1(config)#interface GigabitEthernet0/1 R1(config)#ip pat inside
C. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat outside
R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat inside
D. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat inside
R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat outside
Answer: C (メーッセージを残す**)**

最新問題: **334**
展示を参照してください。

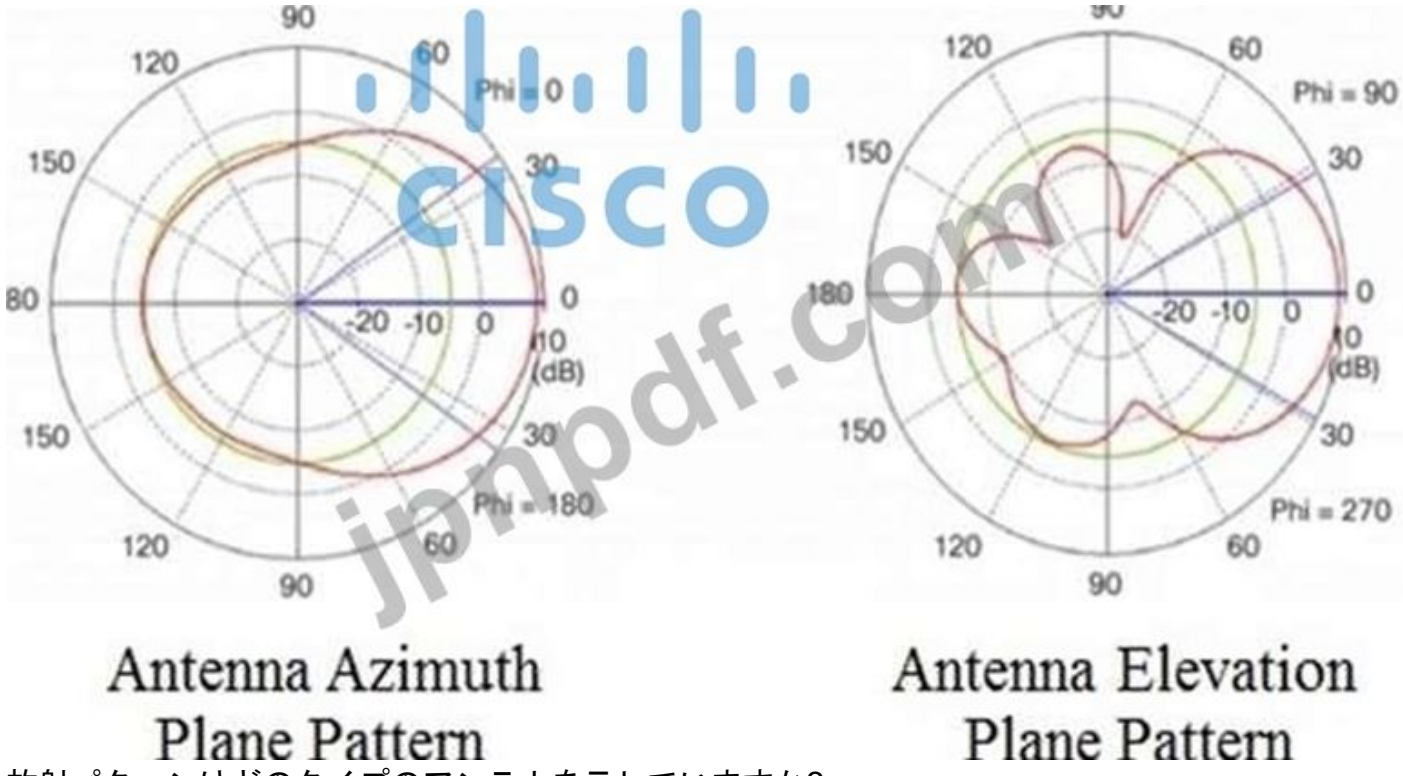
```
R1#debug ip ospf hello
R1#debug condition interface Fa0/1
        Condition 1 Set
```

OPSF デバッグ出力について正しい説明はどれですか?

A. 出力には、ルーター R1 がインターフェイス 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、ルーター R1 がすべてのインターフェー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、ルーター R1 が送信した OSPF hello メッセージがインターフェイス Fa0/1 で受信されたことが表示されます。
D. 出力には、ルーター R1 が送受信した OSPF の hello および LSACK メッセージが表示されます。
Answer: C (メーッセージを残す**)**
このコマンドの組み合わせは 条件付きデバッグ」と呼ばれ、デバッグ出力をフィルタリングします
あなたの条件に基づいて。追加された各条件は、ブール値の And」演算子のように動作します
論理。 debug ip ospf hello」の例を以下に示します。

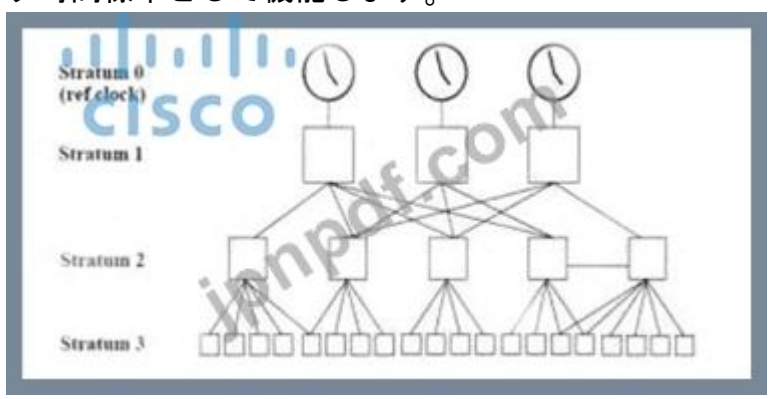
```
*Oct 12 14:03:32.595: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet1/0 from
192.168.12.2
*Oct 12 14:03:33.227: OSPF: Rcv hello from 1.1.1.1 area 0 on FastEthernet1/0 from
192.168.12.1
*Oct 12 14:03:33.227: OSPF: Mismatched hello parameters from 192.168.12.1
```

最新問題: **335**
展示を参照してください。



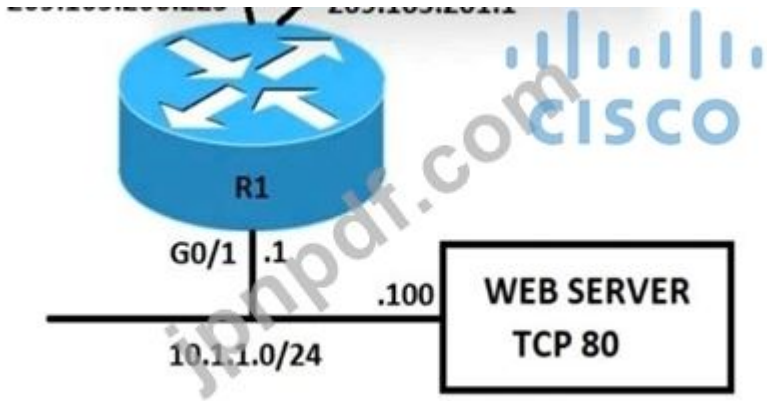
放射パターンはどのタイプのアンテナを示していますか?
A. 八木
B. パッチ
C. 無指向性
D. 双極子
Answer: B (メーッセージを残す**)**
解説 参考 :https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html

最新問題: **336**
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 Stratum レベルですか?
A. ストラタム 0
B. 層 1
C. Stratum 14
D. Stratum 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、それに関連する遅延がほとんどまたはまったくない Stratum 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、コンピュータに直接接続され、Stratum-1 サーバーとして動作します。Stratum 1 タイム サーバーは、主要なネットワーク時間標準として機能します。



Stratum 2 サーバーは Stratum 1 サーバーに接続されています。その後、Stratum 3 サーバーが Stratum 2 サーバーに接続されます。Stratum 2 サーバーは、Stratum 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。層 3 サーバーは、層 2 サーバーからの NTP パケット要求を介して時間を取得します...たとえば、Stratum 2 サーバーは他の Stratum 2 サーバーとピアリングできます)。
NTP は、ストラタムの概念を使用して、ネットワークから NTP ホップがいくつ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。Stratum 1 タイム サーバー
通常、信頼できるタイム ソース (電波時計、原子時計、または全地球測位システム (GPS) タイム ソースなど) が直接接続されており、ストラタム 2 タイム サーバーはストラタム 1 タイム サーバーから NTP を介して時刻を受信します。
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-set.html

最新問題: **337**
展示を参照してください。



エンジニアは、ユーザーが TCP ポート 80 で Web サーバーに HTTP アクセスできるように、R1 で静的 NAT を構成する必要があります。Web サーバーは、ISP 1 および ISP 2 を介して到達可能である必要があります。

A. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 no-alias
ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 no-alias

B. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80 拡張可能
ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80 拡張可能

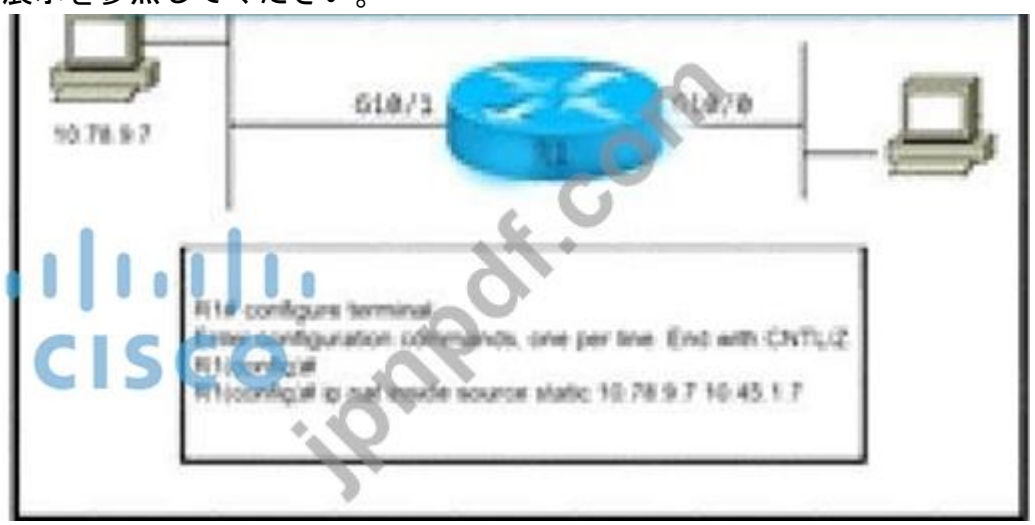
C. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80
ip nat inside source static tcp 10.1.1.100 8080 209.165.201.1 8080

D. ip nat inside source static tcp 10.1.1.100 80 209.165.200.225 80
ip nat inside source static tcp 10.1.1.100 80 209.165.201.1 80

Answer: (解答を表示する**)**

最新問題**: 338**

展示を参照してください。



ネットワーク アーキテクトは、静的 NAT を部分的に構成しました。構成を完了するためにどのコマンドを要求する必要がありますか?

A. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat outside
R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat inside

B. R1(config)#interface GigabitEthernet0/0 R1(config)#ip pat inside
R1(config)#interface GigabitEthernet0/1 R1(config)#ip pat outside

C. R1(config)#interface GigabitEthernet0/0 R1(config)#ip pat outside
R1(config)#interface GigabitEthernet0/1 R1(config)#ip pat inside

D. R1(config)#interface GigabitEthernet0/0 R1(config)#ip nat inside
R1(config)#interface GigabitEthernet0/1 R1(config)#ip nat outside
Answer: A (メーッセージを残す)

最新問題: **339**
ルーターが 100 kbps を受け入れる SSH の量を制限する構成はどれですか?
A)

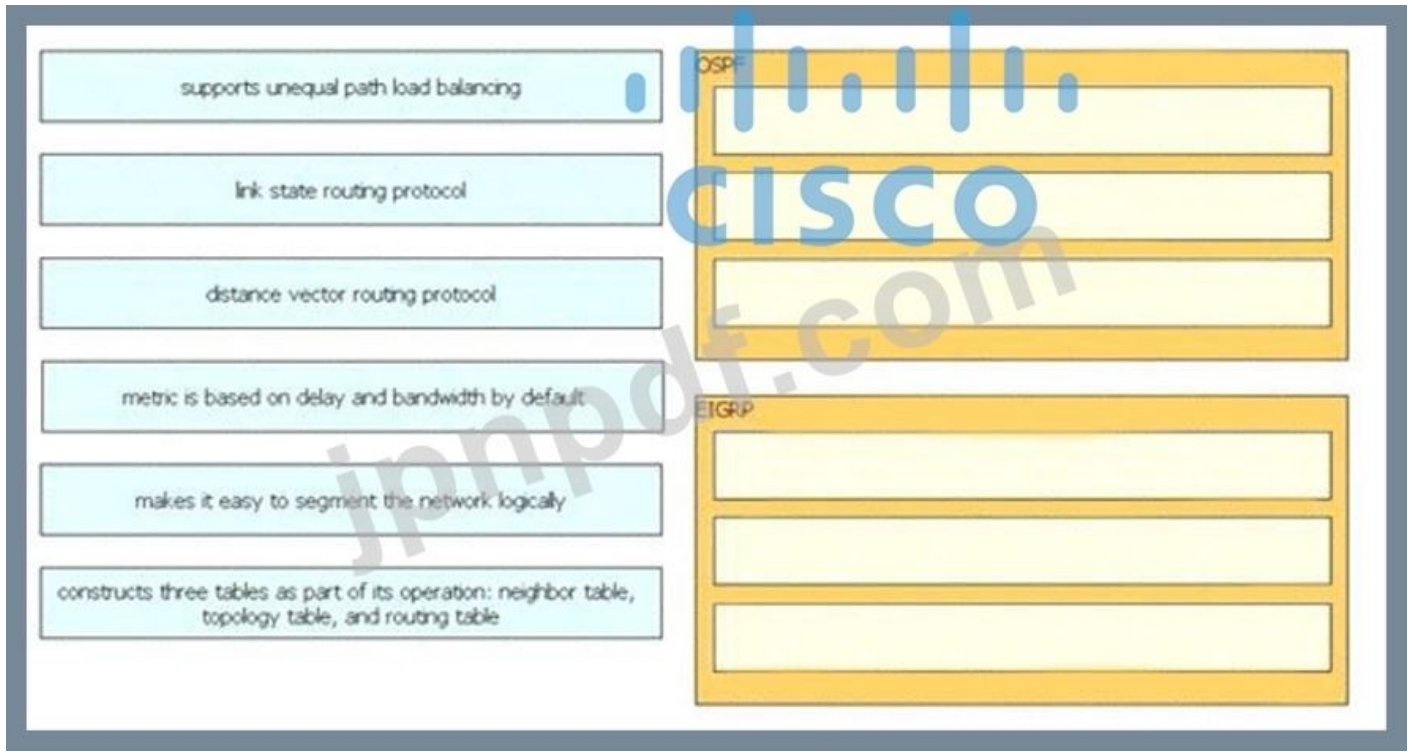
B)

ハ)

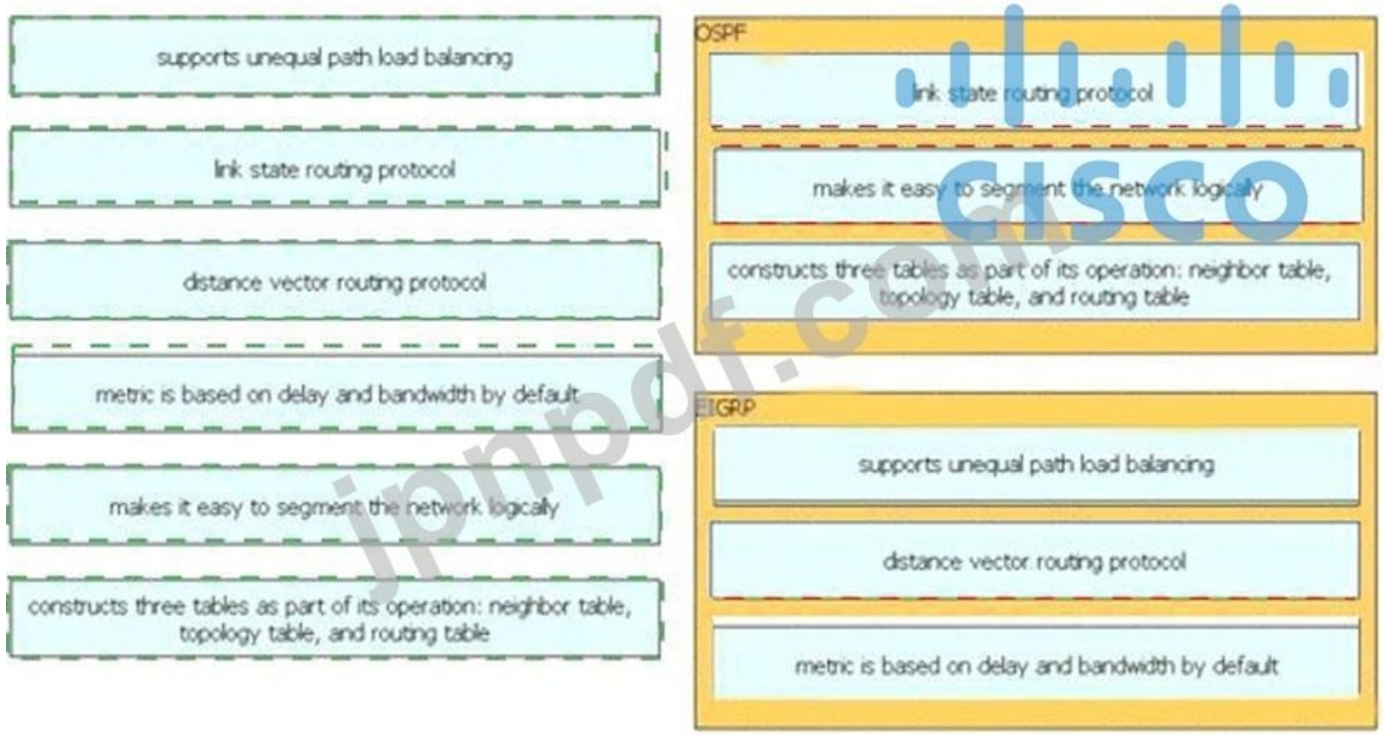
D)

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

最新問題**: 340**
左側の特性を、右側に記述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。

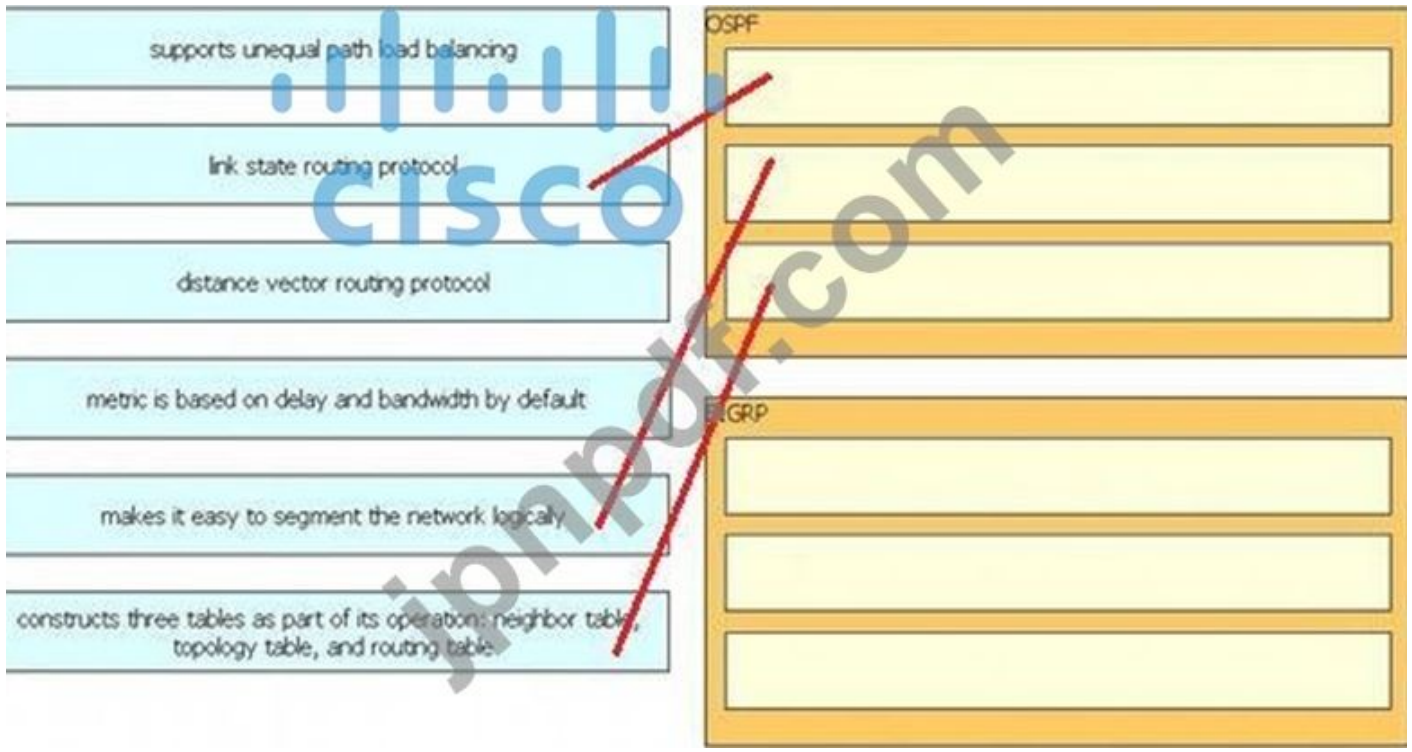


Answer:



説明

図の説明が自動生成される



最新問題: 341

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
MD5 digest                      : 0xE5 0x28 0x5D 0x3E 0x2F 0xE5 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ようにする必要があります。この要件を満たすコマンドはどれですか?

A)

```
SwitchC(config)#vtp pruning
```

B)

```
SwitchC(config)#vtp pruning vlan 110
```

ハ)

```
SwitchC(config)#interface port-channel 1
SwitchC(config-if)#switchport trunk allowed vlan add 210,310
```

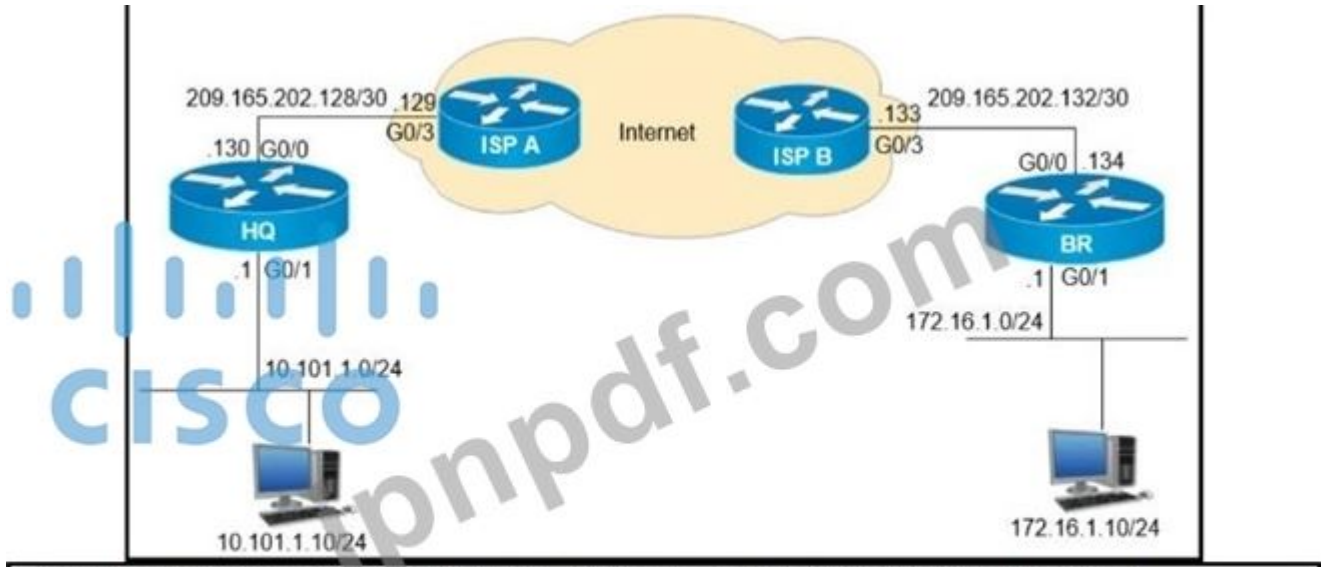
D)

```
SwitchC(config)#interface port-channel 1
SwitchC(config-if)#switchport trunk allowed vlan remove 110
```

jpndf.com

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

最新問題: **342**
展示を参照してください。




```
> Frame 24: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
> Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 50:00:00:02:00:01 (50:00:00:02:00:01)
> Internet Protocol Version 4, Src: 209.165.202.130, Dst: 209.165.202.134
> Generic Routing Encapsulation (IP)
> Internet Protocol Version 4, Src: 10.111.111.1, Dst: 10.111.111.2
> Internet Control Message Protocol
```

HO ルータと BR ルータの間に GRE トンネルが作成されました。
HQ ルーターのトンネル IP は何ですか?
A. 10.111.111.1
B. 10.111.111.2
C. 209.165.202.130
D. 209.165.202.134
Answer: A (メーッセージを残す**)**
上記の出力では、‟209.165.202.130」の IP アドレスがトンネル ソース IP であり、IP 10.111.1.1 がトンネル IP アドレスです。
GRE トンネルの設定例を以下に示します。

cisco
pnpdf.com

R1 (GRE config only)	R2 (GRE config only)
interface s0/0/0 ip address 63.1.27.2 255.255.255.0 **interface tunnel0** **ip address 10.0.0.1 255.255.255.0** **tunnel mode gre ip** //this command can be ignored **tunnel source s0/0** **tunnel destination 85.5.24.10**	interface s0/0/0 ip address 85.5.24.10 255.255.255.0 **interface tunnel1** **ip address 10.0.0.2 255.255.255.0** **tunnel source 85.5.24.10** **tunnel destination 63.1.27.2**

最新問題: **343**

このコードの出力は何ですか?

```
def get_credentials():
    creds={'username': 'cisco', 'password': 'c3577dc8ae4e36c0bfb6fe5398614245'}
    return (creds.get('username'))

print(get_credentials())
```

A. get_credentials

B. シスコ

C. ユーザー名 Cisco

D. ユーザー名

Answer: B (メーッセージを残す**)**

最新問題: **344**

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                      : 0xE5 0x28 0x5D 0x3E 0x2F 0xE5 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ようにする必要があります。この要件を満たすコマンドはどれですか?

A)

```
SwitchC(config)#vtp pruning
```

B)

```
SwitchC(config)#vtp pruning vlan 110
```

ハ）

```
SwitchC(config)#interface port-channel 1
SwitchC(config-if)#switchport trunk allowed vlan add 210,310
```

D)

cisco
jphpdf.com

```
SwitchC(config)#interface port-channel 1
SwitchC(config-if)#switchport trunk allowed vlan remove 110
```

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

最新問題**: 345**
spanning-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 コンバージェンス時間を最小化します。
C. スイッチがリロードされると、すぐにポートをフォワーディング ステートにします。
D. リスニング状態のポートをすぐに有効にします
Answer: B (メーッセージを残す**)**
Port Fast の目的は、インターフェイスがスパニング ツリーのコンバージェンスを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たインターフェイスで使用する場合にのみ有効です。

最新問題**: 346**
Cisco DNA Center テレメトリ機能によって提供される利点はどれですか?
A. ネットワーク構成の展開に役立ちます
B. ユーザー エクスペリエンスを向上させる
C. ネットワーク デバイスのインベントリ
D. 改善されたネットワーク セキュリティを提供します
Answer: (解答を表示する**)**

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら:
https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

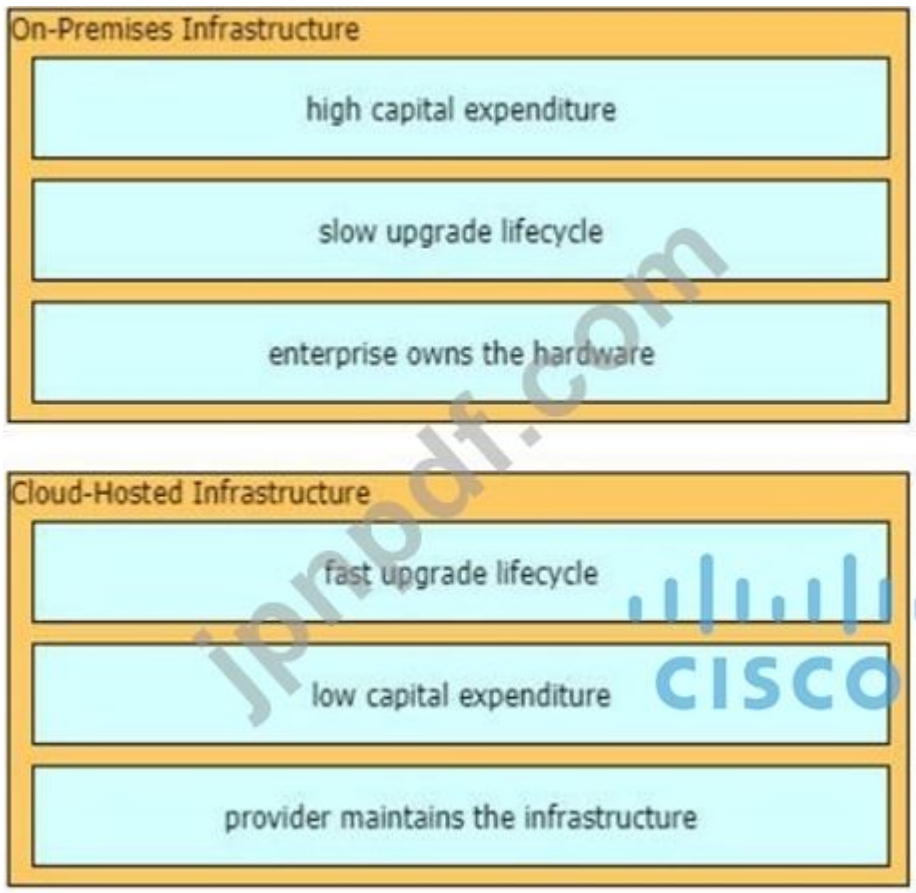
最新問題**: 347**
左側の特性を右側のインフラストラクチャ タイプにドラッグ アンド ドロップします。


enterprise owns the hardware
low capital expenditure
provider maintains the infrastructure
slow upgrade lifecycle
high capital expenditure
fast upgrade lifecycle
On-Premises Infrastructure
Cloud-Hosted Infrastructure

Answer:

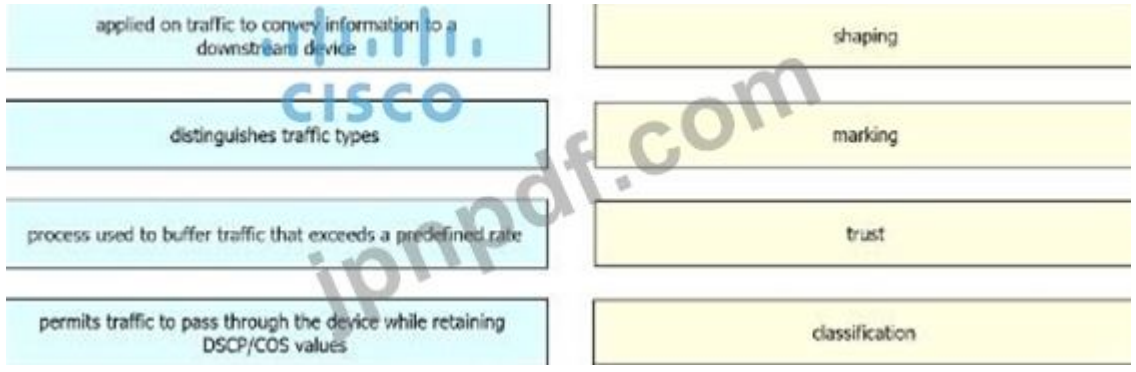

enterprise owns the hardware
low capital expenditure
provider maintains the infrastructure
slow upgrade lifecycle
high capital expenditure
fast upgrade lifecycle
On-Premises Infrastructure
high capital expenditure
enterprise owns the hardware
Cloud-Hosted Infrastructure
fast upgrade lifecycle
low capital expenditure
provider maintains the infrastructure

説明

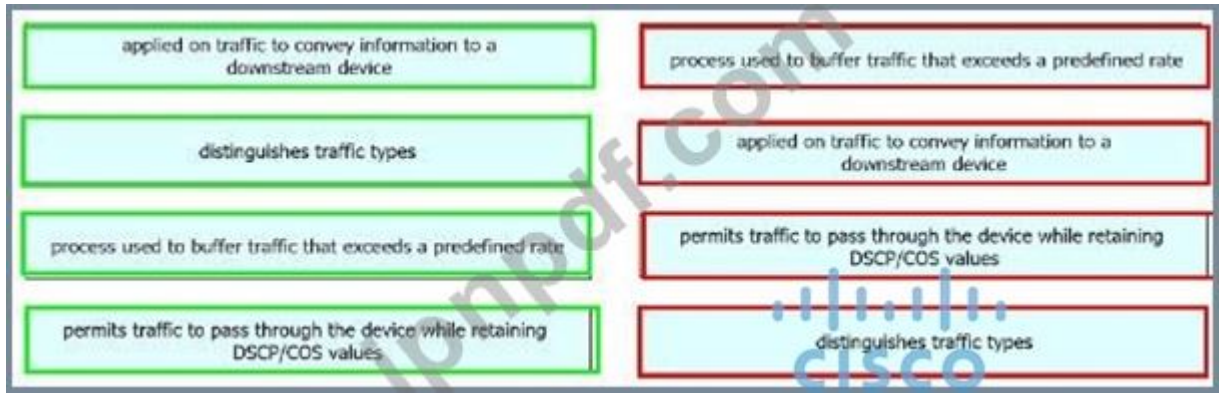


最新問題: **348**

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: **349**

展示を参照してください。

Customer2 のホストが、IP アドレス 192.168.1.200 を持つ Customer1 の FTP サーバーにアクセスできるようにする構成はどれですか?

A. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 グローバル
ip route vrf カスタマー 192.168.1.200 255.255.255.255 192.168.1.1 グローバル
IP ルート 192.168.1.0 255.255.255.0 Vlan10
IP ルート 172.16.1.0 255.255.255.0 Vlan20

B. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer2
IP ルート vrf 顧客 192.168.1.200 255.255.255.255 192.168.1.1 顧客 1

C. ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 Customer1
IP ルート vrf 顧客 192.168.1.200 255.255.255.255 192.168.1.1 顧客 2

D. ip route vrf Customer1 172.16.1.1 255.255.255.255 172.16.1.1 グローバル
ip route vrf カスタマー 192.168.1.200 255.255.255.0 192.168.1.1 グローバル
IP ルート 192.168.1.0 255.255.255.0 Vlan10
IP ルート 172.16.1.0 255.255.255.0 Vlan20

Answer: A (メーッセージを残す)

https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200158-Configure-Route-Leaking-between-Global-a.html
VRF 間の直接スタティック ルートはサポートされていないため、2 つの VRF 間に直接スタティック ルートを設定することはできません。
コマンド 「ip route vrf Customer1 172.16.1.0 255.255.255.0 172.16.1.1 global」は、宛先 172.16.1.0/24 に到達するために、VRF Customer1 でグローバル ルーティング テーブルのネクスト ホップ IP アドレス 172.16.1.1 を使用することを意味します。また、コマンド 「ip route 192.168.1.0 255.255.255.0 Vlan10」は、ルーターに 「192.168.1.0/24 に到達し、Vlan 10 に送信する」ように指示します。

最新問題: **350**
RSPAN セッション構成について正しい説明はどれですか?

A. RSPAN リージョン用に構成されたフィッター mutt

B. 一度に設定できるセッションは 1 つだけです

C. RSPAN 宛先として特別な VLAN タイプを使用する必要があります。

D. 着信トラフィックのみを監視できます

Answer: (解答を表示する)

各 RSPAN セッションのトラフィックは、参加しているすべてのスイッチでその RSPAN セッション専用のユーザ指定の RSPAN VLAN を介して伝送されます -> この VLAN は特別な VLAN タイプと見なすことができます -> 回答 「特別な VLAN タイプを RSPAN として使用する必要があります」行先」が正しいです。

最新問題: **351**

Cisco DNA Center が提供する Intent API を定義する 2 つの特徴はどれですか？ 2つ選んでください。）
A. ノースバウンド API
B. ビジネス成果志向
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**)**

The Intent API is a *Northbound* REST API that exposes specific capabilities of the Cisco DNA Center platform.
The Intent API provides policy-based abstraction of business intent, allowing focus on an outcome rather than struggling with individual mechanisms steps.

最新問題**: 352**
ワイヤレス コントローラとスイッチ間のリンクの合計スループットと冗長性を向上させるために、お客様はワイヤレス コントローラで LAG を有効にしました。WLC が接続できるようにするには、スイッチでどの EtherChannel モードを設定する必要がありますか?
A. オート
B. アクティブ
C. オン
D. パッシブ
Answer: C (メーッセージを残す**)**
リンク アグリゲーション (LAG) は、802.3ad ポート アグリゲーション標準の部分的な実装です。コントローラのすべてのディストリビューション システム ポートを単一の 802.3ad ポート チャネルにバンドルします。
リンクアグリゲーションの制限:
+ LAG では、コントローラと Catalyst スイッチの両方で EtherChannel を 「モード オン」に設定する必要があります。...

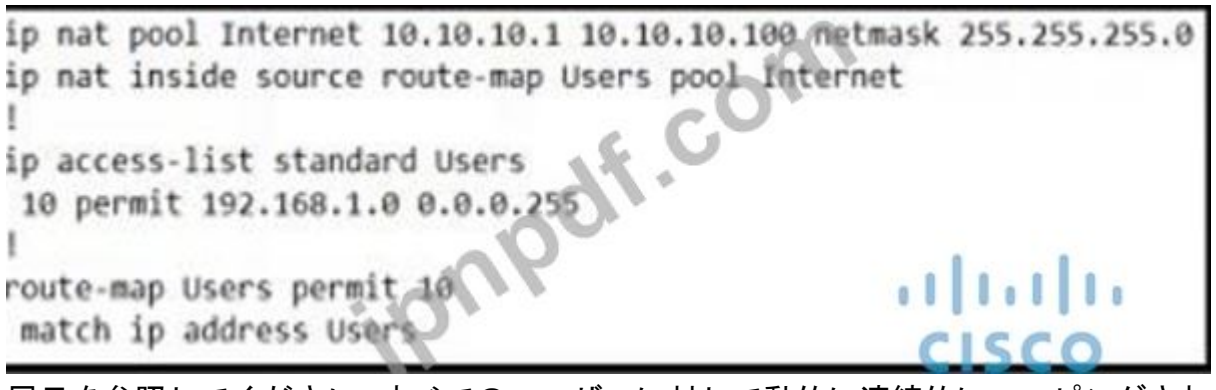
最新問題**: 353**
展示を参照してください。

```
vlan 222
 remote-span
!
vlan 223
 remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

技術者が monitor session 1 destination remote vlan 233 コマンドを追加すると、どのような結果になりますか?
A. RSPAN トラフィックは VLAN 222 および 223 に送信されます。
B. 2 つの宛先を構成するためにエラーがフラグ付けされます。
C. RSPAN トラフィックは、VLAN 222 と 223 の間で分割されます。
D. RSPAN VLAN は VLAN 223 に置き換えられます。

Answer: (解答を表示する)

最新問題: **354**



展示を参照してください。すべてのユーザーに対して動的に連続的にマッピングされた NAT を実現するための構成を完了するアクションはどれですか?

A. 192.168 1 0 アドレス範囲を使用するようにプールを再構成します

B. 1 対 1 型の NAT プールを構成する

C. match-host タイプの NAT プールを構成する

D. NAT プール サイズを増やして、254 の使用可能なアドレスをサポートします。

Answer: (解答を表示する)

最新問題: **355**

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に、[Clients] > [Detail] で設定された Mobility Role Anchor があ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 3 インターコントローラ

B. コントローラー内

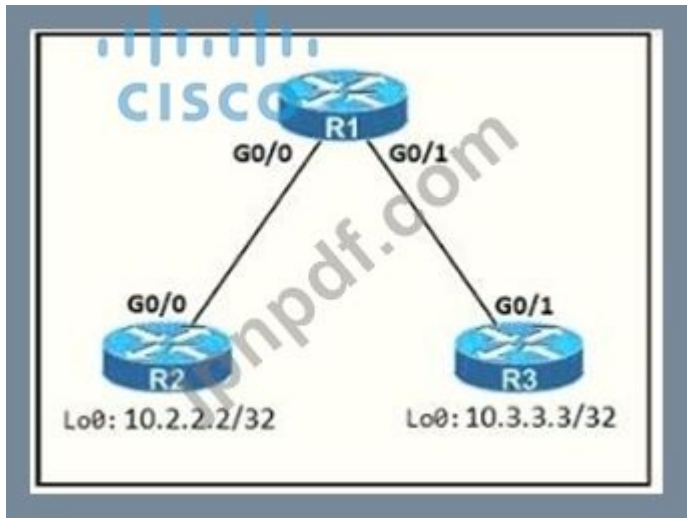
C. 間接

D. レイヤー 2 インターコントローラー

Answer: A (メーッセージを残す)

最新問題: **356**

展示を参照してください。



エンジニアは、週末の時間帯にルーター R3 のループバック インターフェイスからルーター R2 のループバック インターフェイスへの Telnet トラフィックを拒否する必要があります。ルーター R3 と R2 のループバック インターフェイス間の他のすべてのトラフィックは、常に許可する必要があります。このタスクを実行するコマンドはどれですか?

A)

```
R3(config)#time-range WEEKEND
R3(config-time-range)#periodic Saturday Sunday 00:00 to 23:59

R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R3(config)#access-list 150 permit ip any any time-range WEEKEND

R3(config)#interface G0/1
R3(config-if)#ip access-group 150 out
```

B)

```
R1(config)#time-range WEEKEND
R1(config-time-range)#periodic Friday Sunday 00:00 to 00:00

R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R1(config)#access-list 150 permit ip any any

R1(config)#interface G0/1
R1(config-if)#ip access-group 150 in
```

ハ)

```
R1(config)#time-range WEEKEND
R1(config-time-range)#periodic weekend 00:00 to 23:59

R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R1(config)#access-list 150 permit ip any any

R1(config)#interface G0/1
R1(config-if)#ip access-group 150 in
```

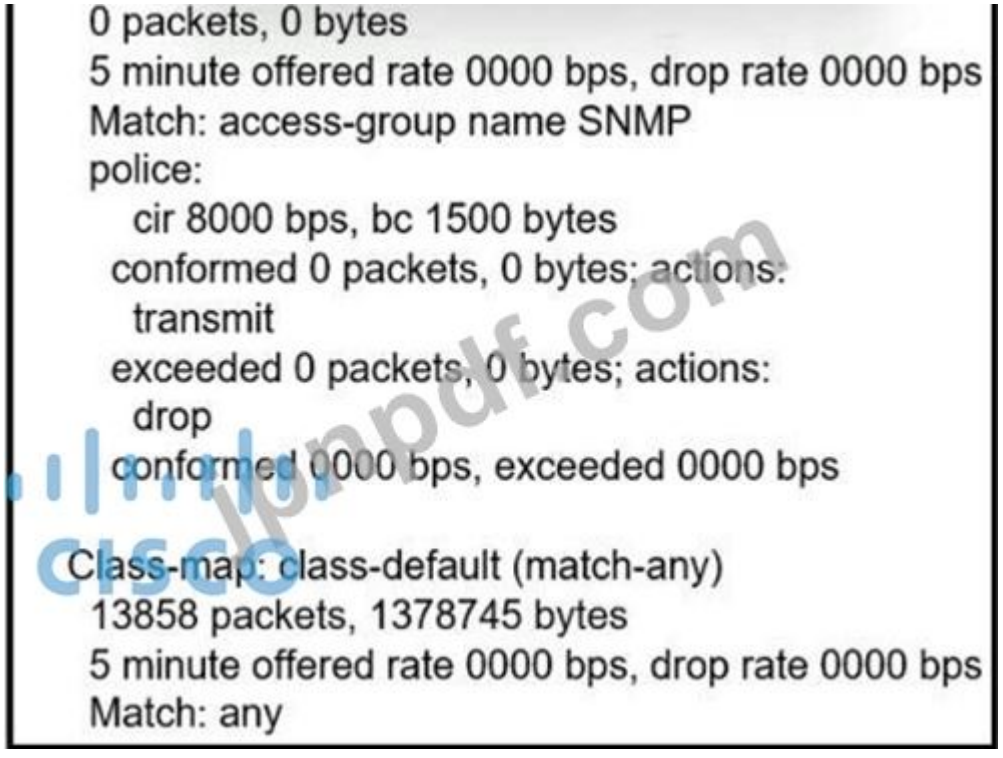
D)

```
R3(config)#time-range WEEKEND
R3(config-time-range)#periodic weekend 00:00 to 23:59

R3(config)#access-list 150 permit tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND
R3(config)#access-list 150 permit ip any any time-range WEEKEND

R3(config)#interface G0/1
R3(config-if)#ip access-group 150 out
```

A. オプション A

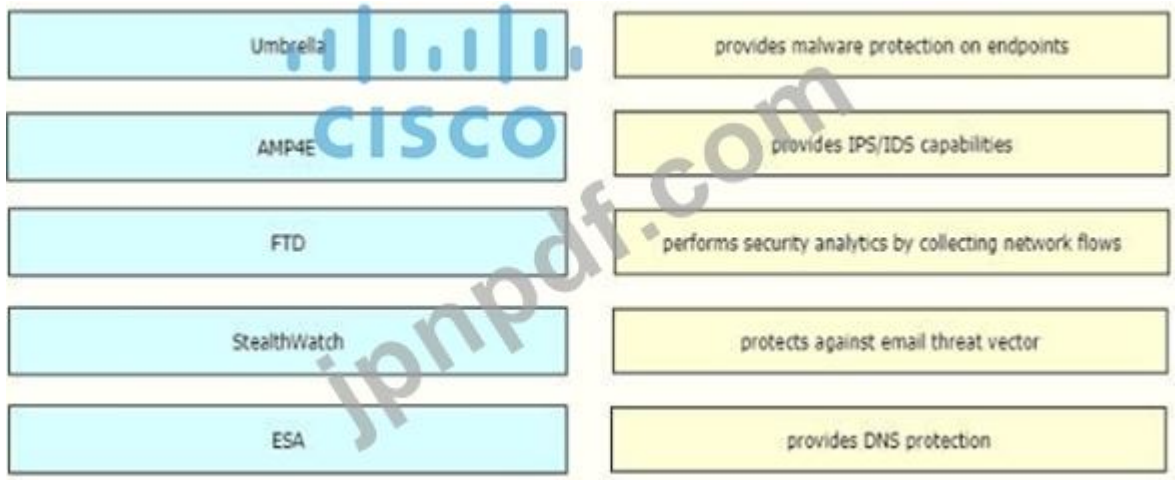
B. オプション B
C. オプション C
D. オプション D
Answer: (解答を表示する**)**
ローカル ルータ (この場合は R3)から発信されたトラフィックをフィルタリングできないため、
R1 または R2 でのみ ACL を設定できます。 週末営業時間」とは、土曜日からという意味です
朝から日曜の夜まで、次のように構成する必要があります: 定期的な週末 00:00
23時59分まで」。
注: 時間は 24 時間制 (hh:mm) で指定されます。時間の範囲は 0 からです。
から 23 まで、分の範囲は 0 から 59 までです。

最新問題**: 357**
展示を参照してください。



CoPP ポリシーがルーターに設定された後、ルーターはトラフィックをどのように処理しますか?
A. アクセス リスト SNMP に一致する R1 を通過するトラフィックがポリシングされます。
B. アクセス リスト SNMP に一致しない R1 に着信するトラフィックはドロップされます。
C. アクセス リスト SNMP に一致する R1 によって生成されたトラフィックがポリシングされます。
D. アクセス リスト SNMP に一致する R1 に着信するトラフィックがポリシングされます。
Answer: A (メーッセージを残す**)**

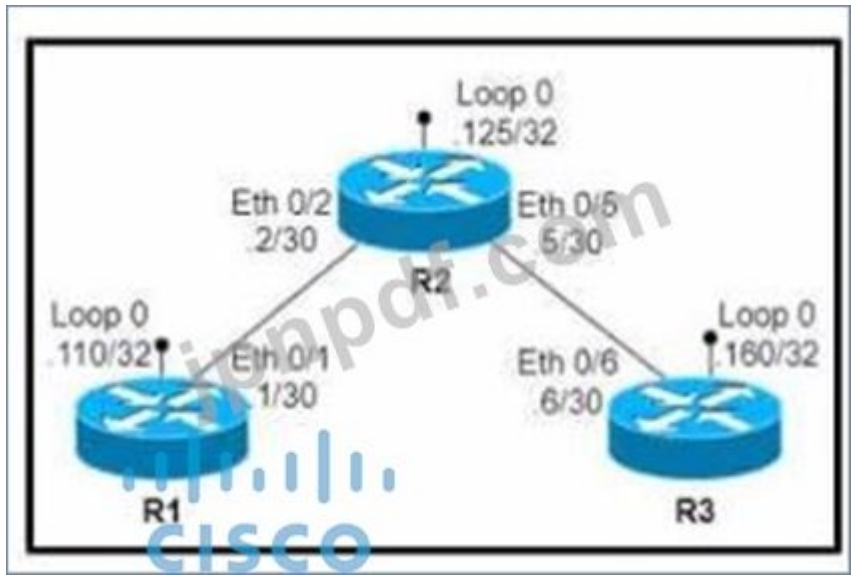
最新問題**: 358**
脅威防御ソリューションを左側から右側の説明にドラッグ アンド ドロップします。



Answer:

最新問題: **359**

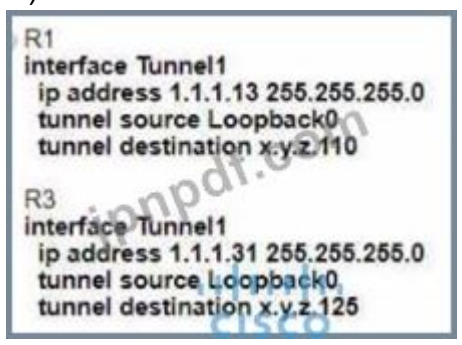
展示を参照してください。



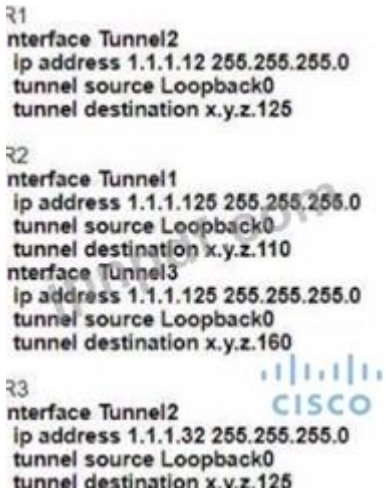
エンジニアは、すべてのルーター間のルーティングを構成し、GRE トンネル経由で R1 を R3 に接続する構成を構築する必要があります。どの構成を適用する必要がありますか?

A)

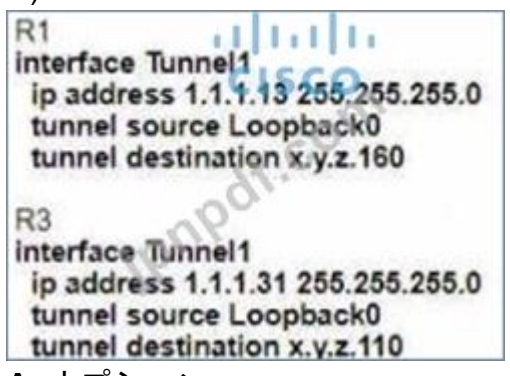
B)



ハ)



D)



A. オプション

B. オプション

C. オプション

D. オプション

Answer: (解答を表示する)

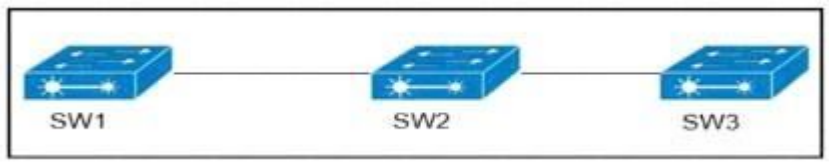
最新問題: **360**

ファブリック アクセス ポイントについて正しいのはどれですか?
A. ローカル モードであり、ファブリック エッジ スイッチに直接接続する必要があります。
B. ローカル モードであり、ファブリック ボーダー ノードに直接接続する必要があります。
C. FlexConnect モードであり、ファブリック ボーダー ノードに直接接続する必要があります。
D. FlexConnect モードであり、ファブリック エッジ スイッチに直接接続する必要があります。
Answer: (解答を表示する**)**
解説 参考 :https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.html

最新問題**: 361**
Cisco DNA Center で REST API を使用して次の URI に POST を実行しているときに、404 の応答コードが受信されます。
/dna/intent/api/v1/template-programmer/project
コードの意味は何ですか？
A. POST/PUT 要求が実行され、新しいリソースが作成されました。リソースに関する情報は、応答本文にあります。
B. 処理は受け付けられましたが、処理が完了していません。
C. クライアントは、存在しないリソースを要求しました。
D. サーバーは、要求を満たすために必要な機能を実装していません。
Answer: C (メーッセージを残す**)**
説明
解説 参考 :https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/application-policy-infrastructure-controller-enterprise-module/1-2-x/config- guide/b_apic-em_config_guide_v_1-2-x/b_apic-em_config_guide_v_1-2-x_chapter_01001.html

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード**: Freepdfdumps**)

最新問題**: 362**
出品物参照。



VLAN 50 および 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、SW1 は VTP サーバです SW3 が VLAN からのみフレームを受信することを保証するコマンド
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**)**

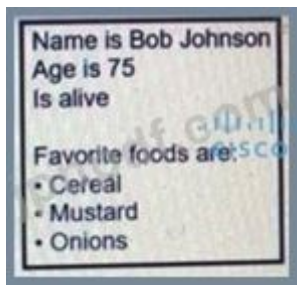
説明
SW3 には VLAN 60 がないため、この VLAN のトラフィック (SW2 から送信) を受信しないはずです。
したがって、SW2 が VLAN 60 トラフィックを SW3 に転送しないように、SW3 で VTP プルーニングを設定する必要があります。また、SW2 ではなく SW1 (VTP サーバ) でプルーニングを設定する必要があることにも注意してください。

最新問題: **363**
エンジニアがルーターのログを確認し、次のエントリを発見しました。イベントのログの重大度レベルは?

A. 情報提供
B. 警告
C. エラー
D. 通知
Answer: C (メーッセージを残す**)**

最新問題: **364**
タイプ 1 ハイパーバイザーとは何ですか?
A. 物理サーバー上で直接実行され、以前にインストールされたオペレーティング システムに依存します
B. 物理サーバー上で直接実行され、独自のオペレーティング システムが含まれます
C. 仮想サーバー上で実行され、既にインストールされているオペレーティング システムに依存します。
D. 仮想サーバー上で実行され、独自のオペレーティング システムが含まれます
Answer: B (メーッセージを残す**)**
説明
ハイパーバイザーには、タイプ 1 ハイパーバイザーとタイプ 2 ハイパーバイザーの 2 種類があります。
タイプ 1 ハイパーバイザー (またはネイティブ ハイパーバイザー) では、ハイパーバイザーは物理サーバーに直接インストールされます。次に、オペレーティング システム (OS) のインスタンスがハイパーバイザーにインストールされます。タイプ 1 ハイパーバイザーは、ハードウェア リソースに直接アクセスできます。したがって、ホストされたアーキテクチャよりも効率的です。タイプ 1 ハイパーバイザーの例としては、VMware vSphere/ESXi、Oracle VM Server、KVM、および Microsoft Hyper-V があります。
タイプ 1 ハイパーバイザーとは対照的に、タイプ 2 ハイパーバイザー (またはホスト型ハイパーバイザー) は、物理ハードウェアではなく、オペレーティング システム上で実行されます。タイプ 2 ハイパーバイザーの大きな利点は、管理コンソール ソフトウェアが必要ないことです。タイプ 2 ハイパーバイザーの例としては、VMware Workstation (Windows、Mac、および Linux で実行可能) または Microsoft Virtual PC (Windows でのみ実行) があります。

最新問題: **365**
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. {"~Name': "~Bob Johnson', "~Age': 75, "~Alive': True, "~Favorite Foods': "~Cereal', "~Mustard', "~Onions' }
B. {名前: ボブ ·ジョンソン、年齢: 75歳、生存: true、好きな食べ物: [シリアル、マスタード、タマネギ]}
C. {"Name": "Bob Johnson", "Age": Seventyfive, "Alive": true, "Favorite Foods": ["Cereal", "Mustard", "玉ねぎ"]}
D. {"Name": "Bob Johnson", "Age": 75, "Alive": true, "Favorite Foods": ["Cereal", "Masterd", "Onions"]}
Answer: D (メーッセージを残す**)**

最新問題**: 366**
ログ ファイルの日付の横に * が含まれるのはなぜですか?
A. ネットワーク デバイスは、ログに NTP タイム スタンプを使用するように構成されていません。
B. ログ メッセージが記録されたときに、ネットワーク デバイスが NTP サーバーに到達できませんでした。
C. ネットワーク デバイスが NTP を使用するように構成されていません
D. ログ メッセージが記録されたときにネットワーク デバイスが NTP 時刻を受信していた
Answer: C (メーッセージを残す**)**

最新問題**: 367**
展示を参照してください。

```
vlan 222
 remote-span
!
vlan 223
 remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

jpdf.com
CISCO

技術者がモニター セッション 1 宛先リモート vlan 223 コマンド 1 を追加すると、どのような結果になりますか?
A. 2 つの送信先を構成するとエラーが発生します。
B. RSPAN トラフィックは VLAN 222 および 223 に送信されます。
C. RSPAN VLAN は VLAN 223 に置き換えられます。
D. RSPAN トラフィックは、VLAN 222 と 223 の間で分割されます。
Answer: C (メーッセージを残す**)**

最新問題**: 368**
HSRP に関する 2 つの記述のうち、正しいものはどれですか? 2つ選んでください。）
A. 仮想 MAC は 0000.0C07.Acxx です。
B. マルチキャスト仮想 MAC は 0000.5E00.01xx です。

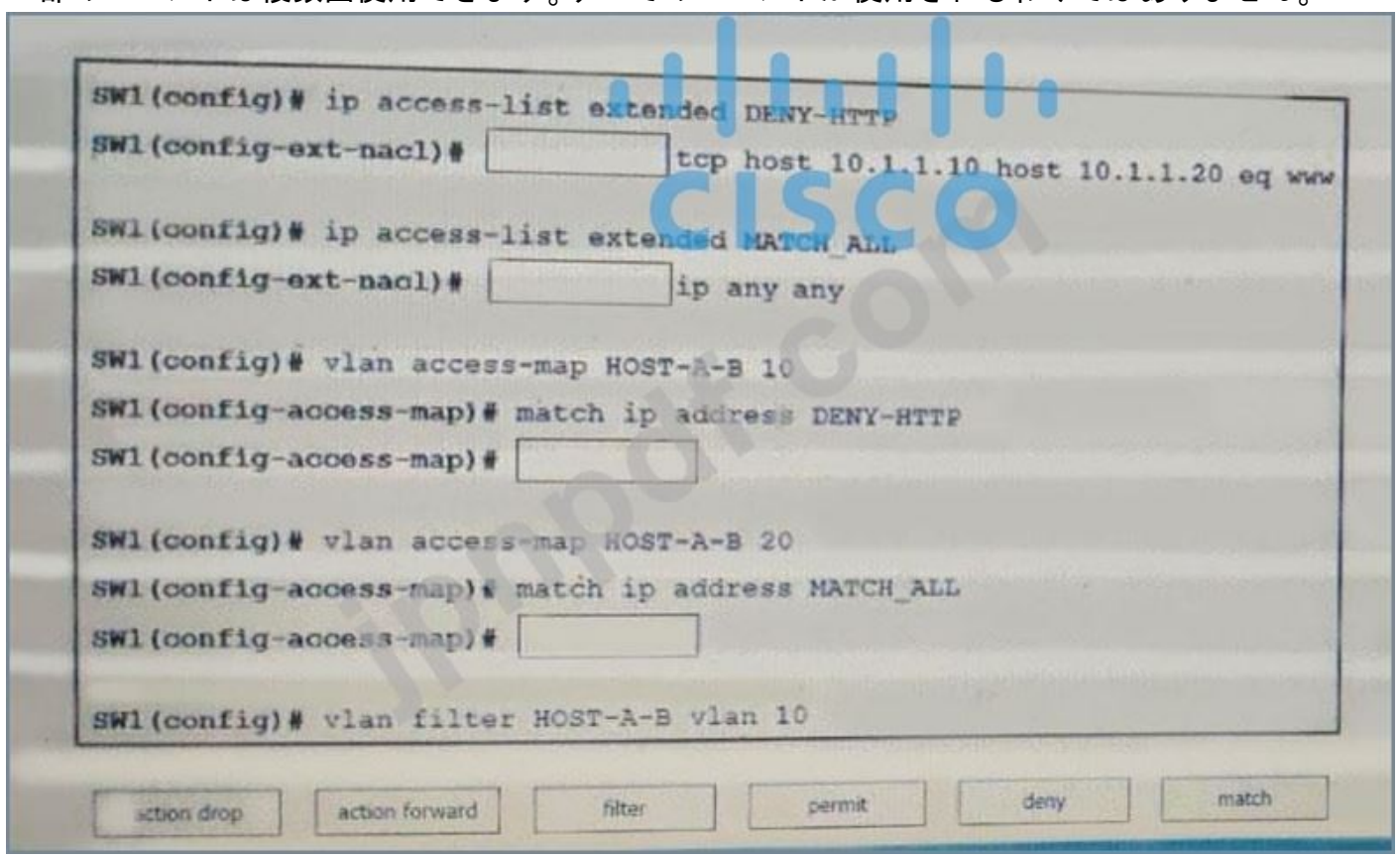
C. デフォルト設定ではプリエンプションが可能です。
D. トラッキングをサポートします。
E. 一意の仮想 MAC アドレスをサポートします。
Answer: A,D (メーッセージを残す**)**
HSRP バージョンを変更すると、Cisco NX-OS は新しい仮想 MAC アドレスを持つようになったため、グループを再初期化します。HSRP バージョン 1 は MAC アドレス範囲 0000.0C07.ACxx を使用し、HSRP バージョン 2 は MAC アドレス範囲 0000.0C9F.F0xx を使用します。
HSRP はインターフェイス トラッキングをサポートしています。これにより、特定のグループの HSRP プライオリティを変更するために、HSRP プロセスが監視するルータ上の別のインターフェイスを指定できます。

最新問題**: 369**
IP アドレス 10.10.10.1 のワークステーションから発信された http トラフィックを除くすべてのトラフィックを許可する、ルーターの WAN インターフェイスに適用されるアウトバウンド アクセス リストはどれですか?
A. ip access-list 拡張 10
拒否 TCP ホスト 10.10.10.1 任意の eq 80
IP を許可する
B. ip access-list 拡張 NO_HTTP
拒否 TCP ホスト 10.10.10.1 任意の eq 80
C. ip access-list 拡張 100
拒否 TCP ホスト 10.10.10.1 任意の eq 80
IP を許可する
D. ip access-list 拡張 200
拒否 tcp ホスト 10.10.10.1 eq 80 任意
IP を許可する
Answer: C (メーッセージを残す**)**

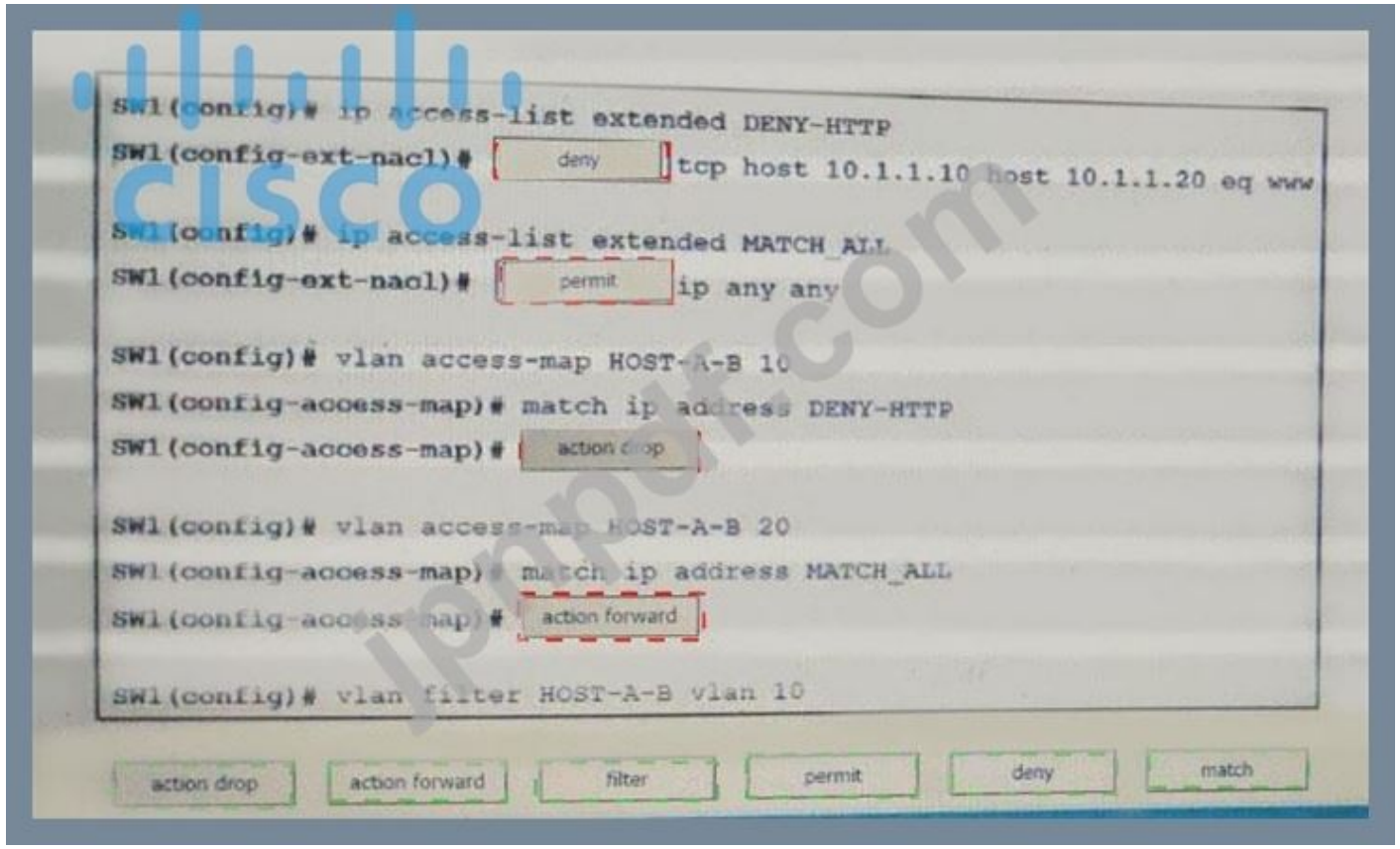
最新問題**: 370**


展示を参照してください。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する必要があります。これらの結果を得るには、コマンドを構成にドラッグ アンド ドロップします。

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:



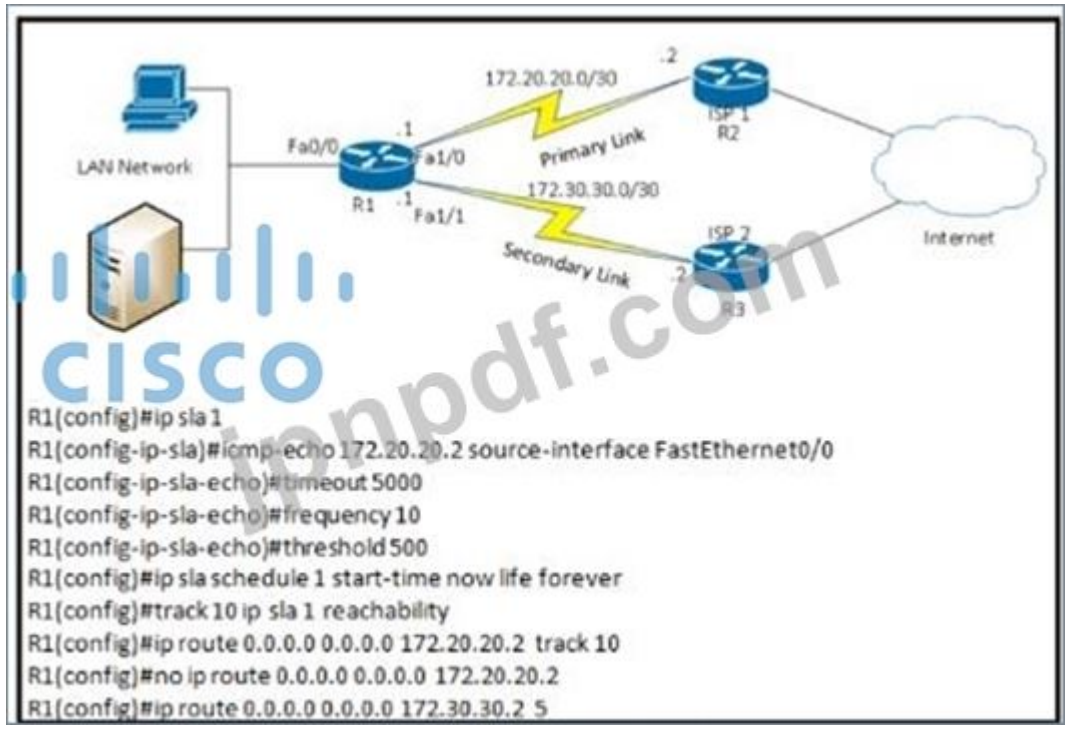
説明

拒否

許可

アクションドロップ
アクションフォワード

最新問題: **371**
展示を参照してください。

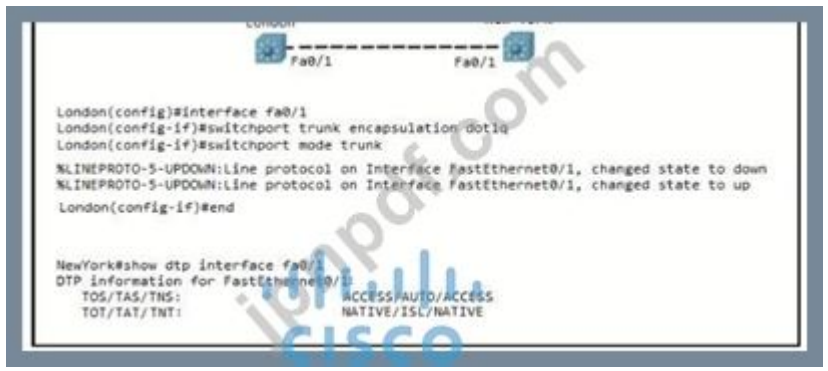


IP SLA トラッキングが失敗する 2 つの理由は何ですか? (2つ選択)
A. ソース インターフェイスが正しく構成されていません。
B. icmp-echo の宛先は 172 30 30 2 でなければなりません
C. しきい値が間違っています
D. デフォルト ルートのネクスト ホップ IP アドレスが正しくありません
E. R1 LAN ネットワークに戻るルートが R2 にありません。
Answer: C,E (メーッセージを残す)

最新問題: **372**
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 ノードとは何ですか?
A. ポリシーの適用とファブリック内のネットワーク セグメンテーションを担当します。
B. ファブリック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。
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. 従来の非ファブリック対応環境との統合を提供します。
Answer: C (メーッセージを残す)
ファブリック コントロール プレーン ノード (C): LISP Map-Server (MS) および Map-Resolver (MR) 機能を実装する 1 つ以上のネットワーク要素。コントロール プレーン ノードのホスト トラッキング データベースは、ファブリック サイト内のすべてのエンドポイントを追跡し、LISP で EID-to-RLOC バインディングとして知られている方法でエンドポイントをファブリック ノードに関連付けます。

最新問題: **373**

展示を参照してください



ロンドンとニューヨーク間の通信がダウンしています。この問題を解決するには、どのコマンド セットを適用する必要がありますか?

A)

```
NewYork(config)#int f0/1
NewYork(config)#switchport trunk encap dot1q
NewYork(config)#end
NewYork#
```

B)

```
NewYork(config)#int f0/1
NewYork(config)#switchport mode trunk
NewYork(config)#end
NewYork#
```

ハ）

```
NewYork(config)#int f0/1
NewYork(config)#switchport nonegotiate
NewYork(config)#end
NewYork#
```

D)

```
NewYork(config)#int f0/1
NewYork(config)#switchport mode dynamic desirable
NewYork(config)#end
NewYork#
```

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: A (メーッセージを残す)

最新問題: **374**

ネットワーク エンジニアは、コア スイッチへの HTTPS アクセスを有効にしています。これには、企業の認証局によって署名された証明書をスイッチにインストールする必要があります。コア スイッチから証明書署名要求を発行するには、どの構成コマンドが必要ですか?

A)

```
Core-Switch(config)#crypto pki enroll Core-Switch
Core-Switch(config)#ip http secure-trustpoint Core-Switch
```

B)

```
Core-Switch(config)#crypto pki trustpoint Core-Switch
Core-Switch(ca-trustpoint)#enrollment terminal
Core-Switch(config)#crypto pki enroll Core-Switch
```

ハ）

```
Core-Switch(config)#crypto pki trustpoint Core-Switch
Core-Switch(ca-trustpoint)#enrollment terminal
Core-Switch(config)#ip http secure-trustpoint Core-Switch
```

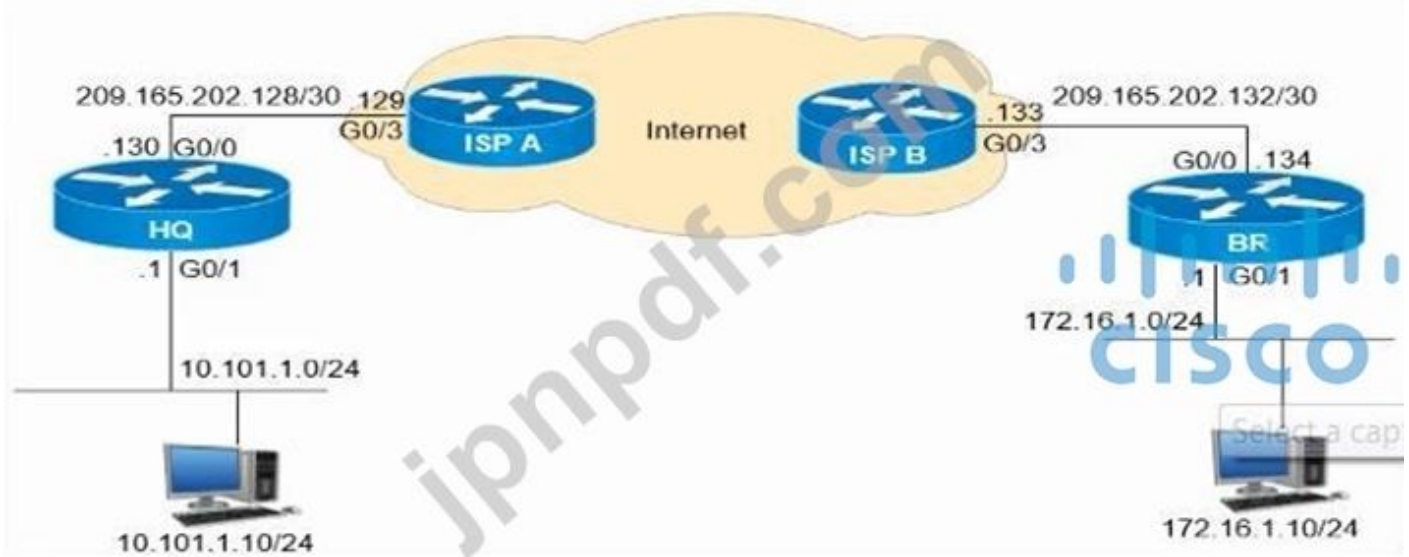
D)

```
Core-Switch(config)#ip http secure-trustpoint Core-Switch
Core-Switch(config)#crypto pki enroll Core-Switch
```

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**)**

認証局 (CA) は、証明書要求を管理し、参加している IPSec ネットワーク デバイスに証明書を発行する責任があります。これらのサービスは、参加デバイスのセキュリティ キーと証明書の集中管理を提供します。特定の CA サーバは「トラストポイント」と呼ばれます。コマンド「crypto pki trustpoint name」は、トラストポイントと特定の名前を宣言し、ca-trustpoint コンフィギュレーション モードに入ります。コマンド「登録端末」は、手動のカットアンドペースト証明書登録方法を指定します。コンソール端末に証明書要求が表示されるので、手動でコピー (またはカット) できます。コマンド「crypto pki enroll name」は、証明書要求を生成し、証明書サーバーにコピー アンド ペーストするための要求を表示します。完全な構成は、以下のリファレンスに示されています。参照:
https://www.cisco.com/c/en/us/td/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/convert/sec_pki_xe_3s_book/sec_cert_enroll_pki_xe.html

最新問題**: 375**
展示を参照してください。



HQ ルーターと BR ルーターの間に GRE トンネルを設定するには、HQ ルーターにどの構成を適用する必要がありますか?

A)

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.134
```

B)

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.133
```

ハ）

```
interface Tunnel1
 ip address 10.111.111.1 255.255.255.0
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

D)

```
interface Tunnel1
 ip address 209.165.202.130 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.202.129
```

A. オプション C

B. オプション A

C. オプション D

D. オプション B

Answer: B (メーッセージを残す)

最新問題**: 376**

展示を参照してください。

```
PUBLIC IP                              PORT  LOCAL COLOR     PROXY STATE UPTIME      ID
-------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------
------
vsmart  dtls 4.4.4.70          100       1      192.168.100.80
12446 10.10.20.70                              12446 default         No    up
0:02:24:09  0
vbond   dtls 0.0.0.0           0         0      192.168.100.81
12346 10.10.20.80                              12346 default         -     up
0:02:24:10  0
vmanage dtls 4.4.4.90          100       0      192.168.100.82
12446 10.10.20.90                              12446 default
```

認証の問題を解決するには、どの手順を実行しますか?

A. 基本認証を使用

B. vsmart ホストを再起動します。

C. ポートを 12446 に変更します

D. URI のターゲット 192 168 100 82

Answer: (解答を表示する)

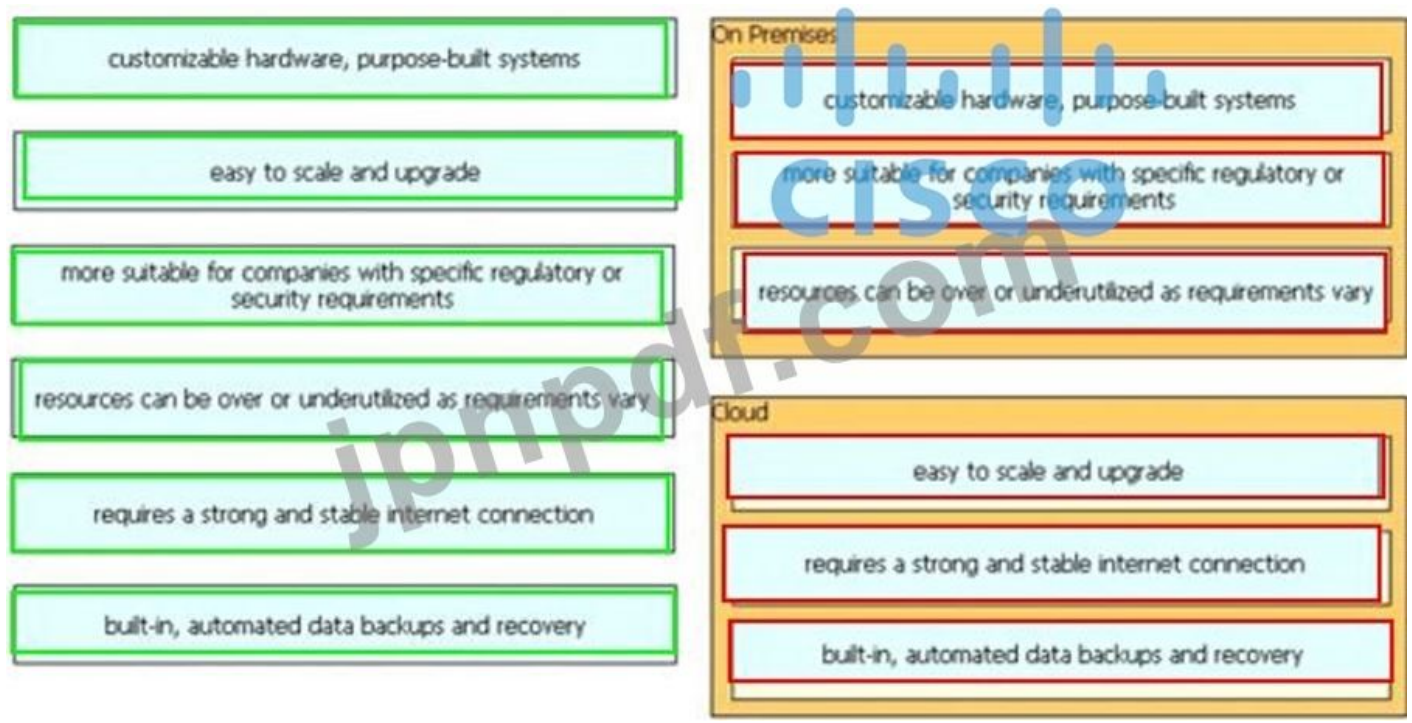
jpnpdf.com

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **377**

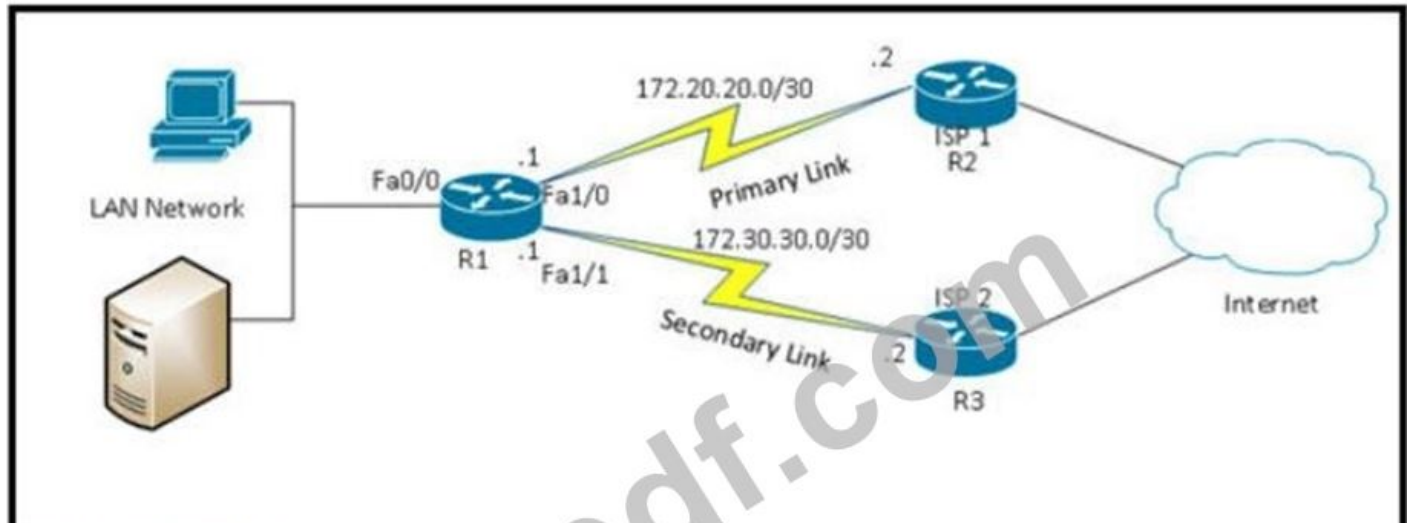
左側の特性を右側の適切なインフラストラクチャ展開タイプにドラッグ アンド ドロップします。

Answer:



最新問題: **378**

出品物参照。




```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 172.20.20.2 source-interface FastEthernet0/0
R1(config-ip-sla-echo)#timeout 5000
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2  track 10
R1(config)#no ip route 0.0.0.0 0.0.0.0 172.20.20.2
R1(config)#ip route 0.0.0.0 0.0.0.0 172.30.30.2  5
```

IP SLA トラッキングが失敗する 2 つの理由は何ですか? (2つ選択)

A. ソース インターフェイスが正しく構成されていません

B. icmp-echo の宛先は 172.30.30.2 でなければなりません

C. R1 LAN ネットワークに戻るルートが R2 にありません

D. デフォルト ルートのネクスト ホップ IP アドレスが正しくありません

E. しきい値が間違っています

Answer: (解答を表示する**)**

タイムアウト (ミリ秒単位) は、IP SLA 操作が要求パケットからの応答を待機する時間を設定します。つまり、タイムアウトは、失敗したと見なされる前にルーターが ping への応答を待機する時間を指定します。しきい値 (ミリ秒単位) は、IP SLA 操作によって作成されたネットワーク監視統計を計算するための上限しきい値を設定します。しきい値は、IP SLA 違反への応答をアクティブにするために使用されます。たとえば、SNMP トラップを送信したり、セカンダリ SLA 操作を開始したりします。言い換えると、しきい値は、到達可能性に影響を与えないしきい値イベントを示すためにのみ使用されますが、timeout コマンドの適切な設定を評価するために使用される場合があります。

到達可能性の追跡では、リターン コードが OK または OverThreshold の場合、到達可能性はアップしています。OK でない場合、到達可能性はダウンしています。

このチュートリアルは、IP SLA トラッキングのトピックを修正するのに役立ちます。.com/using-ip-sla-to-change-routing/

注: なぜこれら 2 つのコマンドがあるのか疑問に思う人もいるでしょう。

R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10 R1(config)#no ip route 0.0.0.0 0.0.0.0 172.20.20.2

実際には、次の 2 つのコマンドがあります。

ip ルート 0.0.0.0 0.0.0.0 172.20.20.2 トラック 10 ip ルート 0.0.0.0 0.0.0.0 172.20.20.2

異なっています。これら 2 つのスタティック ルートは、ルーティング テーブルに共存できます。したがって、追跡がダウンした場合、最初のコマンドは削除されますが、2 番目のコマンドはまだ存在し、バックアップ パスは優先されません。そのため、2 番目のものを削除する必要があります。

最新問題: **379**
展示を参照してください。

エンジニアは、ゲスト ユーザーが顧客のゲスト WLAN に接続しているときに、ゲスト ユーザーが他のゲスト ユーザー デバイスにアクセスできる理由を調査しています。この問題を解決するアクションは何ですか?

A. P2P ブロッキングを実装する
B. スプリット トンネリングを実装する
C. Wi-Fi ダイレクト ポリシーを実装する
D. MFP クライアント保護を実装する
Answer: (解答を表示する)

最新問題: **380**
特性を左側から右側に記述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:

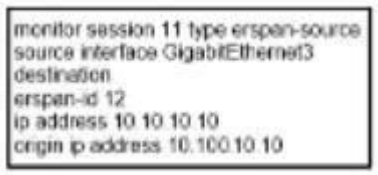
最新問題: **381**
ワイヤレス クライアントが 2 つの異なるワイヤレス コントローラ間をローミングすると、ネットワーク接続が一定期間停止します。この問題の原因となる構成の問題はどれですか?
A. モビリティ グループ内のすべてのコントローラが同じモビリティ グループ名を使用しているわけではありません。
B. モビリティ グループ内のすべてのコントローラが同じ仮想インターフェイス IP アドレスを使用しているわけではありません。
C. モビリティ グループ内のすべてのコントローラが同じ仮想インターフェイス IP アドレスを使用しています。
D. モビリティ グループ内のすべてのコントローラが同じモビリティ グループ名を使用しています。
Answer: B (メーッセージを残す**)**
モビリティ グループを設定するための前提条件は、すべてのコントローラは、
同じ仮想インターフェイスの IP アドレス"。モビリティ グループ内のすべてのコントローラが使用していない場合
同じ仮想インターフェイスの場合、コントローラ間ローミングは機能しているように見えますが、ハンドオフは
は完了せず、クライアントは一定期間接続を失います。→答えBは
正しい。
参照：
b_cg85/mobility_groups.html

最新問題: **382**
Cisco SD-Access ワイヤレス ネットワークの導入では、どの設計原則に従う必要がありますか?
A. WLC はファブリック オーバーレイの一部です。
B. WLC はファブリックの外側に接続されています
C. アクセスポイントはファブリックの外側に接続されています。
D. WLC はファブリック アンダーレイの一部です。
Answer: (解答を表示する**)**

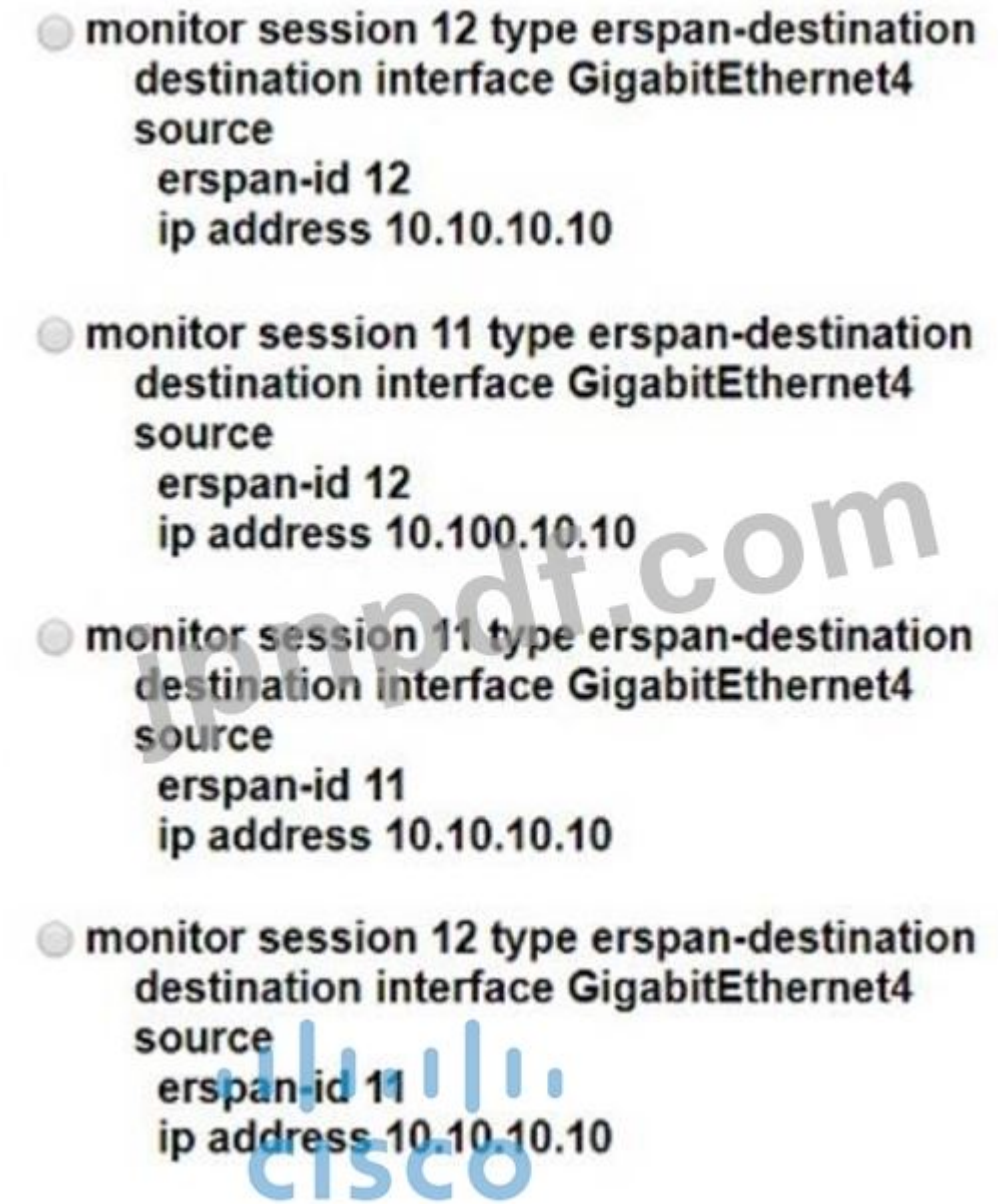
最新問題: **383**
ファブリック アクセス ポイントはネットワークにどのように適合しますか?
A. ローカル モードであり、ファブリック ボーダー ノードに直接接続する必要があります。
B. FlexConnect モードであり、ファブリック ボーダー ノードに直接接続する必要があります。
C. ローカル モードであり、ファブリック エッジ スイッチに直接接続する必要があります。
D. FlexConnect モードであり、ファブリック エッジ スイッチに直接接続する必要があります。
Answer: C (メーッセージを残す**)**
説明
ファブリック モード AP は、従来の AP がサポートするのと同じワイヤレス メディア サービスを引き続きサポートします。AVC、サービス品質 (QoS)、およびその他のワイヤレス ポリシーを適用します。CAPWAP コントロール プレーンをファブリック WLC に確立します。ファブリック AP はローカル モード AP として参加し、ファブリック エッジ ノード スイッチに直接接続して、ファブリック WLC を介した RLOC 割り当てなどのファブリック登録イベントを有効にする必要があります。ファブリック エッジ ノードは、CDP を使用して AP を特別な有線ホストとして認識し、特別なポート構成を適用して、ファブリック全体の共通 EID スペース内の一意のオーバーレイ ネットワークに AP を割り当てます。この割り当てにより、単一のサブネットを使用してファブリック サイトの AP インフラストラクチャをカバーすることで、管理を簡素化できます。

参照: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.html

最新問題: **384**

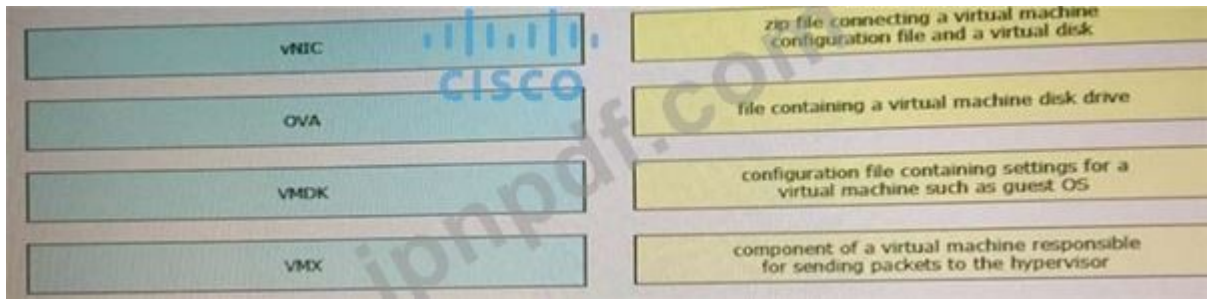


展示を参照してください。ERSPAN セッションの設定を完了するコマンド セットはどれですか?

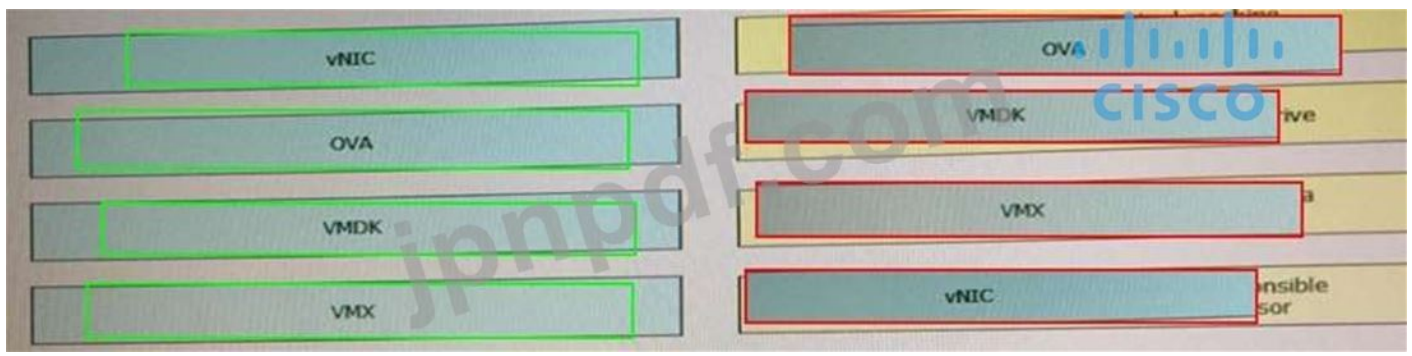


A. オプション D
B. オプション B
C. オプション C
D. オプション A
Answer: D (メーッセージを残す**)**

最新問題: **385**
仮想コンポーネントを左側から右側の説明にドラッグ アンド ドロップします。



Answer:



Explanation:

+ ゲスト OS などの仮想マシンの設定を含む構成ファイル: VMX
+ ハイパーバイザーへのパケットの送信を担当する仮想マシンのコンポーネント: vNIC
+ 仮想マシン構成ファイルと仮想ディスクを含む zip ファイル: OVA
+ 仮想マシンのディスク ドライブを含むファイル: VMDK

VMX ファイルは、仮想マシンの構成を保持するだけです。

VMDK (Virtual Machine Disk の略) は、VMware Workstation や VirtualBox などの仮想マシンで使用される仮想ハード ディスク ドライブのコンテナーを記述するファイル形式です。

OVA ファイルは、仮想マシンの圧縮された「インストール可能な」バージョンを含む Open Virtualization Appliance です。OVA ファイルを開くと、VM が抽出され、コンピューターにインストールされている仮想化ソフトウェアにインポートされます。

最新問題**: 386**

CEF スイッチングは、シスコ 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 カードの専用メモリ内の隣接テーブルをソートす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 スイッチングは CDP プロトコルによって構築された隣接テーブルを使用し、プロセス スイッチングはルーティング テーブルを使用します。

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 ルックアップに 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

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）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スケーラブルなスイッチングの独自の形式です。CEF スイッチングでは、従来はルート キャッシュに格納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、Gigabit Route Processor（GRP; ギガビット ルート プロセッサ）で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。これは、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、ファースト スイッチングや最適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 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、リンク層を介してシングル ホップで相互に到達できる場合、隣接していると見なされます。FIB に加えて、CEF は隣接関係テーブルを使用して、レイヤ 2 アドレッシング情報を先頭に追加します。隣接テーブルは、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。
* セントラル 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 プロセッサ上に存在し、ルート プロセッサは高速転送を実行します。CEF スイッチングにライン カードを使用できない場合、または分散型 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 と隣接テーブルの同一のコピーを維持します。ラインカードはそれ自体でエクスプレス フォワーディングを実行できるため、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) がスイッチング操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、Inter-Process Communication (IPC; プロセス間通信) 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: 387
展示を参照してください。

Customer2 のホストが、IP アドレス 192.168.1.200 を持つ Customer1 の FTP サーバーにアクセスできるようにする構成はどれですか?
A. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 Customer2 ip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customerl
B. ip route vrf Customerl 172.16.1.1 255.255.255.255 172.16.1.1 グローバル
ip route vrf カスタマー 192.168.1.200 255.255.255.0 192.168.1.1 グローバル
IP ルート 192.168.1.0 255.255.255.0 VlanlO
IP ルート 172.16.1.0 255.255.255.0 Vlan20
C. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 グローバル
ip route vrf カスタマー 192.168.1.200 255.255.255.255 192.168.1.1 グローバル
IP ルート 192.168.1.0 255.255.255.0 VlanlO
IP ルート 172.16.1.0 255.255.255.0 Vlan20

D. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 Customerl ip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customer2
Answer: C (メーッセージを残す)

最新問題**: 388**
ログイン方法は、これらのパラメータを使用してルータの VTY 回線で設定されます。
最初の認証方式は TACACS です
TACACS が利用できない場合、提供された資格情報なしでログインが許可されます。このタスクを実行する構成はどれですか?
A. R1#sh 実行 | aaaを含む
aaa ニューモデル
aaa 認証 ログイン VTY グループ tacacs+ なし
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
パスワード 7 0202039485748
R1#sh 実行 | ユーザー名を含める
R1#
B. R1#sh 実行 | aaaを含む
aaa ニューモデル
aaa authentication login telnet group tacacs+ none
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
R1#sh 実行 | ユーザー名を含める
R1#
C. R1#sh 実行 | aaaを含む
aaa ニューモデル
AAA 認証ログイン デフォルト グループ tacacs+ なし
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
パスワード 7 0202039485748
D. R1#sh 実行 | aaaを含む
aaa ニューモデル
AAA 認証ログイン デフォルト グループ tacacs+
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
トランスポート入力なし
R1#

Answer: C (メーッセージを残す)
要件 (最初に TACACS+ を使用し、次に認証なしでログインを許可する) に従って、AAA コマンドに 「aaa authentication login ... group tacacs+ none」を使用する必要があります。
次に確認することは、「aaa authentication login default」または 「aaa authentication login list-name」が使用されているかどうかです。「default」キーワードは、すべてのログイン接続 (tty、vty、console、aux など) に適用することを意味します。このキーワードを使用する場合、tty、vty、および aux ラインの下で他に何も構成する必要はありません。このキーワードを使用しない場合は、認証機能を適用する行を指定する必要があります。
上記の情報から、答え 'R1#sh run | ' を見つけることができます。include aaa aaa new-model aaa authentication login default group tacacs+ none aaa session-id common R1#sh run | section vty line vty 0 4 password 7 0202039485748 AAA 設定の詳細については、AAA TACACS+ および RADIUS チュートリアル - パート 2 をお読みください。
参考までに、「R1#sh run |」と答えてください。aaaを含む
aaa ニューモデル
aaa authentication login telnet group tacacs+ none
aaa セッション ID 共通
R1#sh 実行 | セクション vty
回線 vty 0 4
R1#sh 実行 | ユーザー名を含める
vty 行 (「ine vty 0 4」) の下に次のコマンドを追加すると、R1# は正しくなります: 「ogin authentication telnet」(「elnet」は上記の AAA リストの名前です)

最新問題: **389**
展示を参照してください。

```
switch1(config)# interface GigabitEthernet 1/1
switch1(config-if)# switchport mode trunk
switch1(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-90
switch1(config)# exit
switch1(config)# monitor session 1 source vlan 10
switch1(config)# monitor session 1 destination remote vlan 70



switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)# switchport mode trunk
switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,80-90
switch2(config)# exit
switch2(config)# monitor session 2 source remote vlan 70
switch2(config)# monitor session 2 destination interface GigabitEthernet1/1
```

ipnpdf.com

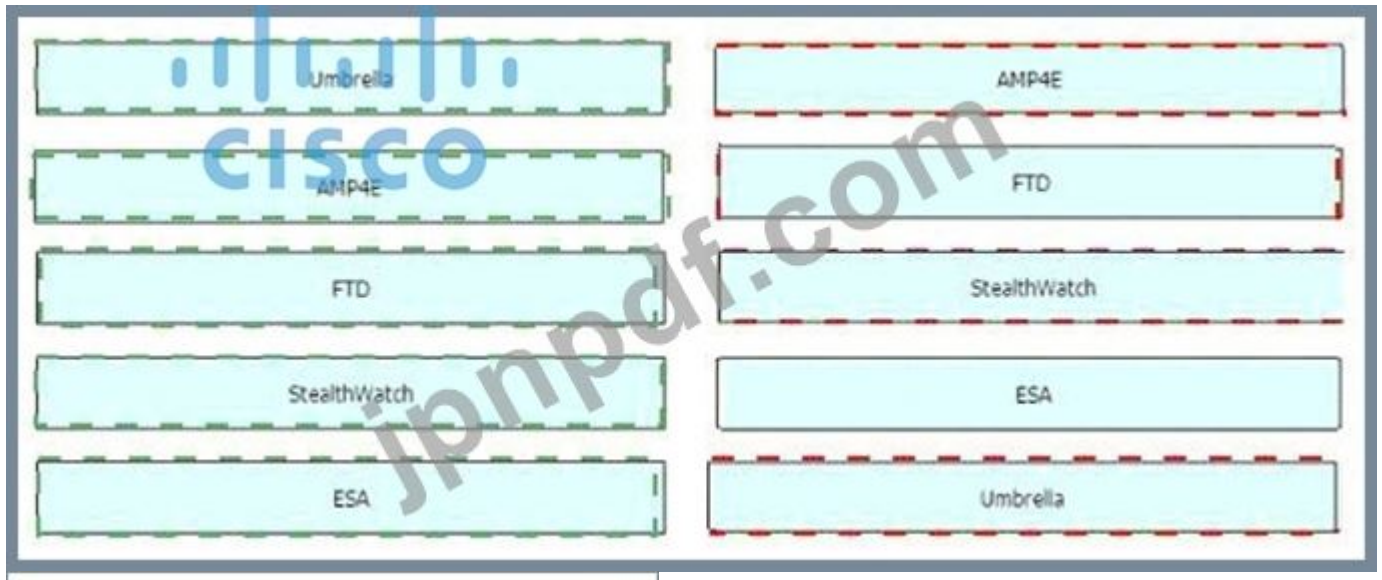
ネットワーク管理者は、スイッチ 1 とスイッチ 2 の間の問題をトラブルシューティングするために RSPAN を構成しました。スイッチは、インターフェイス GigabitEthernet 1/1 を使用して接続されています 外部パケット キャプチャ デバイスは、swich2 インターフェイス GigabitEthernet1/2 に接続されています この設定を完了するために追加する必要がある 2 つのコマンドはどれですか?
(2つ選んでください)
A. switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-80

B. switch2(config)# monitor session 1 source remote vlan 70 switch2(config)# monitor session 1 destination interface GigabitEthernet1/1
C. switch2(config)# モニター セッション 2 宛先 VLAN 10
D. 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
E. switch2(config)# monitor session 1 source remote vlan 70 switch2(config)# monitor session 1 destination interface GigabitEthernet1/2
Answer: A,E (メーッセージを残す)

最新問題**: 390**
GRE トンネルがダウンし、エラー メッセージ %TUN-5-RECUR DOWN:
Tunnel0 temporarily disabled due to recursive routing error.
エラーの考えられる原因を説明する 2 つのオプションはどれですか? (2つ選んでください)
A. トンネルでリンク フラッピングが発生しています
B. トンネルに誤った宛先 IP アドレスが構成されている
C. トンネル モードとトンネル IP アドレスが正しく構成されていません
D. 経路フラッピングによりネットワークが不安定
E. トンネルの宛先がトンネル インターフェイスの外にルーティングされています。
Answer: D,E (メーッセージを残す)
説明
%TUN-5-RECURDOWN: Tunnel0 temporary disabled due to recursive routing エラー メッセージは、Generic Routing Encapsulation (GRE) トンネル ルーターが再帰ルーティングの問題を検出したことを意味します。この状態は通常、次のいずれかの原因によるものです。
+ ルーターがトンネル インターフェイス自体を使用してトンネルの宛先アドレスにルーティングしようとする構成ミス (再帰ルーティング)
+ ネットワークの他の場所でのルート フラッピングによって引き起こされる一時的な不安定性

最新問題**: 391**
脅威防御ソリューションを左側から右側の説明にドラッグ アンド ドロップします。


cisco
jpnpdf.com
Answer:



有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **392**
ログ ファイルの日付の横に * が含まれるのはなぜですか?
A. ログ メッセージが記録されたときにネットワーク デバイスが NTP 時刻を受信していた
B. ログ メッセージが記録されたときに、ネットワーク デバイスが NTP サーバーに到達できませんでした。
C. ネットワーク デバイスが NTP を使用するように構成されていません
D. ネットワーク デバイスは、ログに NTP タイム スタンプを使用するように構成されていません。
Answer: B (メーッセージを残す**)**
説明
システム クロックが設定されていない場合、日付と時刻の前にアスタリスク (*) が表示され、日付と時刻が正しくない可能性があることが示されます。
参照：
https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/service_timestam

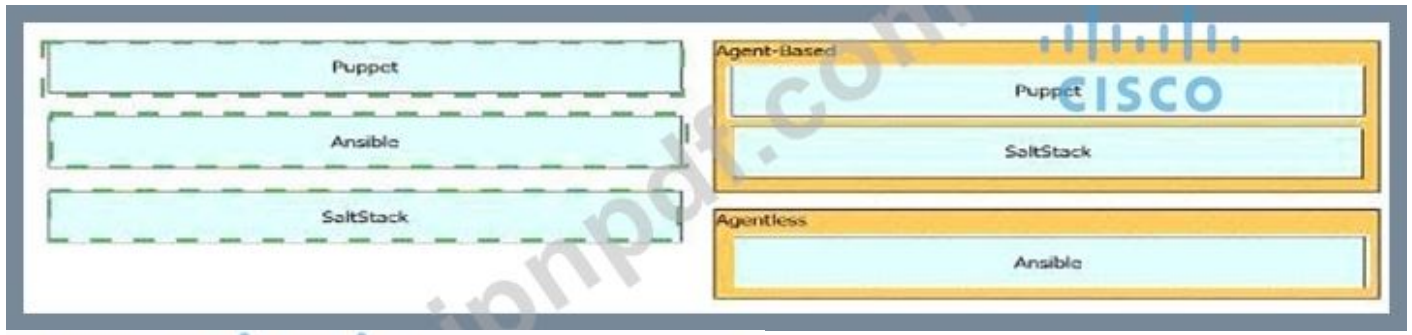
最新問題: **393**
展示を参照してください。

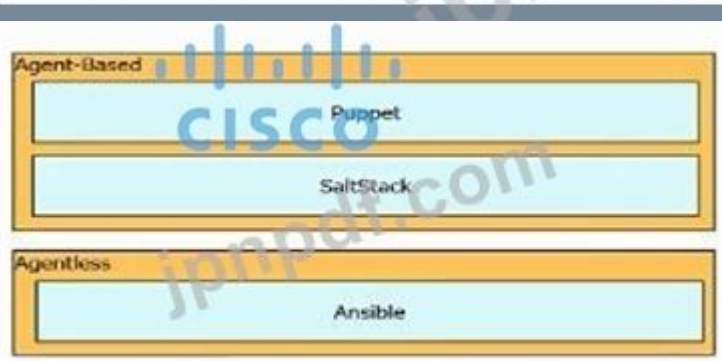
エンジニアは、AS 200 を出るすべてのトラフィックがリンク 2 を出口ポイントとして選択するようにする必要があります。すべての BGP ネイバー関係が形成され、どのルーターでも属性が変更されていないと仮定すると、どの構成でタスクが達成されますか?

A. R4(config-router)bgp デフォルト ローカル プリファレンス 200
B. R3(config-router) ネイバー 10.1.1.1 重み 200
C. R3(config-router)bgp デフォルト ローカル プリファレンス 200
D. R4(config-router)nighbor 10.2.2.2 重み 200
Answer: A (メーッセージを残す**)**
説明
ローカル プリファレンスは、特定のネットワークに到達するために、どのパスが AS を出るのが優先されるかについての AS への指示です。ローカル プリファレンスの高いパスが優先されます。ローカル プリファレンスのデフォルト値は 100 です。
ローカル ルーターにのみ関連する重み属性とは異なり、ローカル プリファレンスはルーターが同じ AS で交換する属性です。ローカル プリファレンスは「bgp default local-preference」で設定されます。この場合、R3 と R4 の両方に出口リンクがありますが、R4 の方がローカル プリファレンスが高いため、R4 が AS 200 からの優先出口ポイントとして選択されます。

最新問題: **394**
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: **395**

展示を参照してください。

Link1 は銅線接続で、Link2 はファイバー接続です。ファイバー ポートは、すべての転送のプライマリ ポートである必要があります。SW2 での show spanning-tree コマンドの出力は、ファイバ ポートがスパニング ツリーによってブロックされていることを示しています。エンジニアが SW2 の GO/1

で spanning-tree port-priority 32 コマンドを入力しますが、ポートはブロックされたままです。問題を解決するには、Link2 に接続されているポートでどのコマンドを入力する必要がありますか?

A. SW1 でスパニング ツリー ポート プライオリティ 32 を入力します。
B. SW1 でスパニング ツリー ポート プライオリティ 224 を入力します。
C. SW2 でスパニング ツリー ポート プライオリティ 4 を入力します。
D. SW2 でスパニング ツリー ポート プライオリティ 64 を入力します。

Answer: A (メーッセージを残す)

説明

SW1 は、2 つのスイッチ間のブリッジング ループを回避するために、SW2 へのポートの 1 つをブロックする必要があります。

残念ながら、ファイバー ポート Link2 がブロックされました。しかし、SW2 はブロックされたポートをどのように選択するのでしょうか? その答えは、SW1 から受信した BPDU に基づいています。answer 'Enter spanning-tree port-priority 32 on SW1' BPDU は、次の場合に他のものよりも優れています。

1. SW1 でスパニング ツリー ポート プライオリティ 32 を入力してください」と答え、ルート ブリッジ ID を下げます。
2. SW1 でスパニング ツリー ポート プライオリティ 32 を入力してください」と答えて、ルートへのパス コストを下げます
3. SW1 でスパニング ツリー ポート プライオリティ 32 を入力してください」と回答し、送信ブリッジ ID を下げます。
4. answer 'Enter spanning-tree port-priority 32 on SW1' Lower 送信ポート ID これら 4 つのパラメータが順番に検査されます。この特定のケースでは、SW1 によって送信されたすべての BPDU は、同じルート ブリッジ ID、ルートへの同じパス コスト、および同じ送信ブリッジ ID を持ちます。最適なものを選択するために残された唯一のパラメーターは、送信ポート ID (ポート ID = ポート優先度 + ポート インデックス) です。また、Gi0/0 のポート インデックスは Gi0/1 のポート インデックスよりも小さいため、リンク 1 がプライマリ リンクとして選択されています。

したがって、プライマリ リンクを変更するには、ポート プライオリティを変更する必要があります。ポート プライオリティの数値が小さいほど、そのポートのプライオリティは高くなります。つまり、SW1 の Gi0/1 (SW2 の Gi0/1 ではなく) のポート プライオリティを、Gi0/0 のポート プライオリティよりも低い値に変更する必要があります。

最新問題: **396**

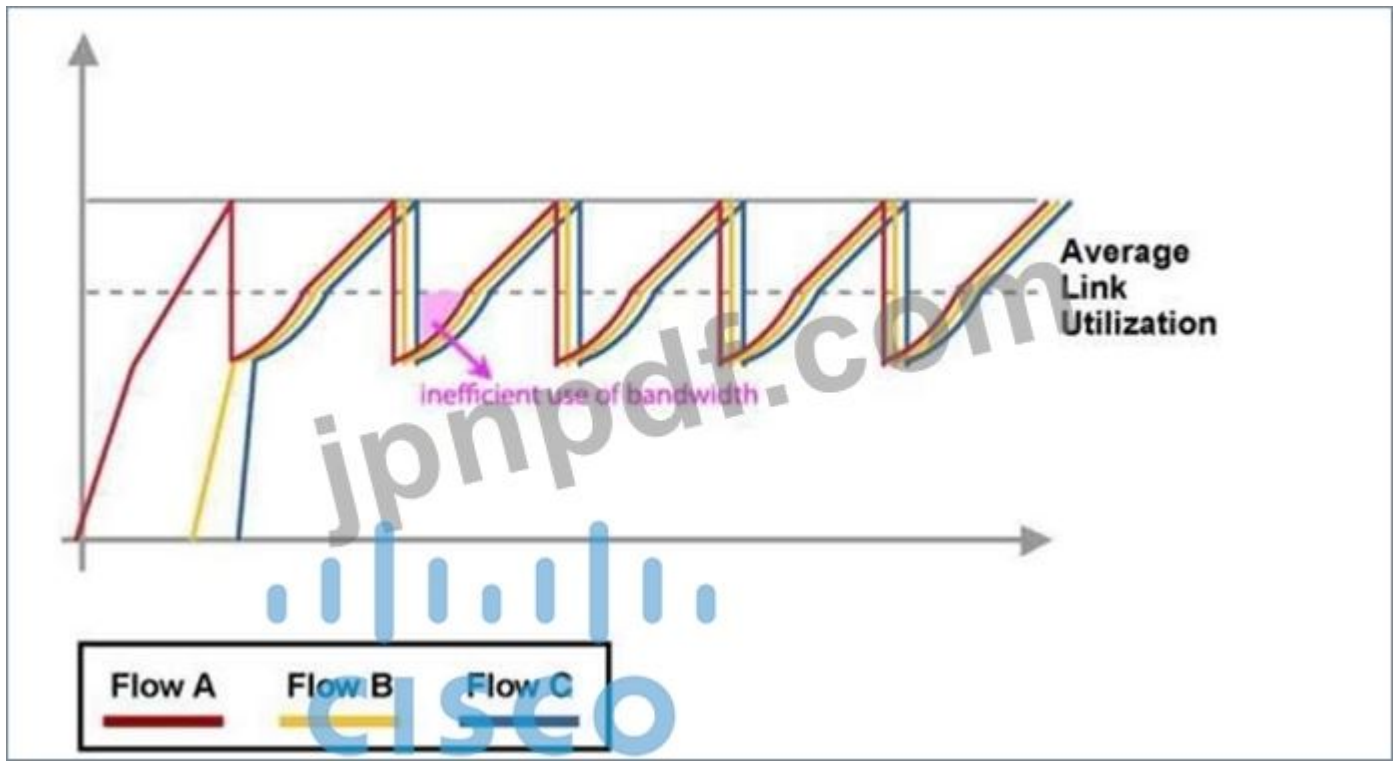
SD-Access ソリューションにおけるフュージョンの役割は?

A. 外部ネットワークへの接続を提供します
B. DNS サーバーとして機能します。
C. ユーザー定義の仮想ネットワークと共有サービスの間でルート リークを実行します。
D. ファブリックに追加の転送容量を提供します

Answer: C (メーッセージを残す)

現在、ダイナミック ネットワーク アーキテクチャ ソフトウェア定義アクセス (DNA-SDA) ソリューションには、
ユーザ VRF と共有サービスの間で VRF ルート リークを実行するフュージョン ルータ。
グローバル ルーティング テーブル (GRT) または別の VRF で。共有サービスは、DHCP、ドメインで構成される場合があります
ネーム システム (DNS)、ネットワーク タイム プロトコル (NTP)、ワイヤレス LAN コントローラ (WLC)、ID
サービス エンジン (ISE)、他の仮想ネットワークで使用できるようにする必要がある DNAC コンポーネント
(VN の) キャンパス内。

参照：
213525-sda-steps-to-configure-fusion-router.html



最新問題: **397**

OSI モデルのレイヤ 2 ですべてのトラフィックに安全な通信チャネルを提供するテクノロジはどれですか?

A. SSL

B. IPsec

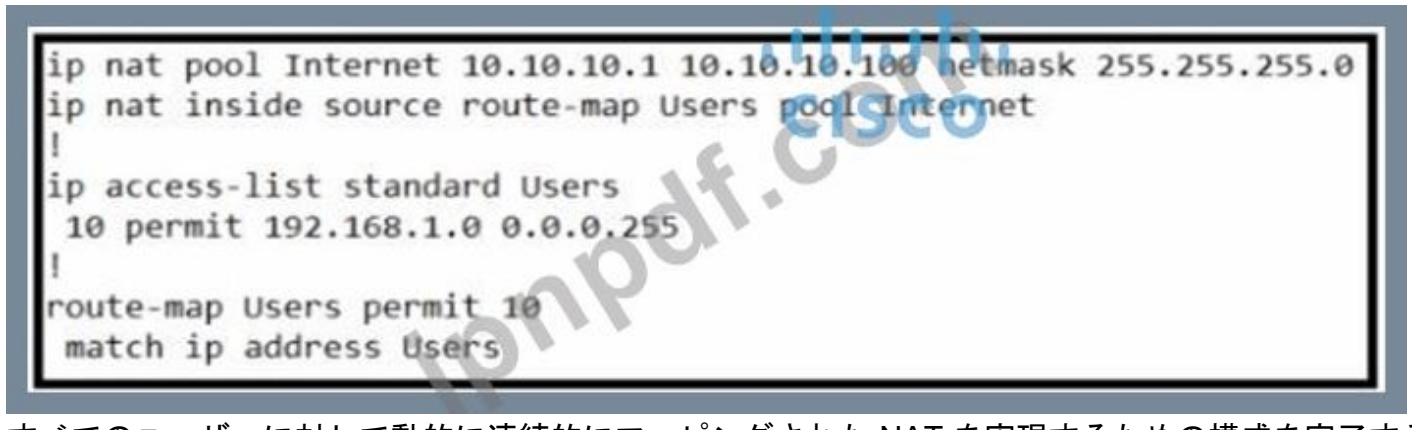
C. MACsec

D. Cisco Trustsec

Answer: (解答を表示する)

最新問題: **398**

展示を参照してください。



すべてのユーザーに対して動的に連続的にマッピングされた NAT を実現するための構成を完了するアクションはどれですか?

A. NAT プール サイズを増やして、254 の使用可能なアドレスをサポートします。

B. 192.168 1 0 アドレス範囲を使用するようにプールを再構成します

C. match-host タイプの NAT プールを構成する

D. 1 対 1 型の NAT プールを構成する

Answer: A (メーッセージを残す)

最新問題**: 399**
IP アドレス 209 16b 201 2b を持つクライアントは、209 l6b.200.22b のポート 80 で Web サーバーにアクセスする必要があります。
このトラフィックを許可します。エンジニアは、Web サーバーに接続するポートのインバウンド方向に適用されるアクセス制御リストにステートメントを追加する必要があります。どのステートメントがこのトラフィックを許可しますか?
A. tcp ホスト 209.165.200.225 ホスト 209.165.201.25 eq 80 を許可します。
B. 許可 tcp ホスト 209 165.201 25 ホスト 209.165.200.225 eq 80
C. tcp ホスト 209 165 200 225 eq 80 ホスト 209.165.201.25 を許可します。
D. tcp ホスト 209.165.200 225 を許可する 80 ホスト 209.165.201.25
Answer: B (メーッセージを残す)

最新問題**: 400**
Cisco DNA Center の完全なアップグレードに必要な 2 つの手順はどれですか? 2つ選んでください。）
A. アプリケーションの更新
B. プロキシ設定
C. 自動バックアップ
D. システムアップデート
E. ゴールデン イメージの選択
Answer: C,D (メーッセージを残す)

最新問題**: 401**

```
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
```

展示を参照してください。送信元のすべてのトラフィックを許可して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
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

```
Router(config)#no access-list 100 permit ip 172.16.0.0 0.0.15.255 any
Router(config)#access-list 100 permit ip 172.16.0.0 0.0.15.255 any log
Router(config)#interface GigabitEthernet0/1
Router(config-if)#access-group 100 in

Router(config)#access-list 100 seq 5 permit ip host 172.20.10.1 any log
Router(config)#interface GigabitEthernet0/1
Router(config-if)#access-group 100 in

Router(config)#ip access-list extended 100
Router(config-ext-nacl)#5 permit ip 172.20.10.0 0.0.0.255 any log
Router(config)#interface GigabitEthernet0/1
Router(config-if)#access-group 100 in

Router(config)#access-list 100 permit ip host 172.20.10.1 any log
Router(config)#interface GigabitEthernet0/1
Router(config-if)#access-group 100 in
```

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)

最新問題: **402**
展示を参照してください。

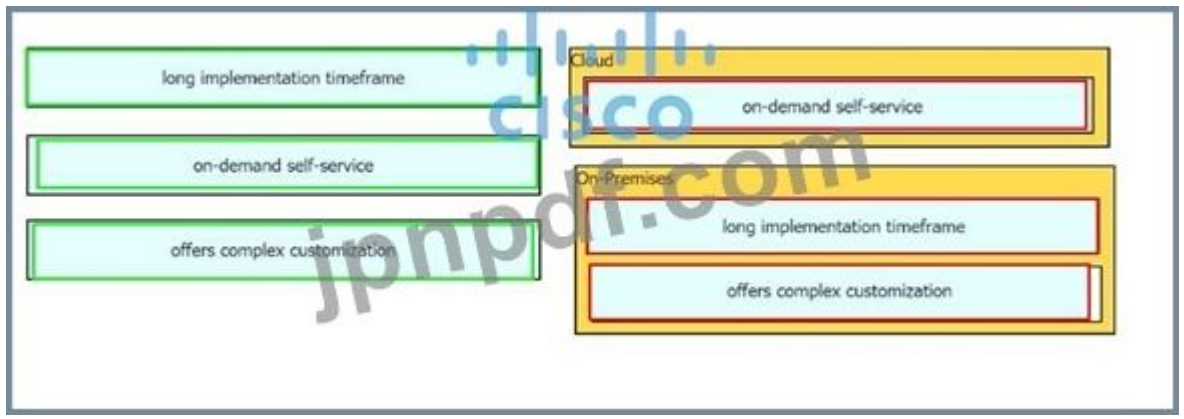
```
ip vrf BLUE
 rd 1:1
!
interface Vlan100
 description GLOBAL_INTERFACE
 ip address 10.10.1.254 255.255.255.0
!
access-list 101 permit ip 10.10.5.0 0.0.0.255 10.10.1.0
255.255.255.0
!
route-map VRF_TO_GLOBAL permit 10
 match ip address 101
set global
!
interface Vlan500
 description VRF_BLUE
 ip vrf forwarding BLUE
 ip address 10.10.5.254 255.255.255.0
ip policy route-map VRF_TO_GLOBAL
```

エンジニアは、Blue VRF がグローバル ルーティング テーブルにリークできるように構成を作成しようとしましたが、その構成は期待どおりに機能しません。この問題を解決するアクションはどれですか?
A. ルート マップのアクセス リスト番号を変更します。
B. ルート マップの構成を VRF_BLUE に変更します。
C. アクセス リストの宛先マスクをワイルドカードに変更します。

D. アクセス リスト 101 で指定されている送信元ネットワークを変更します。
Answer: C (メーッセージを残す**)**

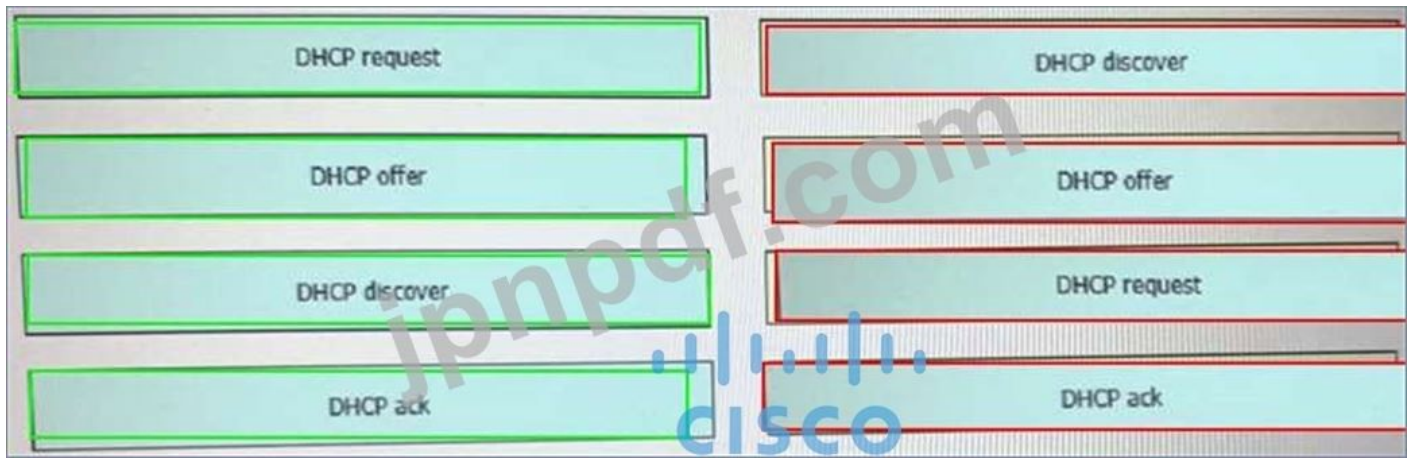
最新問題**: 403**
左の特性を右の配置モデルにドラッグ アンド ドロップします。

Answer:



最新問題**: 404**
クライアントと AP の間で交換される DHCP メッセージを、右側の交換される順序にドラッグ アンド ドロップします。

Answer:



DHCP クライアントと DHCP サーバーの間で送信されるメッセージは、DHCPDISCOVER、DHCPOFFER、DHCPREQUEST、および DHCPACKNOWLEDGEMENT の 4 つです。
このプロセスは、多くの場合、DORA (発見、提供、要求、承認) と略されます。

最新問題: **405**
REST API 内で OAuth 2.0 を使用するアカウント認証の方法はどれですか?
A. アクセストークン
B. ユーザー名/役割の組み合わせ
C. 基本的な署名ワークフロー
D. クッキー認証
Answer: (解答を表示する**)**

最新問題: **406**
展示を参照してください。

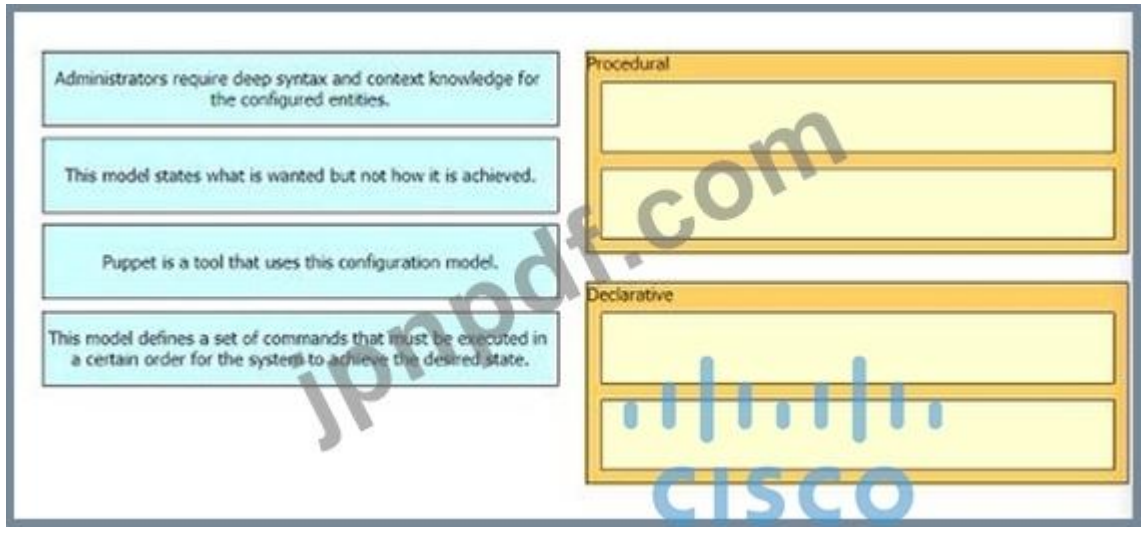
```
vlan 222
 remote-span
!
vlan 223
 remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

技術者が monitor session 1 destination remote vlan 223 コマンドを追加すると、どのような結果になりますか?
A. 2 つの宛先を構成すると、エラーがフラグされます。
B. RSPAN トラフィックは、VLAN 222 と 223 の間で分割されます。
C. RSPAN トラフィックは VLAN 222 および 223 に送信されます。
D. RSPAN VLAN は VLAN 223 に置き換えられます。
Answer: D (メーッセージを残す**)**

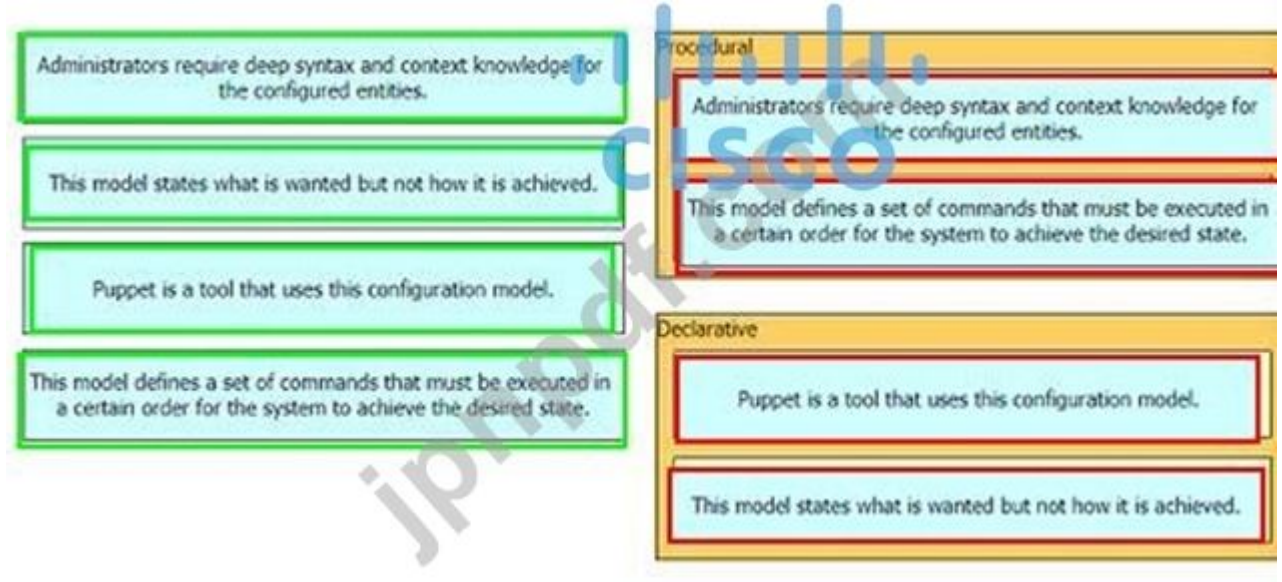
有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **407**

10 個の特性を右側の構成モデルにドラッグ アンド ドロップします。



Answer:



最新問題: **408**

NTP stratum レベルの数字は何を表していますか?

A. マスター タイム サーバーに到達するまでのホップ数。

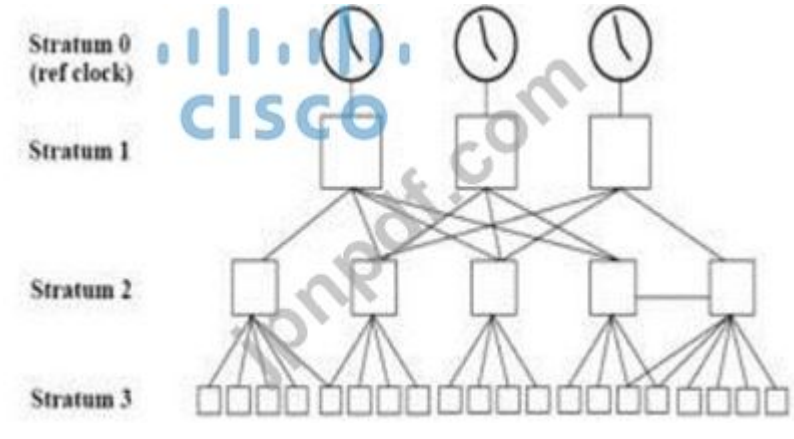
B. 信頼できるタイム ソースに到達するまでにかかるホップ数。

C. デバイス クロックと実際の時間の間のオフセットの量。

D. デバイス クロックと実際の時間の間のずれの量。

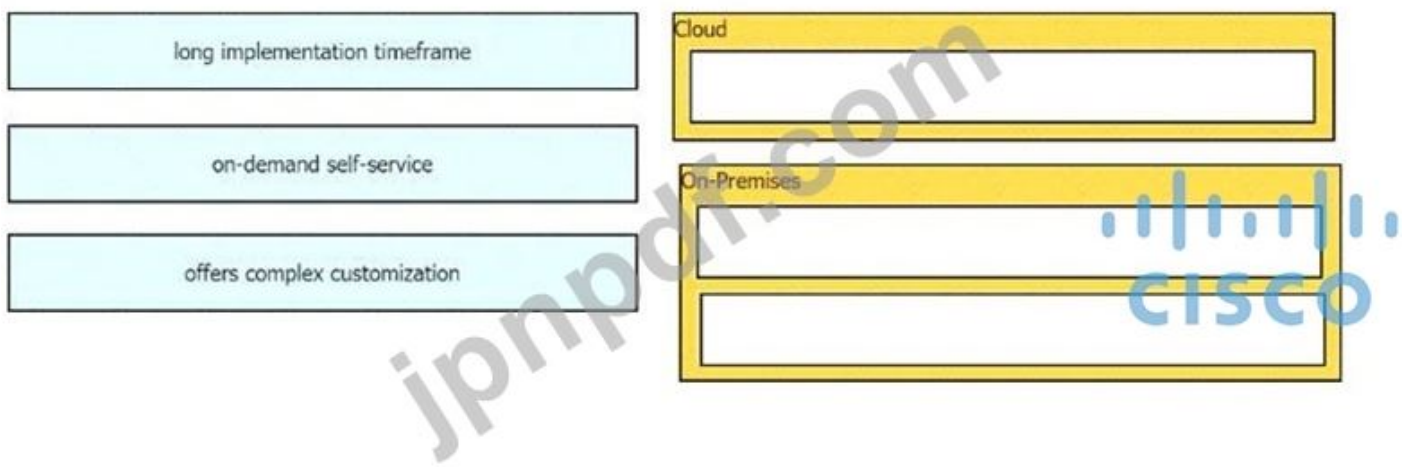
Answer: (解答を表示する**)**

NTP はストラタムの概念を使用して、マシンが信頼できる時刻源 (通常は参照クロック) から何ホップ (ルーター) 離れているかを示します。基準クロックは、正確であると想定され、それに関連する遅延がほとんどまたはまったくない Stratum 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、コンピュータに直接接続され、Stratum-1 サーバーとして動作します。Stratum 1 タイム サーバーは、主要なネットワーク時間標準として機能します。

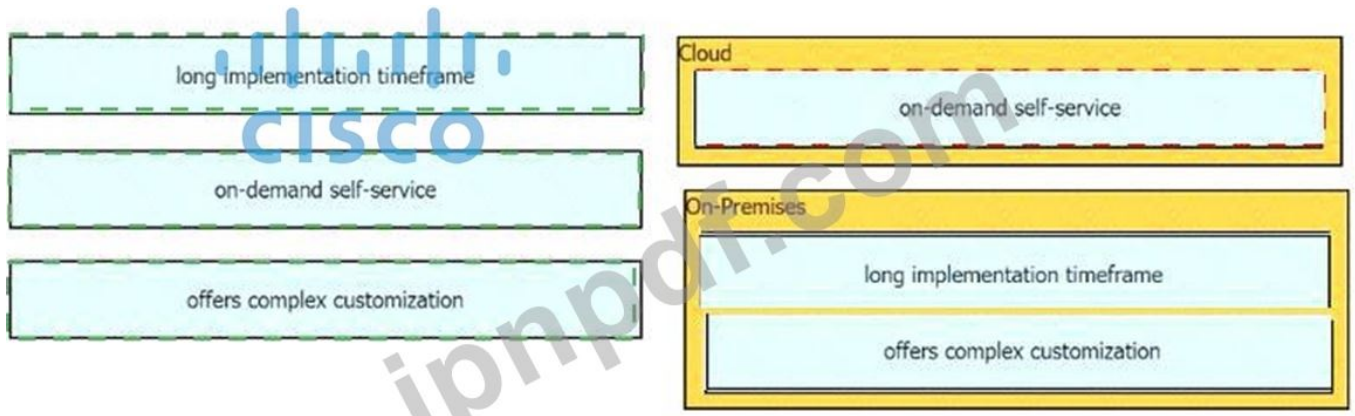


最新問題: **409**
WLAN で WPA2 Enterprise を構成する場合、どの追加のセキュリティ コンポーネント構成が必要ですか?
A. NTP サーバー
B. PKI サーバー
C. RADIUS サーバー
D. TACACS サーバー
Answer: C (メーッセージを残す**)**
WPA2-Enterprise を展開するには、ネットワーク ユーザー アクセスを認証するタスクを処理する RADIUS サーバーが必要です。実際の認証プロセスは 802.1X ポリシーに基づいており、EAP と呼ばれるいくつかの異なるシステムで提供されます。各デバイスは接続前に認証されるため、個人用の暗号化されたトンネルがデバイスとネットワークの間に効果的に作成されます。

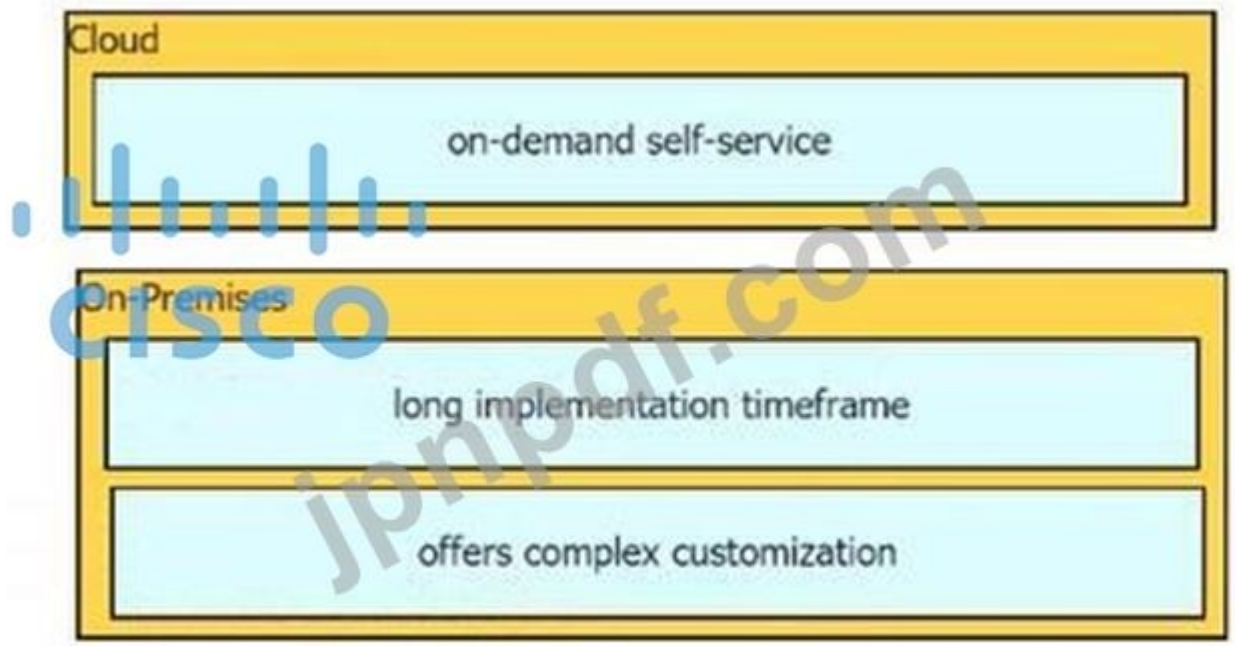
最新問題: **410**
左の特性を右の配置モデルにドラッグ アンド ドロップします。



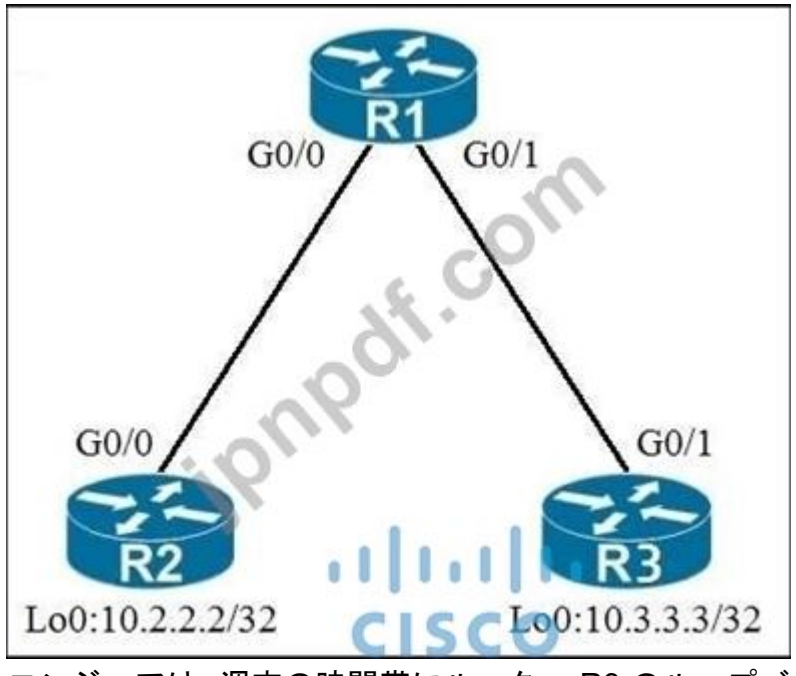
Answer:



説明
グラフィカル ユーザー インターフェイスを含む画像 自動生成された説明



最新問題: 411
展示を参照してください。



エンジニアは、週末の時間帯にルーター R3 のループバック インターフェイスからルーター R2 のループバック インターフェイスへの Telnet トラフィックを拒否する必要があります。ルーター R3 と R2 のループバック インターフェイス間の他のすべてのトラフィックは、常に許可する必要があります。

このタスクを実行するコマンド セットはどれですか?

A. R1(config)#time-range WEEKEND
R1(config-time-range)#periodic 金曜日 日曜日 00:00 ～ 00:00
R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND R1(config)#access-list 150 permit ip any any
R1(config)#interface G0/1 R1(config -if)#ip アクセス グループ 150 で

B. R1(config)#time-range WEEKEND
R1(config-time-range)#定期的な週末 00:00 ～ 23:59
R1(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND R1(config)#access-list 150 permit ip any any
R1(config)#interface G0/1 R1(config -if)#ip アクセス グループ 150 で

C. R3(config)#time-range WEEKEND
R3(config-time-range)#定期 土曜日 日曜日 00:00 ～ 23:59
R3(config)#access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND R3(config)#access-list 150 permit ip any any time-range WEEKEND R3(config)#interface G0/ 1 R3(config-if)#ip アクセス グループ 150 アウト

D. R3(config)#time-range WEEKEND
R3(config-time-range)#定期的な週末 00:00 ～ 23:59
R3(config)#access-list 150 permit tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND R3(config)#access-list 150 permit ip any any time-range WEEKEND R3(config)#interface G0/ 1 R3(config-if)#ip アクセス グループ 150 アウト

Answer: B (メーッセージを残す**)**

最新問題**: 412**

ルーターが 100 kbps を受け入れる SSH の量を制限する構成はどれですか?

A)

B)

A)

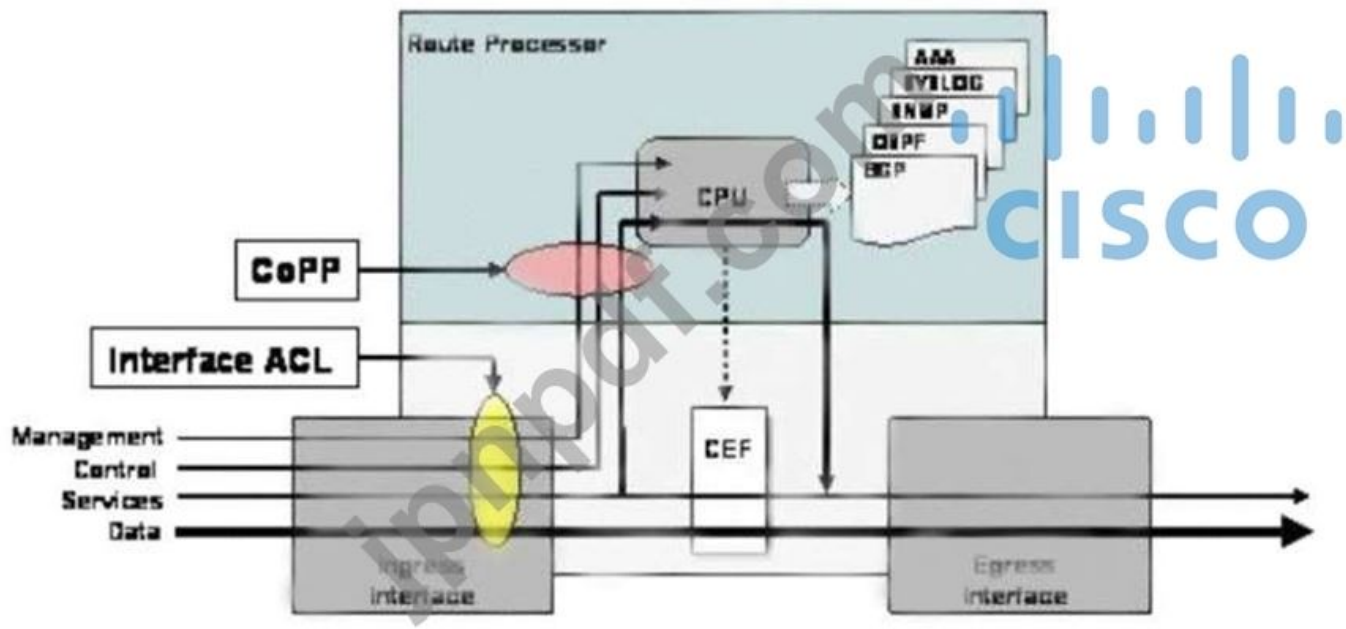
D)

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
CoPP は、ルート プロセッサ リソースを独自の入力インターフェイスを持つ別のエンティティとして扱うことで、ネットワーク デバイス上のルート プロセッサを保護します (一部の実装では、出力も)。CoPP は、次のようなルータのルート プロセッサ宛てのトラフィックをポリシングするために使用されます。
+ OSPF、EIGRP、BGP などのルーティング プロトコル。
+ HSRP、VRRP、GLBP などのゲートウェイ冗長プロトコル。
+ telnet、SSH、SNMP、RADIUS などのネットワーク管理プロトコル。

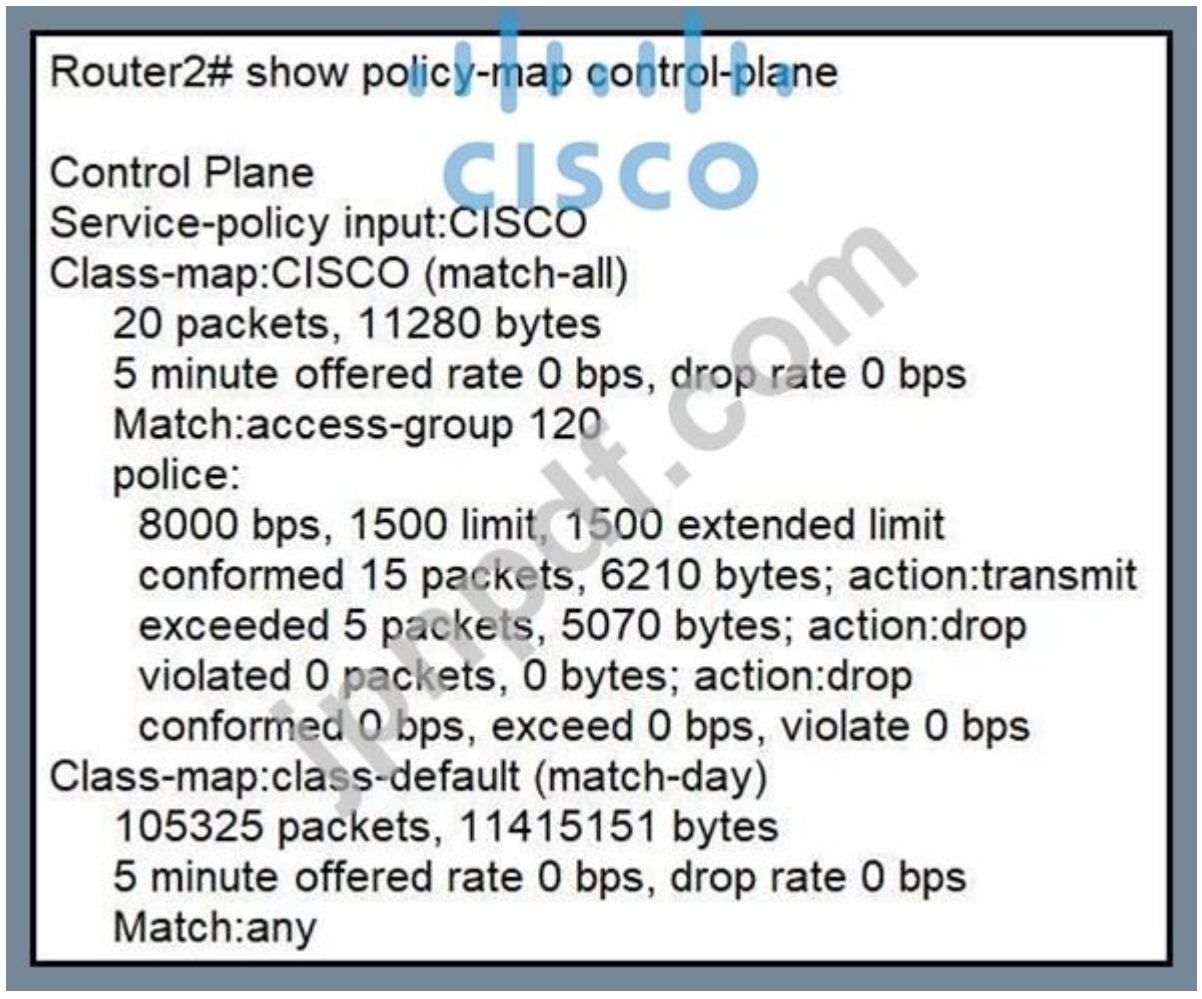


したがって、SSH を処理するために CoPP を適用する必要があります。
管理プレーン。CoPP は「control-plane」コマンドの下に置く必要があります。

最新問題**: 413**
Cisco TrustSec がネットワーク全体でスケーラブルで安全な通信を提供するために使用する機能はどれですか?
A. スイッチ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タグ番号
C. スイッチ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**)**
説明
Cisco TrustSec は、タグを使用して論理グループ特権を表します。セキュリティ グループ タグ (SGT) と呼ばれるこのタグは、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、ルーター、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、認証の結果に基づくか、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 「割り当てられたセキュリティ グループ タグ番号 「スイッチ上の各ユーザーに割り当てられて

いる」というのは正しくありません。割り当てられた ... オンにスイッチ」のみと書かれているためです。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」という回答も正しくありません。」)。

最新問題: **414**



展示を参照してください。エンジニアは CoPP を設定し、show コマンドを入力して実装を確認します。
構成の結果は何ですか?

A. クラス デフォルト トラフィックはドロップされます。
B. トラフィックが指定されたレートを超えると、送信され、再マーキングされます。
C. ICMP は、この構成に基づいて拒否されます。
D. すべてのトラフィックは、アクセス リスト 120 に基づいてポリシングされます。
Answer: D (メーッセージを残す)

最新問題: **415**
展示を参照してください。

OSPF ネイバーシップを形成するために R2 に適用する必要があるコマンドはどれですか?

A. ネットワーク 20.1.1.2 255.255.255 エリア 0

B. ネットワーク 20.1.1.2.0.0.0.0 エリア 0

C. ネットワーク 20.1.1.2 255.255.0.0。エリア0

D. ネットワーク 20.1.1.2.0.0.255.255 エリア 0

Answer: B (メーッセージを残す)

最新問題: **416**

展示を参照してください。

```
vlan 222
 remote-span
!
vlan 223
 remote-span
!
monitor session 1 source interface FastEthernet0/1 tx
monitor session 1 source interface FastEthernet0/2 rx
monitor session 1 source interface port-channel 5
monitor session 1 destination remote vlan 222
!
```

技術者が monitor session 1 destination remote vlan 233 コマンドを追加すると、どのような結果になりますか?

A. RSPAN トラフィックは VLAN 222 および 223 に送信されます。

B. 2 つの送信先を構成するとエラーが発生します。

C. RSPAN VLAN は VLAN 223 に置き換えられます。

D. RSPAN トラフィックは、VLAN 222 と 223 の間で分割されます。

Answer: C (メーッセージを残す)

最新問題: **417**

エンジニアがサンプル コードを実行すると、ターミナルからこの出力が返されます。この問題を修正するサンプル コードの変更はどれですか?

A. JSON メソッドを load() から load() に変更します。

B. test_json 文字列で明示的に read() メソッドを呼び出します

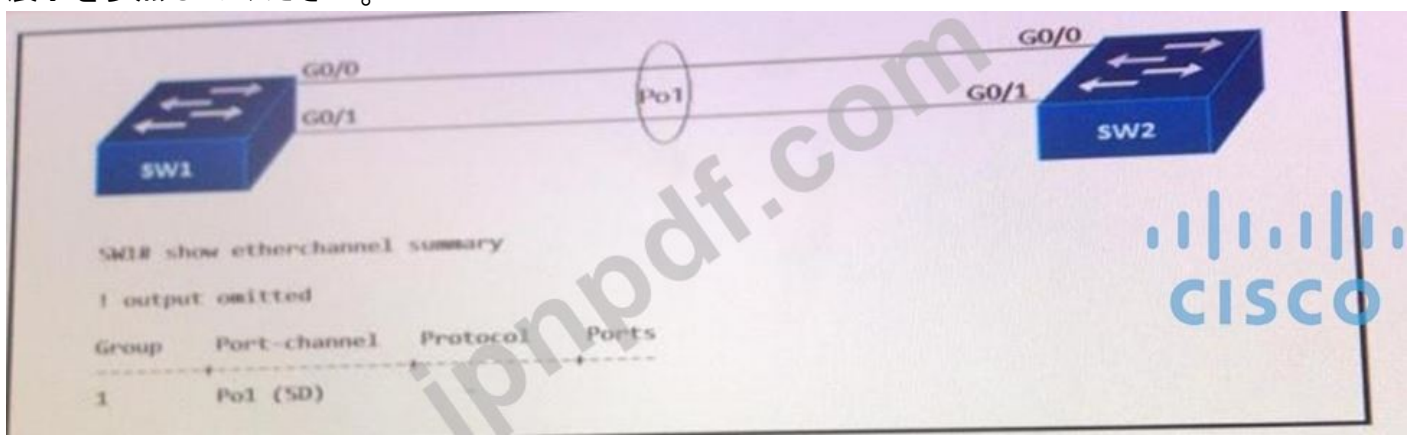
C. 単一の二重引用符のセットを使用し、test_json を 1 行に要約します。

D. test_json 文字列内の null を二重引用符で囲みます

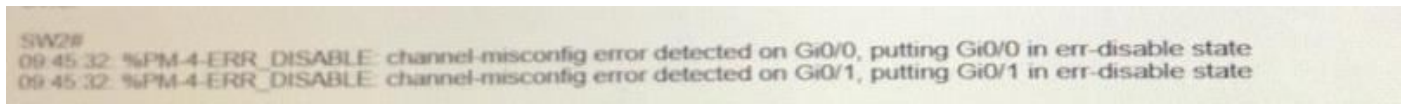
Answer: (解答を表示する**)**

最新問題**: 418**

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 を構成すると、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?

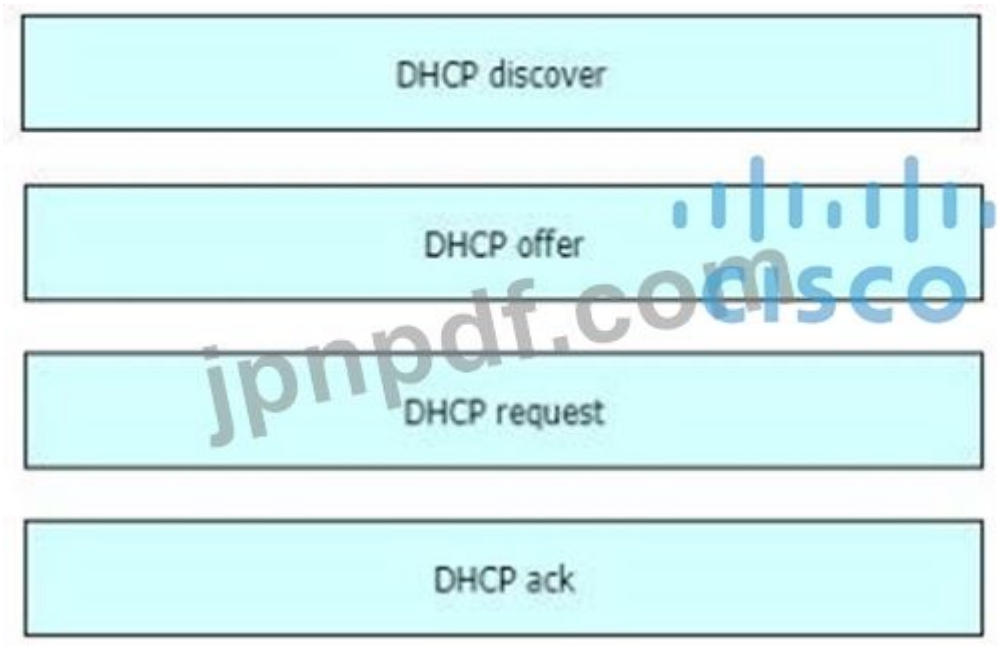
A. スイッチ SW1 と SW2 の EtherChannel で同じプロトコルを構成します。

B. 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。
C. スイッチ SW1 の EtherChannel で正しいポート メンバーを定義します。
D. インターフェイス Gi0/0 スイッチ SW1 の構成エラーを修正します。
Answer: A (メーッセージを残す**)**
この場合、ネゴシエーション プロトコルなしで 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 操作用に構成されていない場合、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、そのループの発生を防止しようとします。

最新問題**: 419**
クライアントと AP の間で交換される DHCP メッセージを、右側の交換される順序にドラッグ アンド ドロップします。

Answer:

説明



DHCP クライアントと DHCP サーバーの間で送信されるメッセージは、DHCPDISCOVER、DHCPO FFER、DHCPREQUEST、および DHCPACKNOWLEDGEMENT の 4 つです。
このプロセスは、多くの場合、DORA (発見、提供、要求、承認) と略されます。

最新問題: 420
展示を参照してください。

```
Router#sh run | b vty

line vty 0 4
 session-timeout 30
 exec-timeout 20 0
 session-limit 30
 login local
line vty 5 15
 session-timeout 30
 exec-timeout 20 0
 session-limit 30
 login local
```

セキュリティ ポリシーでは、すべての idle-exec セッションを 600 秒で終了する必要があります。この目標を達成する構成はどれですか?

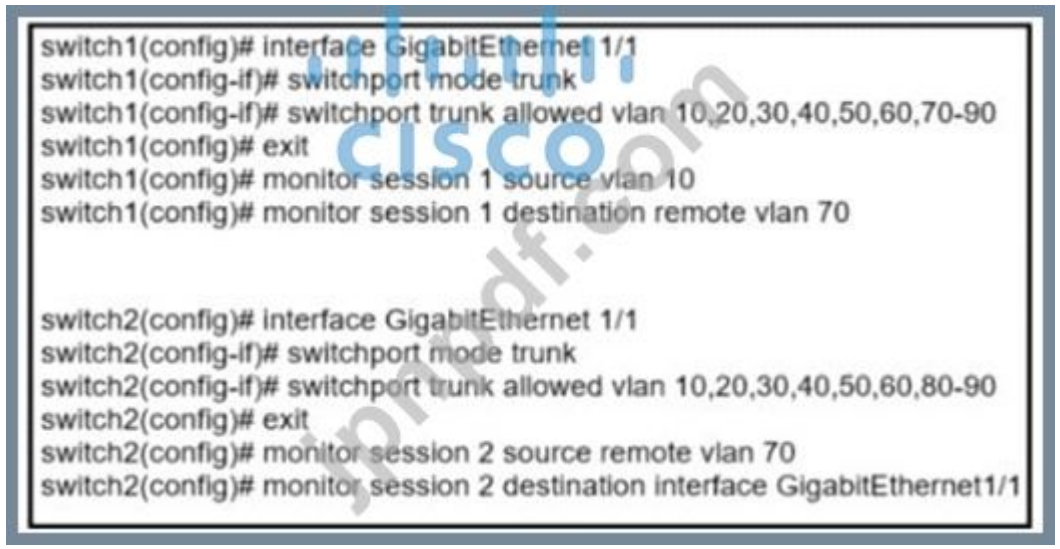
A. 行 vty 0 15 exec-timeout 10 0
B. 行 vty 0 15 exec-timeout
C. 行 vty 0 15 絶対タイムアウト 600
D. 行 vty 0 4 exec-timeout 600

Answer: A (メーッセージを残す**)**

「exec-timeout」コマンドは、コンソール ポートまたは仮想端末で非アクティブ セッションのタイムアウトを設定するために使用されます。このコマンドの構文は次のとおりです。

exec-timeout 分 [秒]
したがって、「exec-timeout 10 0」コマンドを使用して、ユーザーの非アクティブ タイマーを 600 秒 (10 分) に設定する必要があります。

最新問題: **421**
展示を参照してください。



ネットワーク管理者は、スイッチ 1 とスイッチ 2 の間の問題をトラブルシューティングするために RSPAN を構成しました。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ています 外部パケット キャプチャ デバイスは、swich2 インターフェイス GigabitEthernet1/2 に接続されています この設定を完了するために追加する必要がある 2 つのコマンドはどれですか? (2つ選んでください)
A. 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
B. switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-80
C. switch2(config)# monitor session 1 source remote vlan 70 switch2(config)# monitor session 1 destination interface GigabitEthernet1/1
D. switch2(config)# モニター セッション 2 宛先 vlan 10
E. switch2(config)# モニター セッション 1 ソース リモート vlan 70
switch2(config)# モニタ セッション 1 宛先インターフェイス GigabitEthernet1/2
Answer: B,E (メーッセージを残す)
スイッチ 2 は、スイッチ 1 で RSPAN に使用される VLAN 70 を許可していないため、許可する必要があります -> オプション B は正しいです (ただし、VLAN 81 から 90 は通過できません)。
「外部パケット キャプチャ デバイスが switch2 インターフェイス GigabitEthernet1/2 に接続されている」ため、Gi1/2 を宛先ポートとして構成する必要があります。
参考までに、これは 2 つのスイッチでリモート SPAN (RSPAN) 機能を構成する方法です。スイッチ 1 の FastEthernet0/1 のトラフィックは、VLAN 40 経由でスイッチ 2 の Fa0/10 に送信されます。
+ 両方のスイッチで設定
Switch1,2(config)#vlan 40
Switch1,2(config-vlan)#remote-span
+ Switch1 で設定
Switch1(config)# モニタ セッション 1 ソース インターフェイス FastEthernet 0/1
Switch1(config)# モニタ セッション 1 宛先リモート VLAN 40
+ Switch2 で構成する

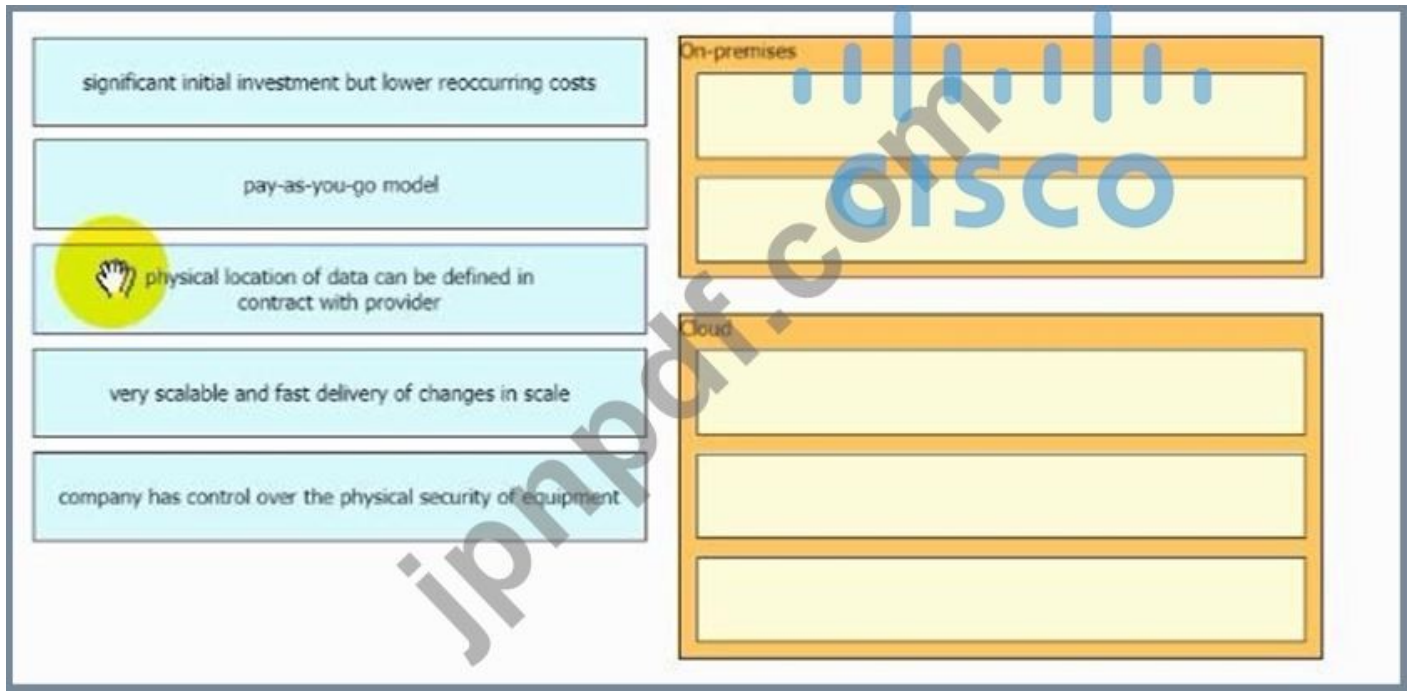
Switch2(config)#monitor セッション 5 ソース リモート VLAN 40
Switch2(config)# モニタ セッション 5 宛先インターフェイス FastEthernet 0/10

有効な **350-401** 問題集は GoShiken.com が提供された合格しやすい 350-401 試験問題集！ GoShiken.com が最新の **350-401** 試験問題集を提供しています。GoShiken.com 350-401 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 350-401 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **422**
Cisco SD-Access アンダーレイ ネットワークを設計する際の考慮事項は何ですか?
A. エンド ユーザーのサブネットとエンドポイントは、アンダーレイ ネットワークの一部です。
B. アンダーレイ スイッチは、エンドポイントの物理接続をユーザーに提供します。
C. スタティック ルーティングが必要です。
D. IPv4 および IPv6 アンダーレイ ネットワークをサポートする必要があります。
Answer: B (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#Underlay

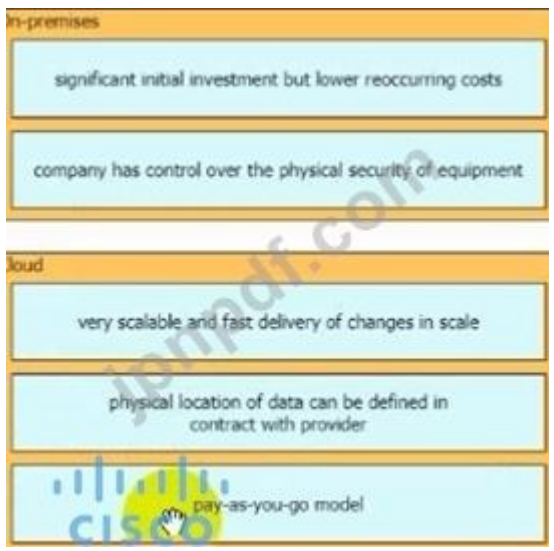
最新問題: **423**
Type 1 ハイパーバイザーの代わりに Type 2 ハイパーバイザーを使用する利点は何ですか?
A. アプリケーションのパフォーマンスの向上
B. 基盤となる OS が削除されるため、セキュリティが向上します。
C. 密度とスケーラビリティの向上
D. 他の OS を実行しているハードウェア上で動作する機能
Answer: (解答を表示する**)**
ハイパーバイザーには、タイプ 1 ハイパーバイザーとタイプ 2 ハイパーバイザーの 2 種類があります。
タイプ 1 ハイパーバイザー (またはネイティブ ハイパーバイザー) では、ハイパーバイザーは物理サーバーに直接インストールされます。次に、オペレーティング システム (OS) のインスタンスがハイパーバイザーにインストールされます。タイプ 1 ハイパーバイザーは、ハードウェア リソースに直接アクセスできます。したがって、ホストされたアーキテクチャよりも効率的です。タイプ 1 ハイパーバイザーの例としては、VMware vSphere/ESXi、Oracle VM Server、KVM、および Microsoft Hyper-V があります。
タイプ 1 ハイパーバイザーとは対照的に、タイプ 2 ハイパーバイザー (またはホスト型ハイパーバイザー) は、物理ハードウェアではなく、オペレーティング システム上で実行されます。タイプ 2 ハイパーバイザーの大きな利点は、管理コンソール ソフトウェアが必要ないことです。タイプ 2 ハイパーバイザーの例としては、VMware Workstation (Windows、Mac、および Linux で実行可能) または Microsoft Virtual PC (Windows でのみ実行) があります。
タイプ 1 はより効率的でパフォーマンスが高く、タイプ 2 よりも安全です。これは、オペレーティング システム固有の欠陥や脆弱性がタイプ 1 のベアメタル ハイパーバイザーには存在しないことが多いためです。タイプ 1 はパフォーマンス、スケーラビリティ、および安定性が優れていますが、限られたハードウェアでサポートされています。

最新問題: **424**
特性を左側から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: **425**

Cisco SD-Access 展開でファブリック AP が実行する機能はどれですか?

A. ファブリック内のワイヤレス クライアントの場所を更新します。

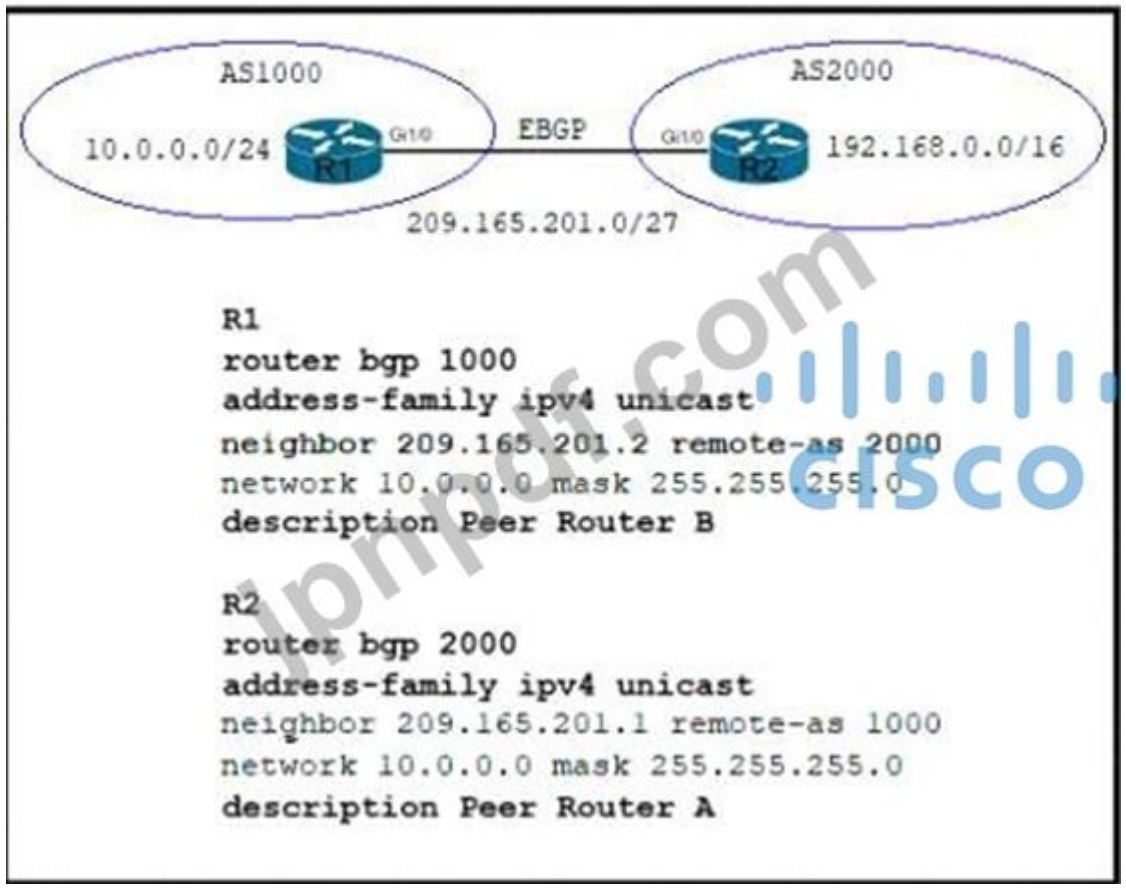
B. ファブリック内のワイヤレス クライアントまでセキュリティ ポリシーを構成します。

C. ワイヤレス クライアントのメンバーシップ情報をファブリックで管理します。

D. ワイヤレス クライアントをファブリックに接続します。

Answer: (解答を表示する**)**

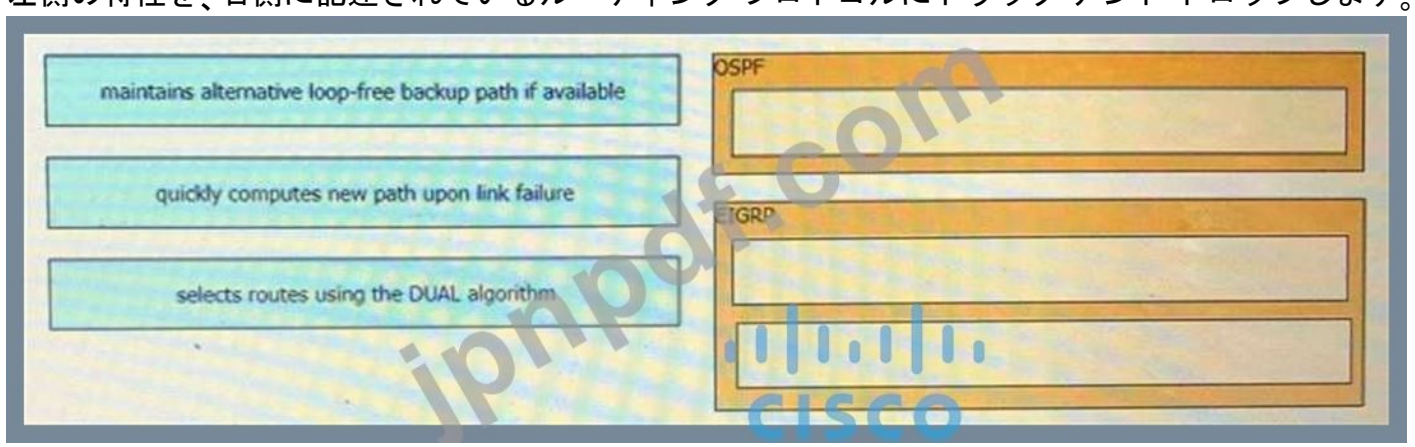
最新問題: **426**



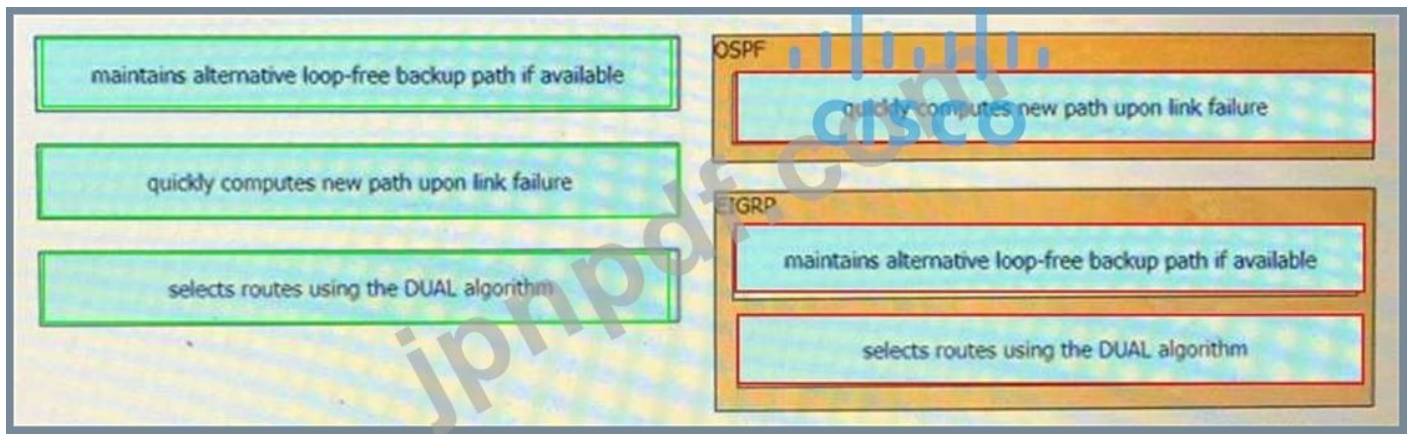
展示を参照してください。AS 1000 と AS 間の完全な到達可能性を可能にするために必要な 2 つのコマンドはどれですか? 2000年? (2つ選んでください)

A. R2#ネットワーク 209.165.201.0 マスク 255.255.192.0
B. R2#ネットワーク 19.168.0.0 マスク 255.255.0.0
C. R1#ネットワークなし 10.0.0.0 255.255.255.0
D. R2#ネットワークなし 10.0.0.0 255.255.255.0
E. R1#ネットワーク 19.168.0.0 マスク 255.255.0.0
Answer: (解答を表示する)

最新問題: **427**
左側の特性を、右側に記述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。



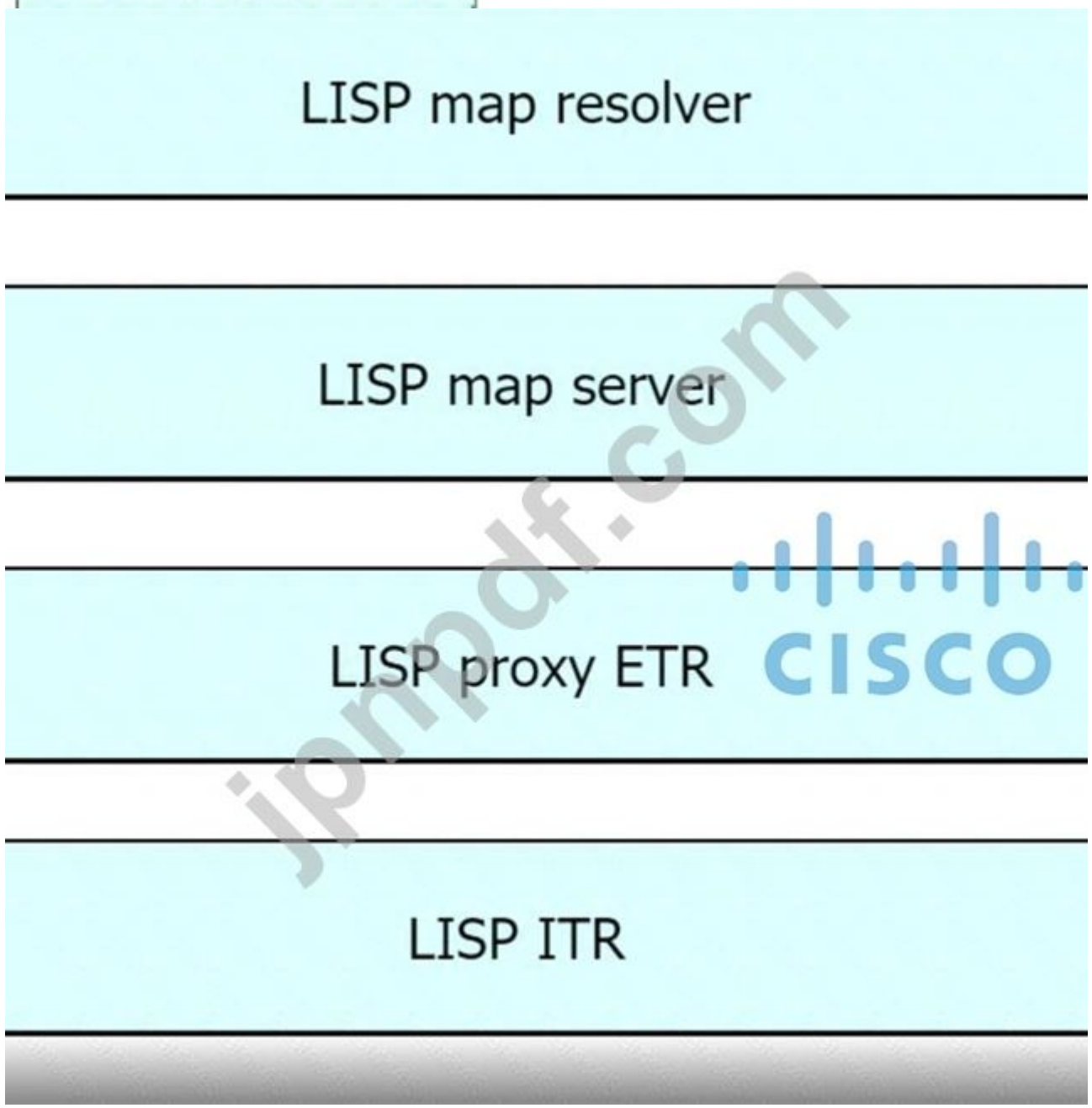
Answer:



最新問題: **428**
ネットワーク管理者は、ルーティング構成の変更を実装しており、変更中のルーティング動作を追跡するためにルーティング デバッグを有効にしています。端末のログ出力が、コマンド入力プロセスを中断しています。
コマンドを誤って入力する可能性を最小限に抑えるために、ネットワーク管理者が実行できるアクションはどれですか? 2つ選んでください。)
A. logging synchronous グローバル コンフィギュレーション コマンドを設定します。
B. TAB キーを押すと、コマンドが新しい行に再表示されます。
C. vty で logging synchronous コマンドを設定します。
D. ロギング区切り機能を構成します。
E. 端末の長さコマンドを使用して、画面の行数を増やします。
Answer: (解答を表示する)

最新問題: **429**
LISP コンポーネントを左側から右側の機能にドラッグ 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: 430
展示を参照してください。

```
ip access-list extended ACL-CoPP-Management
permit udp any eq ntp any
permit udp any any eq snmp
permit tcp any any eq 22
permit tcp any eq 22 any established

class-map match-all CLASS-CoPP-Management
match access-group name ACL-CoPP-Management
```

展示を参照してください。エンジニアは、ルータの CPU を高レートの NTP、SNMP、および SSH トラフィックから保護する必要があります。これらのタイプのトラフィックが継続的に 320 kbps を超える場合にドロップするには、どの 2 つの構成を適用する必要がありますか? (2つ選んでください)

```
R1(config)#policy-map POLICY-CoPP
R1(config-pmap)#class CLASS-CoPP-Management
R1(config-pmap-c)#police 320000 conform-action transmit exceed-action transmit violate-action drop

R1(config)#control-plane
R1(config-cp)# service-policy input POLICY-CoPP

R1(config-pmap)#class CLASS-CoPP-Management
R1(config-pmap-c)#police 32 conform-action transmit exceed-action drop violate-action transmit

R1(config)#control-plane
R1(config-cp)# service-policy output POLICY-CoPP

R1(config)#policy-map POLICY-CoPP
R1(config-pmap)#class CLASS-CoPP-Management
R1(config-pmap-c)#police 320000 conform-action transmit exceed-action drop violate-action drop
```

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

最新問題: **431**
展示を参照してください。

エンジニアは、アクセス ポートからトランクへの SW1 と SW2 の間のポット チャネルを再構成し、すぐに SW1 のログでこのエラーに気付きます。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
```

ハ）

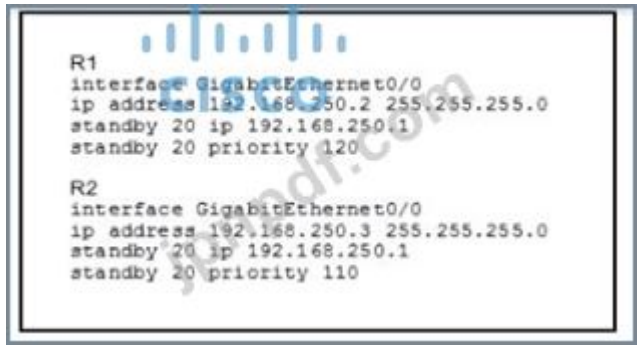
```
SW1(config-if)#interface G0/1
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#shut
SW1(config-if)#no shut
```

D)

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

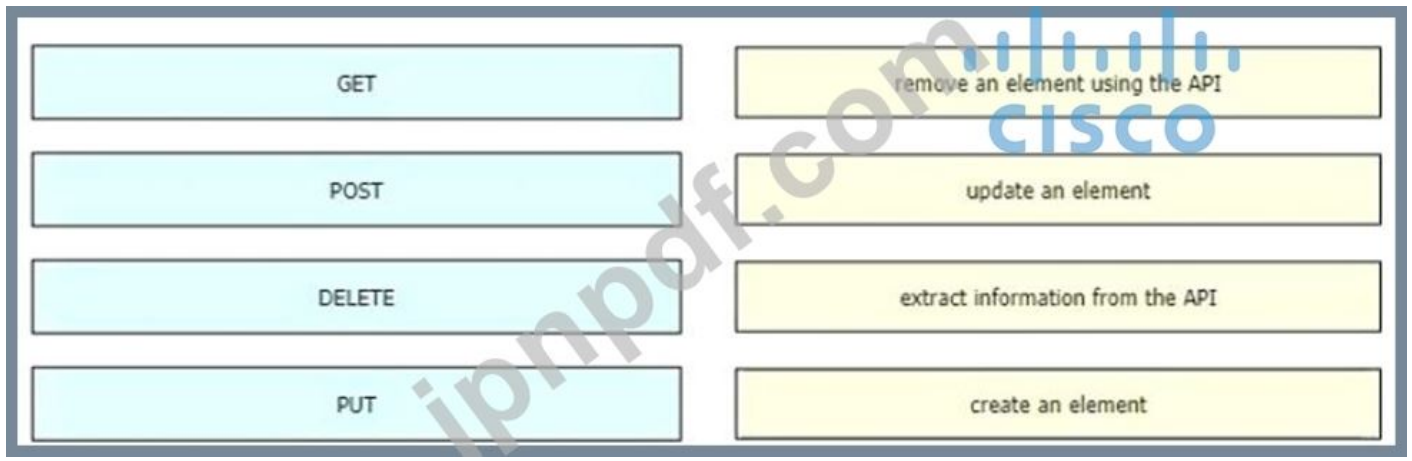
A. オプション B
B. オプション D
C. オプション C
D. オプション A
Answer: (解答を表示する**)**

最新問題**: 432**
展示を参照してください。



この構成の 2 つの効果は何ですか？ 2つ選んでください。）
A. R1 がダウンした場合、R2 はアクティブになりますが、R1 がオンラインに戻るとスタンバイに戻ります。
B. R2 がダウンした場合、R1 はアクティブになりますが、R2 がオンラインに戻るとスタンバイに戻ります。
C. R1 がダウンした場合。R2 がアクティブになり、R1 がオンラインに戻ったときにアクティブ デバイスのままになります。
D. R1 がアクティブ ルーターになります。
E. R1 がスタンバイ ルータになります。
Answer: C,D (メーッセージを残す**)**

最新問題**: 433**
エンジニアが Cisco DNA Center API を使用しています。メソッドを左からドラッグ アンド ドロップして、メソッドが使用されるアクションに右側に配置します。



Answer:

最新問題**: 434**
RESTCONF を使用してネットワーク デバイスに構成を書き込む場合、TLS について正しい記述はどれですか?
A. プロキシ Web サーバーとして機能する NGINX を使用して提供されます。
B. Cisco デバイスではサポートされていません。
C. 認証に証明書が必要でした。
D. HTTP および HTTPS リクエストに使用されます。
Answer: A (メーッセージを残す**)**
デバイスがスタートアップ コンフィギュレーションで起動すると、nginx プロセスが実行されます。NGINX は、プロキシ Web サーバーとして機能する内部 Web サーバーです。Transport Layer Security (TLS) ベースの HTTPS を提供します。HTTPS 経由で送信された RESTCONF リクエストは、最初に NGINX プロキシ Web サーバーによって受信され、さらに構文/セマンティクス チェックのために confd Web サーバーに転送されます。
参照：
ios/prog/configuration/168/b_168_programmability_cg/RESTCONF.html
ステートレス プロトコルである https ベースのプロトコル RESTCONF (RFC 8040) は、安全な HTTP メソッドを使用して、YANG 定義のデータを含む概念的なデータストアで CREATE、READ、UPDATE、および DELETE (CRUD) 操作を提供します -> RESTCONF は HTTP のみを使用します.

最新問題**: 435**
Cisco EAP-FAST について正しいのはどれですか?
A. RADIUS サーバー証明書は必要ありません。
B. クライアント証明書が必要です。
C. IETF 規格です。

D. 透過モードで動作します。
Answer: (解答を表示する**)**
説明
EAP-FAST プロトコルは、強力なパスワード ポリシーを強制できず、デジタル証明書を必要としない 802.1X EAP タイプを展開したいお客様をサポートするためにシスコが開発した、公的にアクセス可能な IEEE 802.1X EAP タイプです。
また、EAP-FAST は、ワイヤレス LAN クライアントまたは RADIUS インフラストラクチャで証明書を必要とせず、組み込みのプロビジョニング メカニズムが組み込まれているため、導入が簡単になるように設計されています。
参照：
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-fixed/72788-CSSC-Deployment-Guide.h

Valid 350-401 Dumps shared by GoShiken.com for Helping Passing 350-401 Exam! GoShiken.com now offer the **newest 350-401 exam dumps**, the GoShiken.com 350-401 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com 350-401 dumps with Test Engine here: https://www.goshiken.com/Cisco/350-401-mondaishu.html (**361** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)