Cisco.300-410.v2024-05-30.q223

試験コード:	300-410
試験名称:	Implementing Cisco Enterprise Advanced Routing and Services
認定資格:	Cisco
無料問題数:	223
バージョン:	v2024-05-30
アクセス数:	923
ページビュー数:	2230
https://www.jpnpdf.com/Cisco.300-410.v2024-05-30.q223-mondaishu.html	

最新問題: **1**
展示を参照してください。

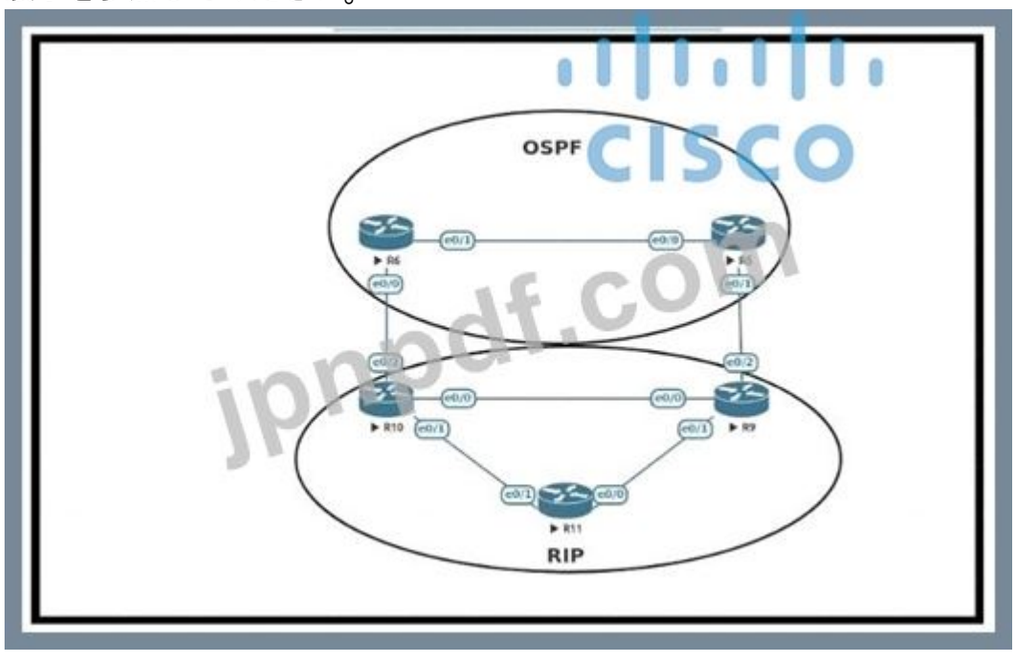
```
Router#show running-config | include ip route
ip route 192.168.2.2 255.255.255.255 209.165.200.225 130
Router#show ip route

<output omitted>

Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.1 is directly connected, Loopback0
      192.168.2.0/32 is subnetted, 1 subnets
O        192.168.2.2[110/11] via 192.168.12.2, 00:52:09, Ethernet0/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Ethernet0/0
L        192.168.12.1/32 is directly connected, Ethernet0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/24 is directly connected, Ethernet0/1
         209.165.200.226/32 is directly connected, Ethernet0/1
```

エンジニアはルーターに静的ルートを設定しますが、宛先へのルートを確認すると、別のネクストホップが選択されます。その理由は何でしょうか?

A. 動的ルーティング プロトコルは常に静的ルートよりも優先されます。
B. OSPF ルートのメトリックがスタティック ルートのメトリックよりも低いです。
C. スタティック ルートに設定された AD は、OSPF の AD よりも上位です。
D. 静的ルートの構文が無効であるため、ルートは考慮されません。
Answer: C (メーッセージを残す)
説明

スタティック ルートの AD は、OSPF ルーターの AD よりも高い 130 に手動で設定されます。
110.

最新問題**: 2**
展示を参照してください。



エンジニアは、R9 および R10 で OSPF を設定し、ルーティング ループを引き起こす OSPF と RIP 間の再配布を設定する必要があります。R9 と R10 のどの設定がこの目的を満たしますか?

A.

```
router ospf 1
 redistribute rip subnets tag 20
!
route-map deny_tag20 permit 10
 match tag 20
route-map deny_tag20 permit 20
!
router ospf 1
distribute-list route-map deny_tag20 in
```

B.

```
router ospf 1
 redistribute rip subnets tag 20
!
route-map deny_tag20 deny 10
 match tag 20
route-map deny_tag20 deny 20
!
router ospf 1
distribute-list route-map deny_tag20 in
```

C.

```
outer ospf 1
redistribute rip subnets tag 20

oute-map deny_tag20 deny 10
match tag 20
oute-map deny_tag20 permit 20

outer ospf 1
distribute-list route-map deny_tag20 i
```

D.

```
router ospf 1
 redistribute rip subnets tag 20
!
route-map deny_tag20 deny 10
 match tag 20
route-map deny_tag20 permit 20
!
router rip 1
distribute-list route-map deny_tag20 in
```

Answer: C (メーッセージを残す)

最新問題: **3**

展示を参照してください。R1 と R2 は EIGRP 隣接関係を確立できません。EIGRP 隣接関係を確立するアクションはどれですか?

A. R1 設定と一致するように、no auto-summary コマンドを R2 設定に追加します。

B. R2 設定と一致するように、passive-interface コマンドを R1 設定に追加します。

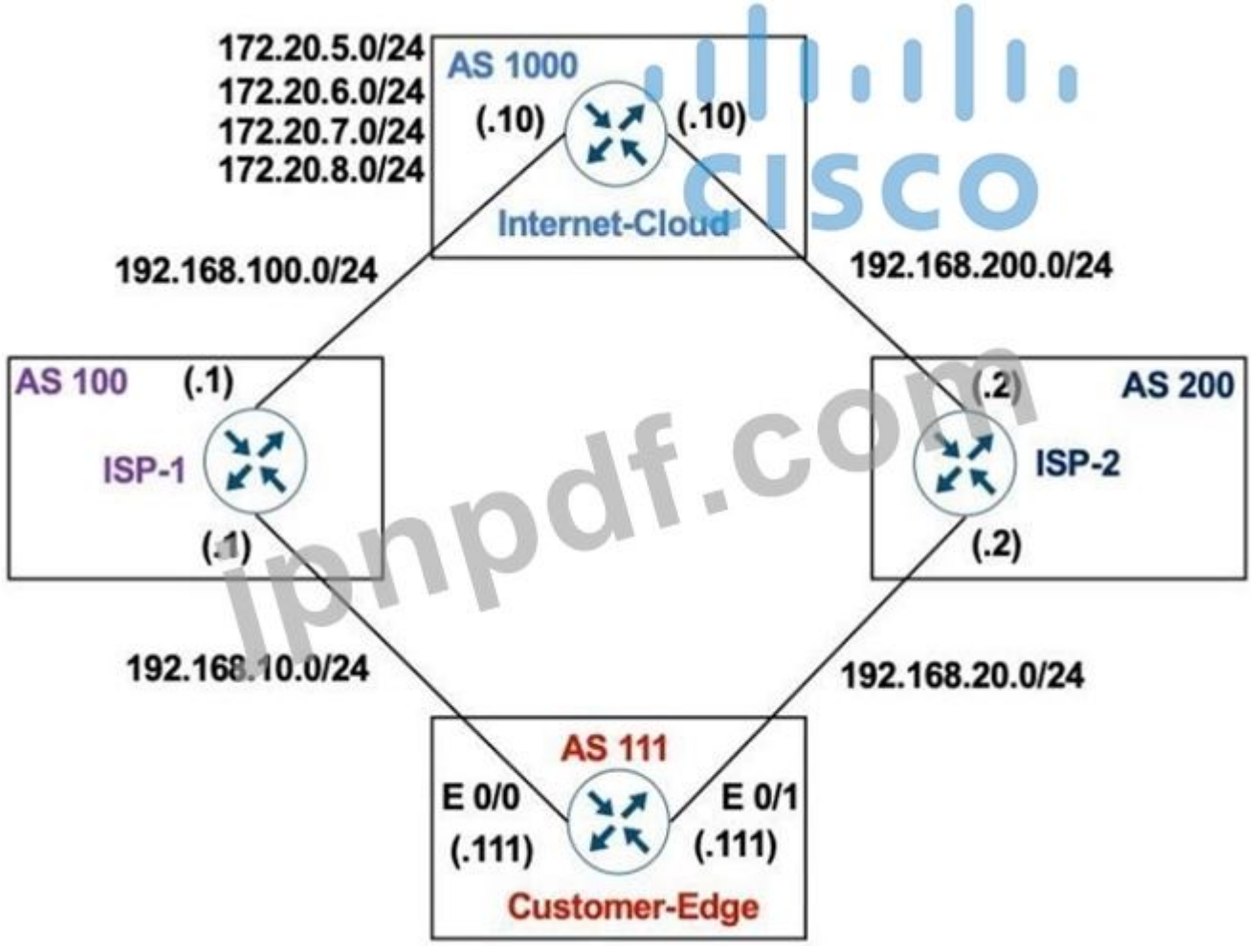
C. いずれかのルーターの現在の自律システム番号を削除し、別の値に変更します。

D. R1 設定と一致するように、R2 設定からpassive-interface コマンドを削除します。

Answer: (解答を表示する**)**

最新問題**: 4**

添付資料を参照してください:



Customer-Edge

```
ip prefix-list PLIST1 permit 172.20.5.0/24
!
route-map SETLP permit 10
 match ip address prefix-list PLIST1
 set local-preference 90
!
router bgp 111
 neighbor 192.168.10.1 remote-as 100
 neighbor 192.168.10.1 route-map SETLP in
 neighbor 192.168.20.2 remote-as 200
```

AS 111 は、AS 200 を 172.20.5.0/24 の優先パスとして使用し、AS 100 をバックアップとして使用したいと考えていました。設定後、AS 100 は他のルートには使用されません。どの構成で問題が解決しますか?

A. ルート mmap SETLP 許可 10
IP アドレス プレフィックス リスト PLIST1 と一致します
ローカル設定を設定する 99
ルートマップ SETLP 許可 20

B. ルートマップ SETLP 許可 10
IP アドレス プレフィックス リスト PLIST1 と一致します
ローカル設定を設定 110
ルートマップ SETLP 許可 20

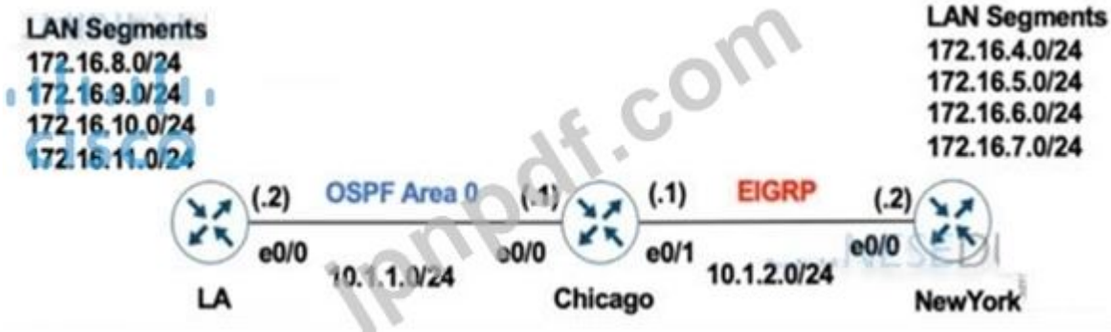
C. ルーター bgp 111
ネイバーなし 192.168.10.1 ルートマップ SETLP
ネイバー 192.168.10.1 ルートマップ SETLP 出力

D. ルーター bap 111
ネイバーなし 192.168.10.1 ルートマップ SETLP
ネイバー 192.168.20.2 ルートマップ SE TLP 入力

Answer: (解答を表示する**)**

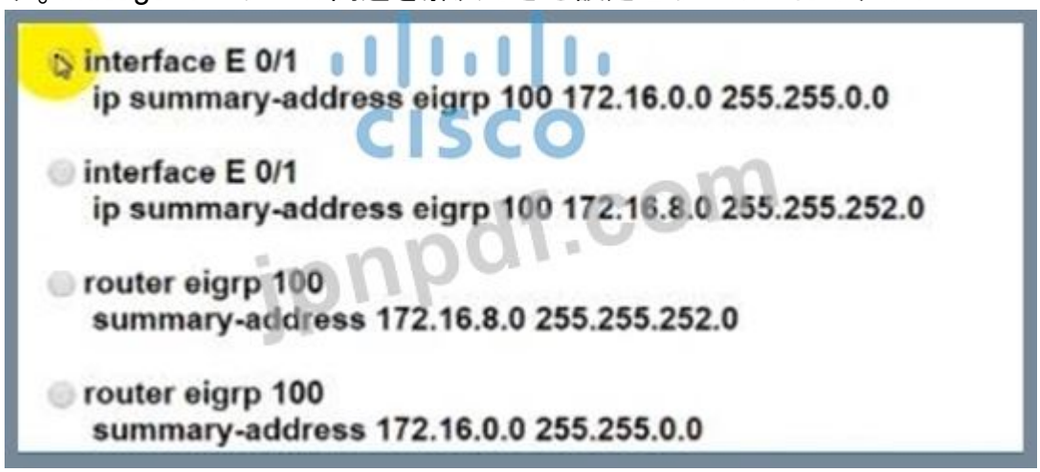
説明
ルートマップの最後には暗黙的な拒否が存在するため、172.20.5.0/24 に一致しない他のトラフィックはすべてドロップされます。したがって、他のトラフィックを許可するには、ルートマップの最後に許可シーケンスを追加する必要があります。
ローカル設定のデフォルト値は 100 であり、より高い値が優先されるため、AS100 のローカル設定を AS200 のローカル設定よりも低く設定する必要があります。

最新問題: **5**
展示を参照してください。



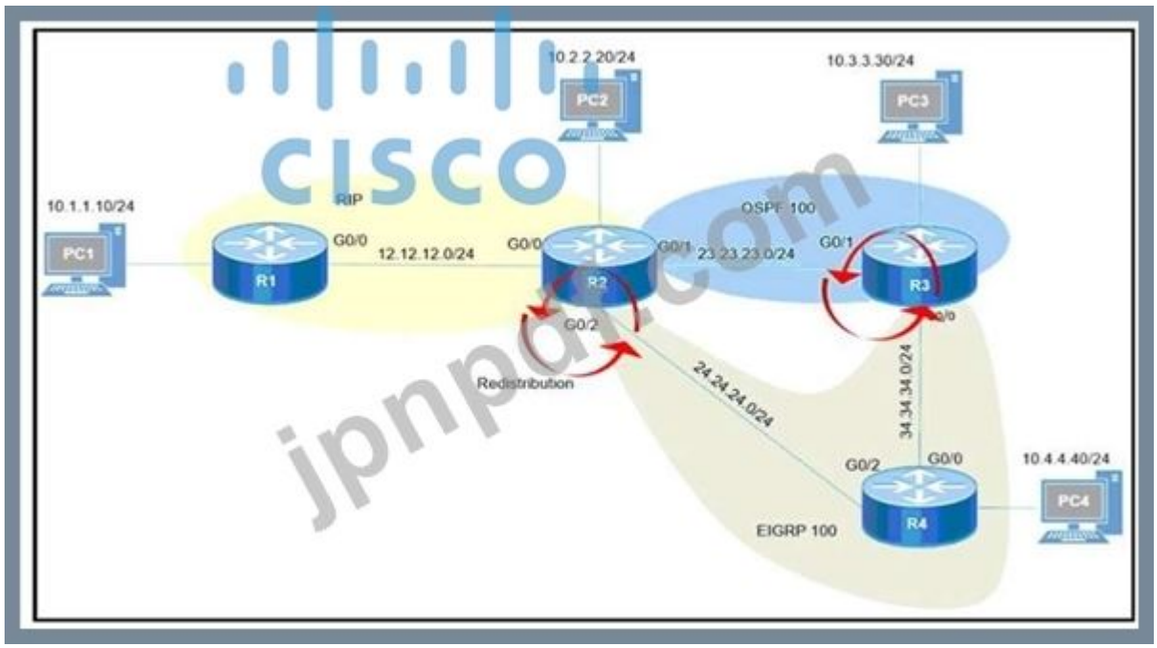
ネットワーク管理者は、OSPF ルートを使用して LA ルートとニューヨーク ルートを相互に再配布し、最長のサマリー マスクを使用して EIGRP で単一のルートとして集約されるようにシカゴ ルータを設定しました。

設定後、ニューヨーク ルーターは、サマリー ルートを除くすべての特定の LA ルートを受信します。Chicago ルーターの問題を解決できる設定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 C
D. オプション B
Answer: D (メーッセージを残す**)**

最新問題**: 6**
展示を参照してください。



ルーティング プロトコル間で再配布が有効になった後。PC2、PC3、および PC4 は PC1 に到達できません。すべての PC にアクセスできるように問題を解決するために、エンジニアはどのようなアクションを実行できますか?

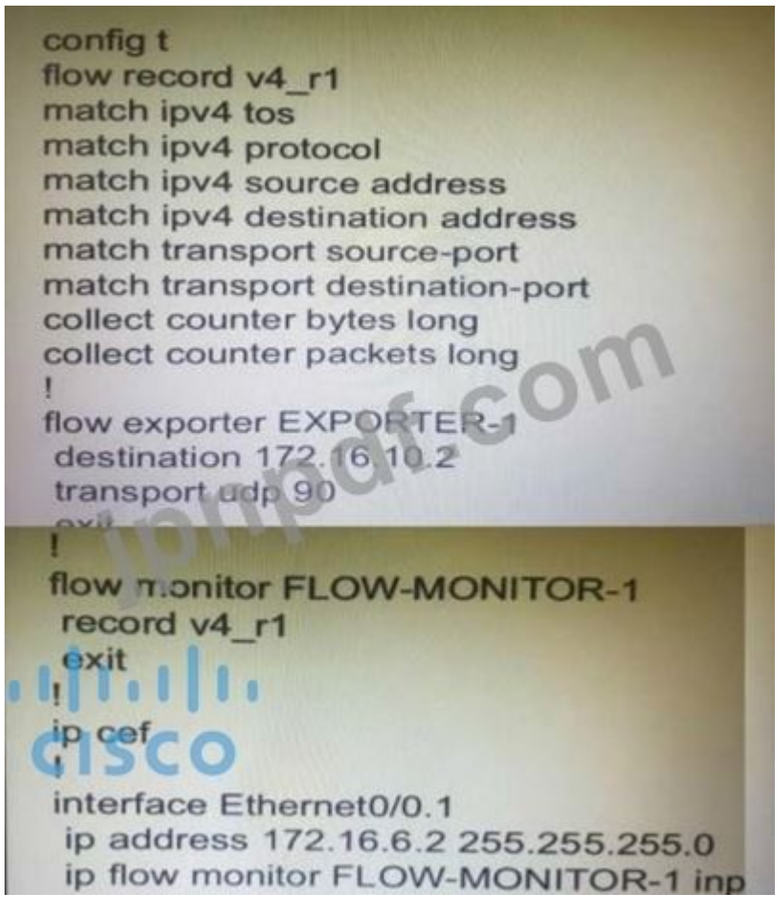
A. R2 上で直接接続されたインターフェイスを再配布します。
B. OSPF から EIGRP に再配布されるときにプレフィックス 10.1.1.0/24 をフィルタリングします。
C. R2 の RIP プロセスでアドミニストレーティブ ディスタンス 100 を設定します。
D. RIP から EIGRP に再配布されるときにプレフィックス 10.1.1.0/24 をフィルタリングします。
Answer: B (メーッセージを残す**)**

最新問題**: 7**
管理者は、TFTP を使用して CPE ルータから Gi0/0 インターフェイス経由で別のデバイスにパック NBAR2 ファイルをダウンロードしようとします。CPE は次のように構成されます。

```
hostname CPE
!
ip access-list extended WAN
<...>
remark => All UDP rules below for WAN ID: S420T92E35F99
permit udp any eq domain any
permit udp any any eq tftp
deny udp any any
!
interface GigabitEthernet0/0
<...>
ip access-group WAN in
<...>
!
tftp-server flash:pp-adv-csr1000v-1612.1a-37-53.0.0.pack
```

転送は失敗します。どのアクションで問題が解決しますか?
A. ファイル名を 8+3 の命名規則に短縮します。
B. UDP 宛先ポート範囲全体を許可するように WAN ACL を変更します。
C. WAN ACL を変更して、UDP ポート 69 で TFTP を許可します。
D. permit udp any eq tftp any エントリを WAN ACL の最後のエントリにします。
Answer: D (メーッセージを残す**)**

最新問題**: 8**
展示を参照してください。



AS 690 のルーターの複数の近隣ルーターから BGP ルーティング アップデートを受信するルーター。ルーターが依然として AS 690 宛てのトラフィックを 10.222.10.1 以外のネイバーに送信する理由は何ですか?

A. 別の近隣ステートメントのローカル優先値が 250 を超えています。

B. ローカル プリファレンス値は、ルート マップの重みと同じ値に設定する必要があります。

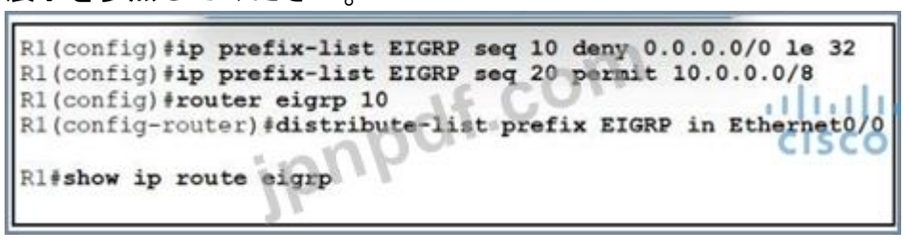
C. ルート マップが間違った方向に適用されています。

D. 別のステートメントの重み値が 200 を超えています。

Answer: C (メーッセージを残す**)**

最新問題**: 9**

展示を参照してください。

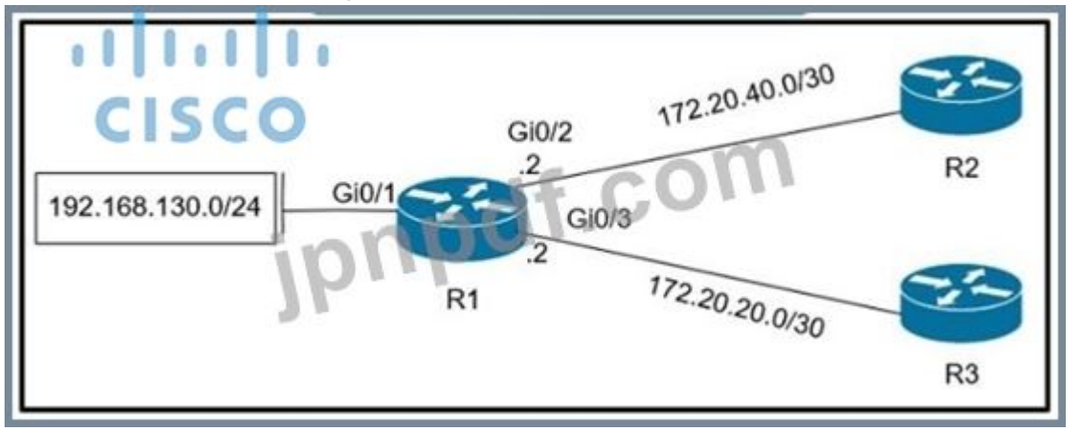


ネットワーク 10 プレフィックスを除く、EIGRP プロセスに受信するルートをフィルタリングするためにプレフィックス リストが作成されます。プレフィックス リストが適用されると、EIGRP からのルーティング テーブルにネットワーク 10 プレフィックスが表示されなくなります。どの構成で問題が解決しますか?

A. ip prefix-list EIGRP seq 5 許可 10.0.0.0/8 ge 9 no ip prefix-list EIGRP seq 20 許可 10.0.0.0/8

B. ip prefix-list EIGRP seq 20 許可 10.0.0.0/8 ge 9.
C. ip プレフィックス リスト EIGRP seq 20 許可 10.0.0.0/8 ge 9 ip プレフィックス リスト EIGRP seq 10 許可 0.0.0.0/0 le 32
D. ip プレフィックス リスト EIGRP シーケンス 10 許可 0.0.0.0/0 ル 32
Answer: D (メーッセージを残す)

最新問題**: 10**
展示を参照してください。



R1 のどのポリシー設定が、192 168 130 0'24 ネットワークから送信されたトラフィックを R2 に転送しますか?

A.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.2
```

B.

C.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.1
```

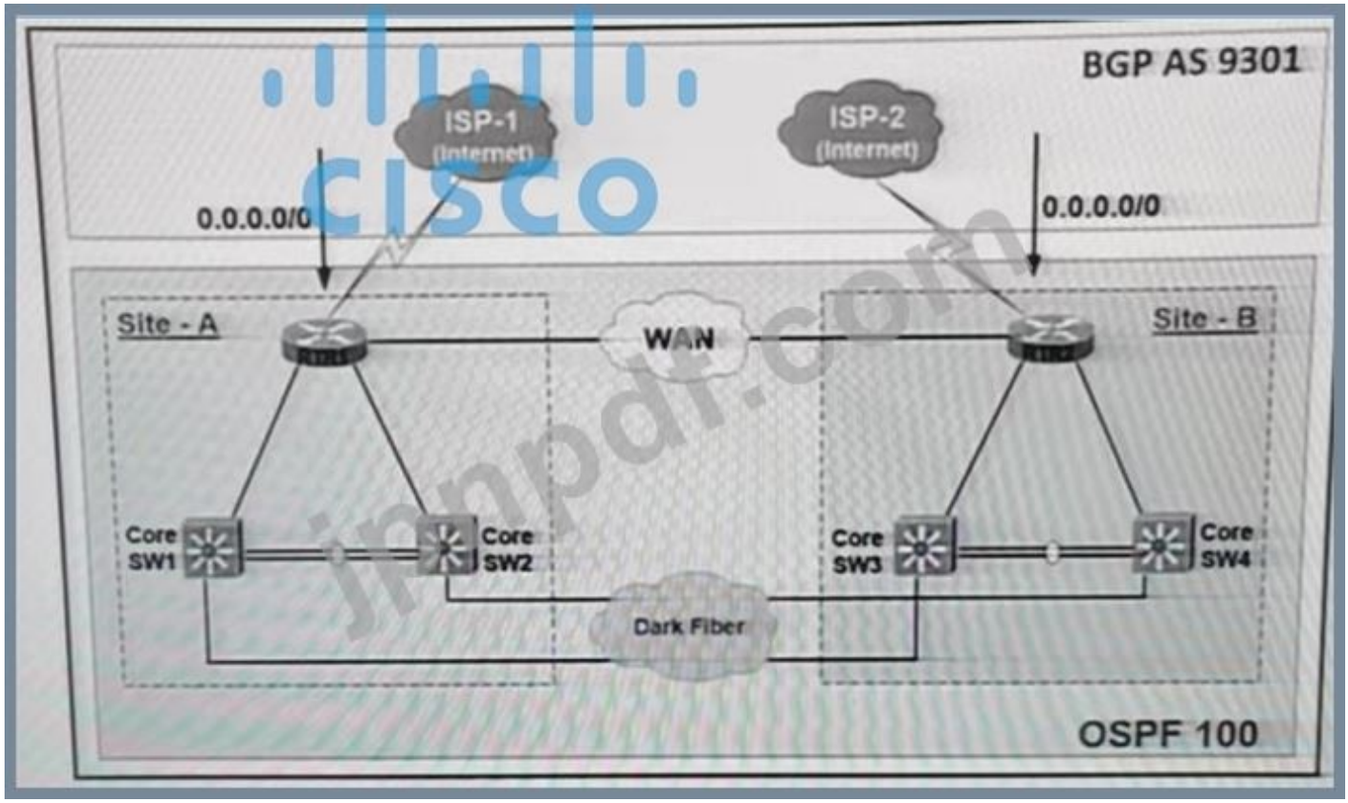
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.2
```

D.

Answer: (解答を表示する**)**

最新問題**: 11**

展示を参照してください。



リンクと BGP 接続が稼働している場合、インターネット トラフィックは常にサイト A ISP-1 を優先する必要があります。それ以外の場合、すべてのインターネット トラフィックは ISP-2 に送信される必要があります。再配布は BGP ルーティング プロトコルと OSPF ルーティング プロトコルの間で構成されており、期待どおりに機能しません。どのようなアクションをとれば問題が解決しますか?

A. サイト A RTR1 でメトリック タイプ 2 を設定し、サイト B RTR2 でメトリック タイプ 1 を設定します。

B. サイト A RTR1 で OSPF コスト 100 を設定し、サイト B RTR2 で OSPF コスト 200 を設定します。

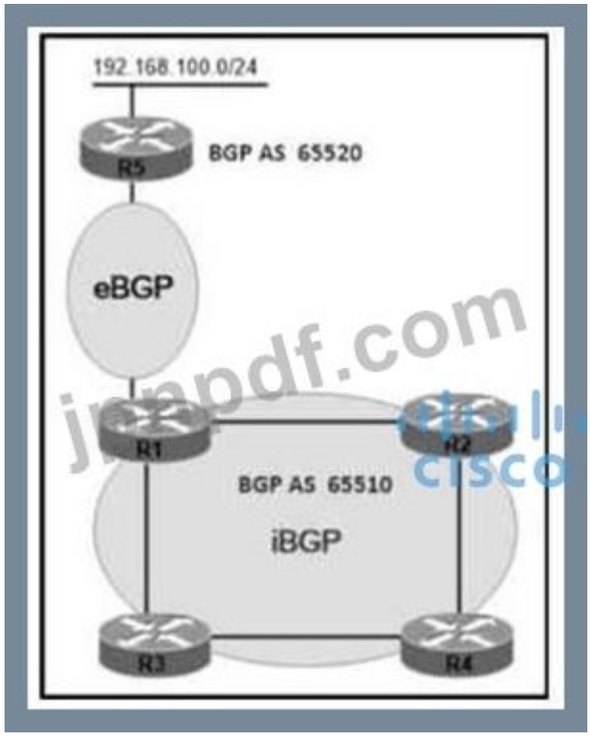
C. サイト A RTR1 で OSPF コスト 200 を設定し、サイト B RTR2 で OSPF コスト 100 を設定します。

D. サイト A RTR1 でメトリック タイプ 1 を設定し、サイト B RTR2 でメトリック タイプ 2 を設定します。

Answer: (解答を表示する**)**

説明
OSPF タイプ 1 ルートは、同じ宛先に対してタイプ 2 ルートよりも常に優先されるため、サイト A RTR1 でメトリック タイプ 1 を設定して、サイト B RTR2 よりも優先されるようにすることができます。
注記：
ルートは OSPF でタイプ 1 (E1) ルートまたはタイプ 2 (E2) ルートとして再配布されます。タイプ 2 がデフォルトです。
- タイプ 1 ルートのメトリックは、内部 OSPF コストと外部再配布コストの合計です。
- タイプ 2 ルートのメトリックは、再配布コストのみとなります。
- ルートがタイプ 2 として OSPF に再配布される場合、OSPF ドメイン内のすべてのルーターは外部ネットワークに到達するために同じコストがかかります。
- ルートがタイプ 1 として OSPF に再配布される場合、外部ネットワークに到達するコストはルーターごとに異なる可能性があります。

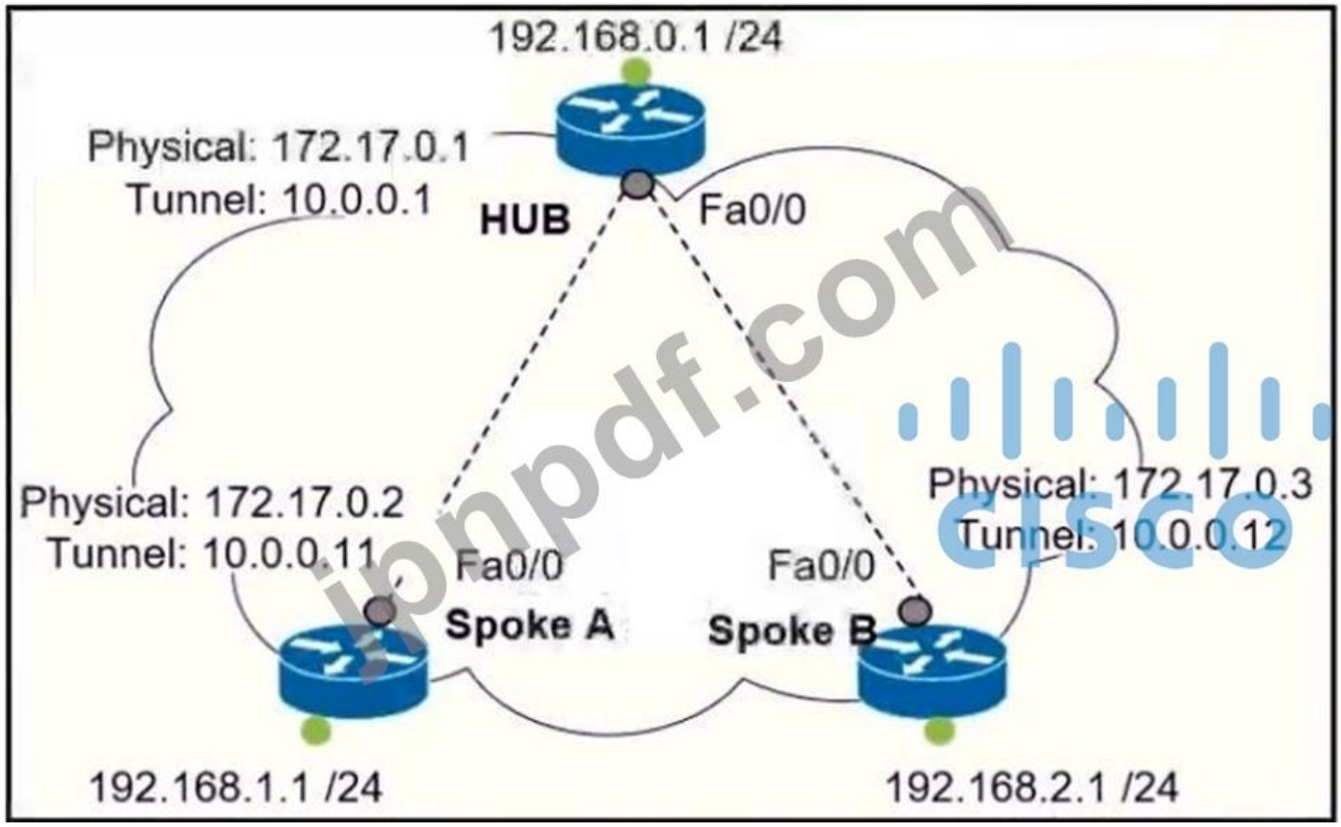
最新問題: **12**
展示を参照してください。



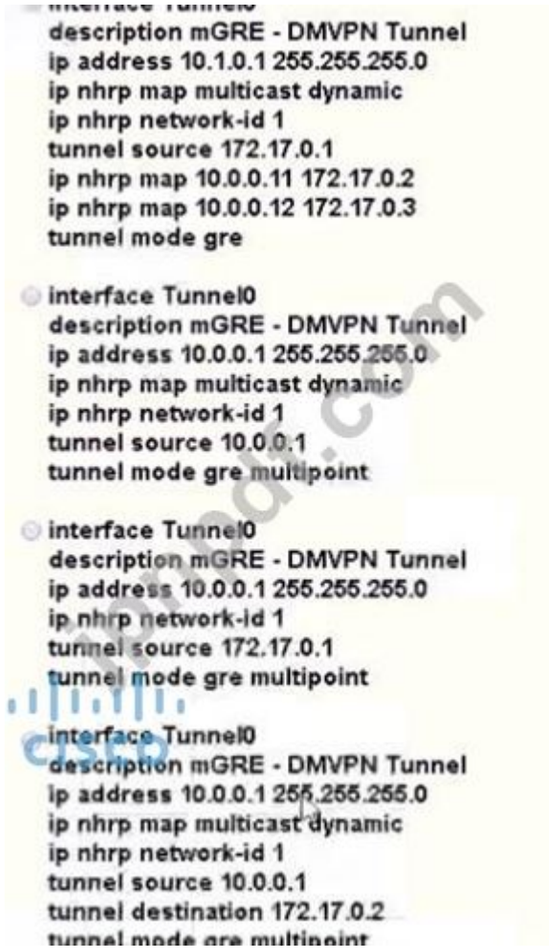
AS65510 iBGP は、直接接続されたネイバー用に構成されています。R4 はネットワーク 192 に ping またはtraceroute を送信できません
168.100.0/24 この問題はどのアクションで解決しますか?
A. R4 をルート リフレクター サーバーとして設定し、R2 と R3 をルート リフレクター クライアントとして設定します。
B. R1 をルート リフレクター サーバーとして構成し、R2 と R3 をルート リフレクター クライアントとして構成します。
C. R1 をルート リフレクター サーバーとして構成し、R4 をルート リフレクター クライアントとして構成します。

D. R4 をルート リフレクター サーバーとして構成し、R1 をルート リフレクター クライアントとして構成します。
Answer: D (メーッセージを残す**)**

最新問題**: 13**
展示を参照してください。



MVPN with mGRE モードを有効にするには、HUB ルータでどのインターフェイス設定を設定する必要がありますか?



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: C (メーッセージを残す**)**
説明
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-m

最新問題**: 14**
展示を参照してください。

```
P 172.29.0.0/16, 1 successors, FD is 307200, serno 2
        via 192.168.254.2 (307200/281600), FastEthernet0/1
        via 192.168.253.2 (410200/352300), FastEthernet0/0
```

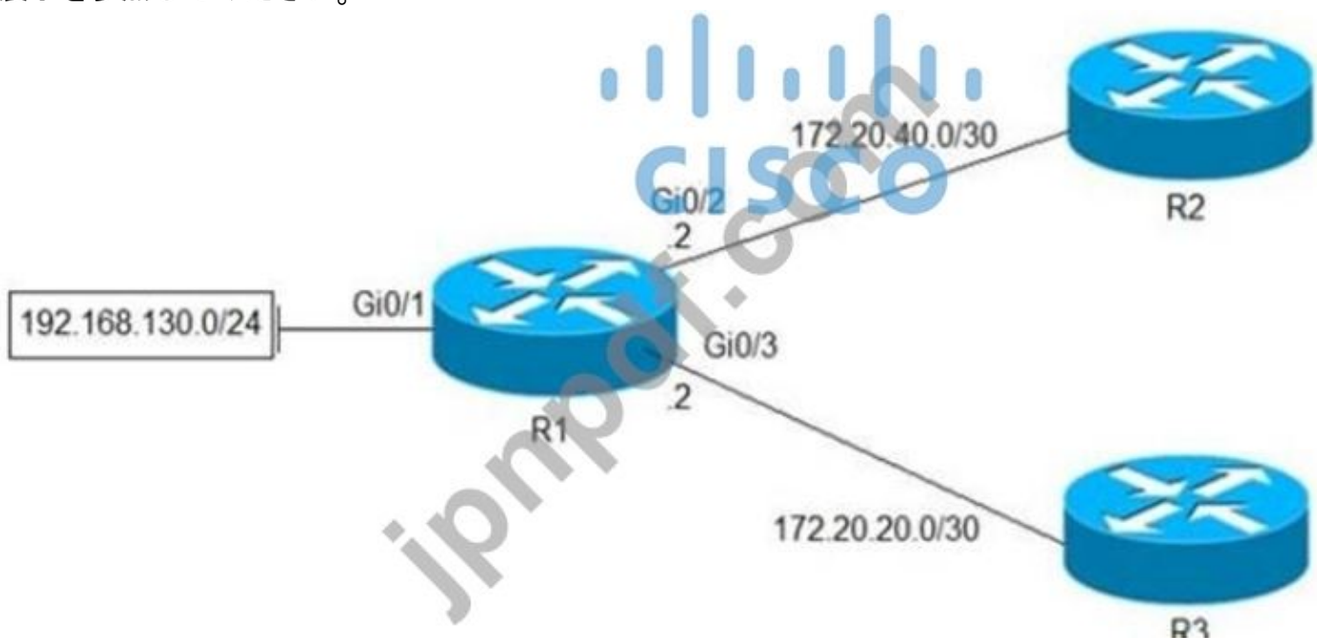
FastEthemet0/1 がダウンすると、192.168.253 2 を経由する 172.29.0 0/16 へのルートが RIB にインストールされません。
どのアクションで問題が解決しますか?
A. 報告される距離を実現可能な距離よりも大きく設定します。
B. 後続の実行可能距離よりも大きな実行可能距離を設定します。

C. 後続の実行可能距離よりも大きい報告距離を設定します。
D. 報告された距離よりも大きい実行可能な距離を構成します
Answer: D (メーッセージを残す)
説明
表示から、ネットワーク 172.29.0.0/16 が 2 つのルート経由で学習されたことがわかります。
+ 192.168.254.2 から FD = 307200 および AD = 281600
+ 192.168.253.2 から FD = 410200 および AD = 352300
最初のルートは、FD が低いため、後続ルートとして RIB にインストールされます。
最初のルートが失敗すると、ルータは実現可能条件を満たさないため、2 番目のルートを使用しません。
実現可能条件では、ルートのアドバタイズドディスタンス (AD、報告距離とも呼ばれる) が、現在の後続ルートの実現可能距離よりも短くなければならないと規定されています。

最新問題: **15**
PE ルーターは MPLS VPN 内で Ipv4 プレフィックスを何に変換しますか?
A. 64 ビットのルート識別子と組み合わせた VPN-IPv4 プレフィックス
B. IP と PE ルーター ID を組み合わせた 48 ビットのルート
C. ASN、PE ルーター ID、および IP プレフィックスを組み合わせたプレフィックス
D. PE セッションと CE セッション間の eBGP パスの関連付け
Answer: A (メーッセージを残す)

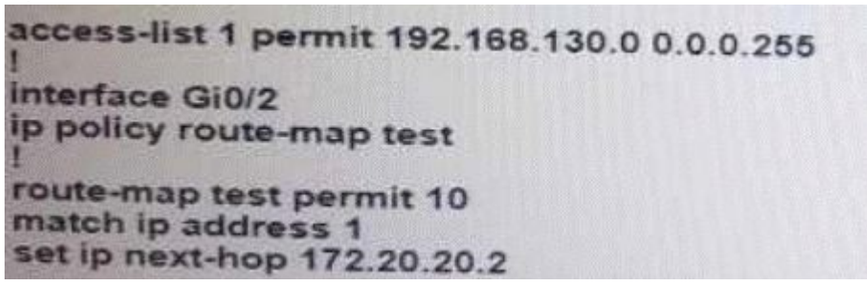
The IP prefix is a member of the IPv4 address family. After the PE device learns the IP prefix, the PE converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher (RD). The generated prefix is a member of the VPN-IPv4 address family. It uniquely identifies the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses. The route distinguisher used to generate the VPN-IPv4 prefix is specified by a configuration command associated with the virtual routing and forwarding (VRF) instance on the PE device.

最新問題: **16**
展示を参照してください。

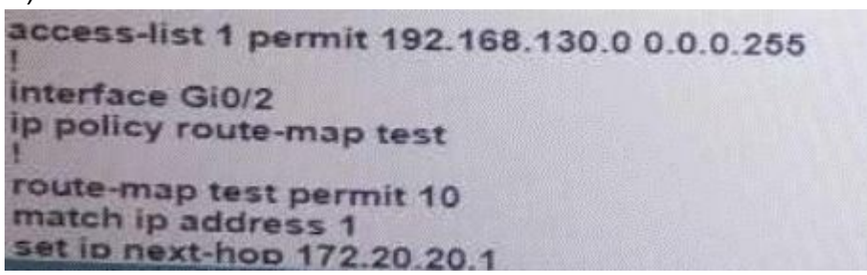


192.168.130.0/24 ネットワークから送信されたトラフィックを 17.20.20.0/30 ネットワークに転送するように R1 上のポリシーを構成する構成はどれですか?

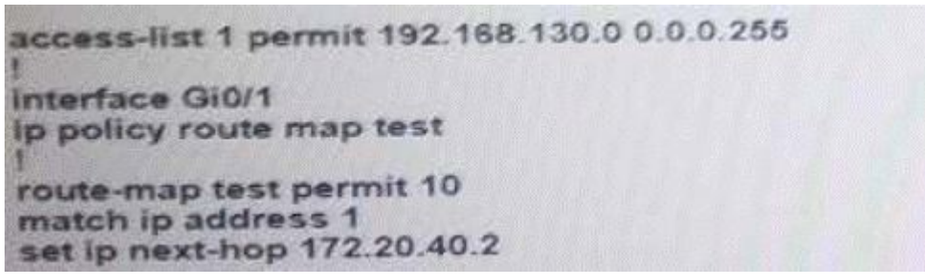
A)



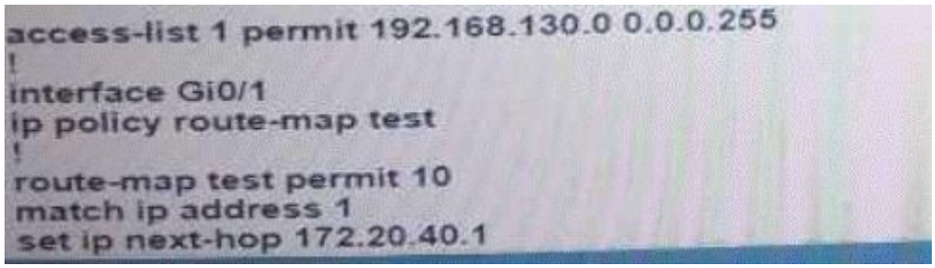
B)



C)



D)



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

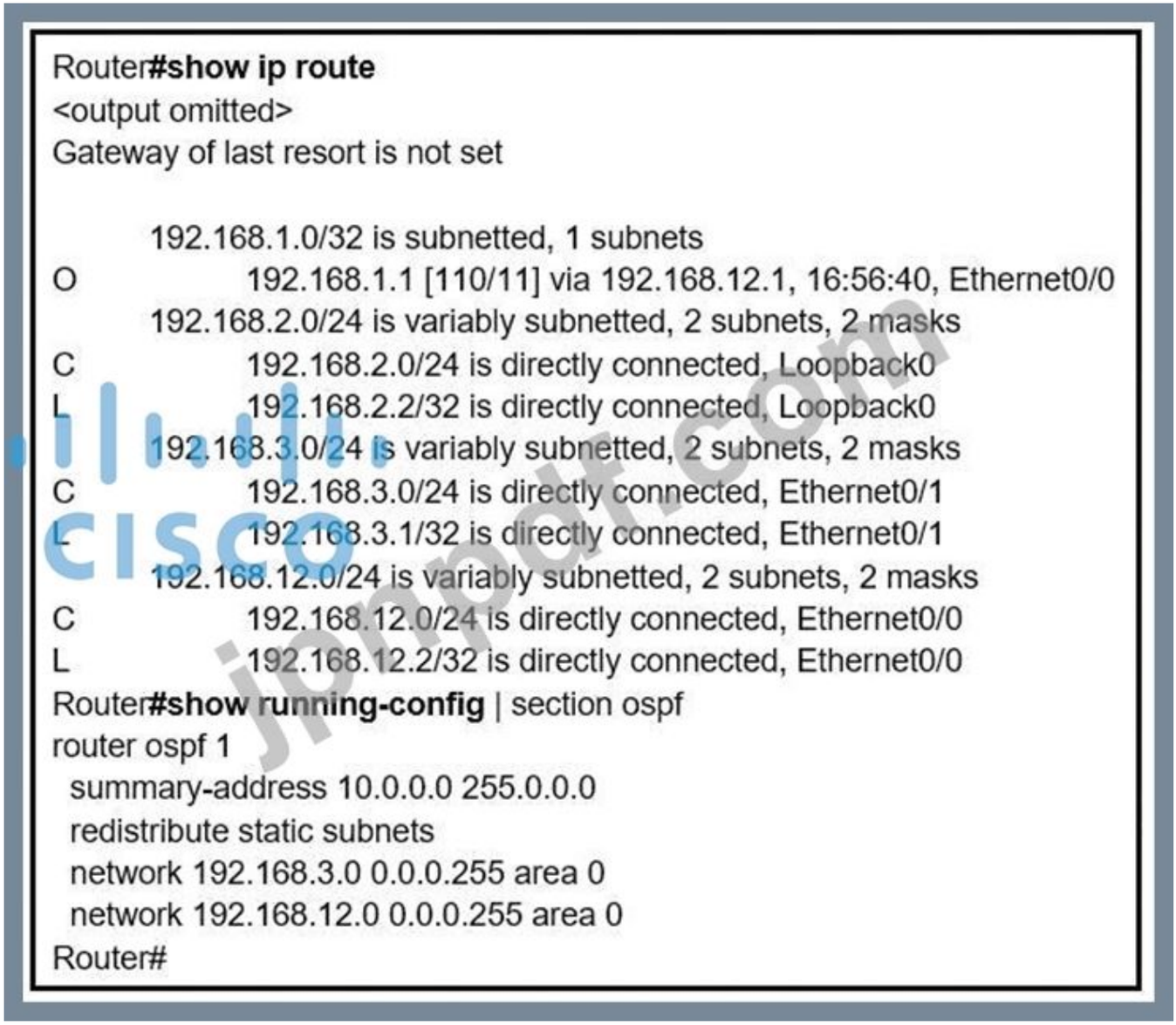
最新問題: **17**

左側のアドレスを右側の適切な IPv6 フィルターの目的にドラッグ アンド ドロップします。

Answer:

最新問題: **18**

展示を参照してください。



エンジニアは OSPF でネットワーク 10.0.0.0/8 のサマリー ルートを生成しようとしていますが、サマリー ルートがルーティング テーブルに表示されません。概要ルートが欠落しているのはなぜですか?

A. summary-address コマンドは、エリア間のプレフィックスを要約するためにのみ使用されます。

B. サマリー ルートは OSPF データベースでのみ表示され、ルーティング テーブルでは表示されません。

C. 10.0.0.0/8 内のサブネットのルートがないため、要約ルートは生成されません。

D. サマリー ルートはこのルーターでは表示されませんが、同じエリア内の他の OSPF ルーターでは表示されます。

Answer: C (メーッセージを残す**)**

説明

summary-address は、自律システム境界で OSPF の集約アドレスを作成するためにのみ使用されます。つまり、このコマンドは、別のプロトコル ドメインから外部に再配布されたルートを要約しようとしている場合、または NSSA エリアがある場合に ASBR でのみ使用する必要があります。ただし、要約ルートを作成するには次の要件があります。

ASBR は、サマリー ルートのアドレス範囲と、その ASBR 上の OSPF に再配布されたすべてのルートを比較して、下位サブネット (サマリー ルート範囲内にあるサブネット) を見つけます。少なくとも 1 つの下位サブネットが存在する場合、ASBR は要約ルートをアドバタイズします。

最新問題: **19**
展示を参照してください。エンジニアが R3 ループバック アドレス経由で R1 にログインしようとしています。どのアクションで問題が解決しますか?
A. Telnet をブロックしている IPv6 トラフィック フィルターを R1 から削除します。
B. トランスポート入力の追加なし
C. トランスポート入力 SCP を追加します
D. SSH をブロックしている IPv6 トラフィックを R1 から削除します。
Answer: A (メーッセージを残す**)**

最新問題: **20**
展示を参照してください。

EIGRP から OSPF ルーティング プロトコルに再配布されるサブネットはどれですか?
A. 10.2.3.0/26
B. 10.1.2.0/24
C. 10.2.2.0/24
D. 10.1.4.0/24
Answer: C (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。

展示を参照してください。管理者は、conf Me パッケージを FTP サーバーにアップロードする必要があります。ただし、FTP サーバーは匿名サービスを拒否し、ユーザーに認証を要求しました。問題を解決する 2 つの方法は何ですか? (2つお選びください。)

A. 代わりに copy flash:packages.conf scp: コマンドを使用し、プロンプトが表示されたら FTP サーバーの認証情報を入力します。

B. 代わりに copy flash-packages conf ftp: コマンドを使用し、プロンプトが表示されたら FTP サーバーの credent-ais を入力します。

C. is ftp username および ip ftp passwd 設定コマンドを使用して、有効な FTP サーバー資格情報を指定します。

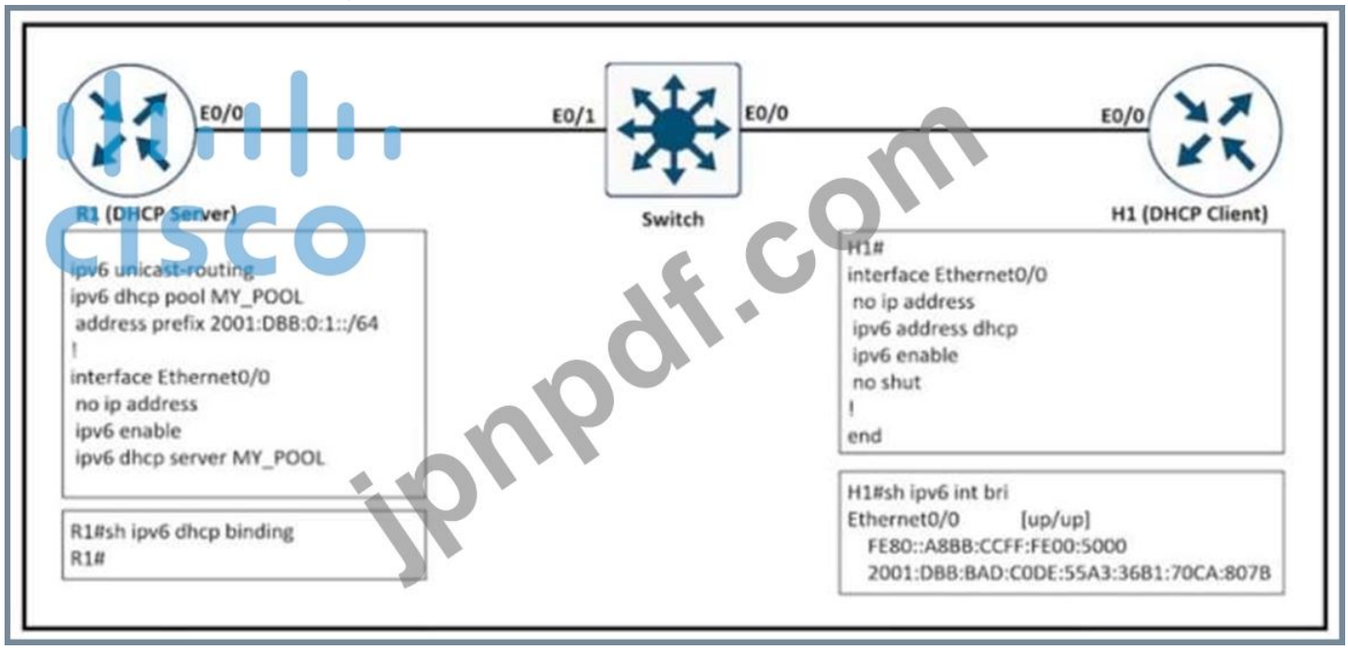
D. FTP サーバー上のユーザー名とパスワードに一致するユーザーを rooter 上に作成し、コピーを試行する前にログインします。

E. ftp://username:passwordQ192.0.2.40/ 構文を使用して、FTP URL に FTP サーバーの資格情報を直接入力します。

Answer: (解答を表示する**)**

最新問題**: 22**

展示を参照してください。

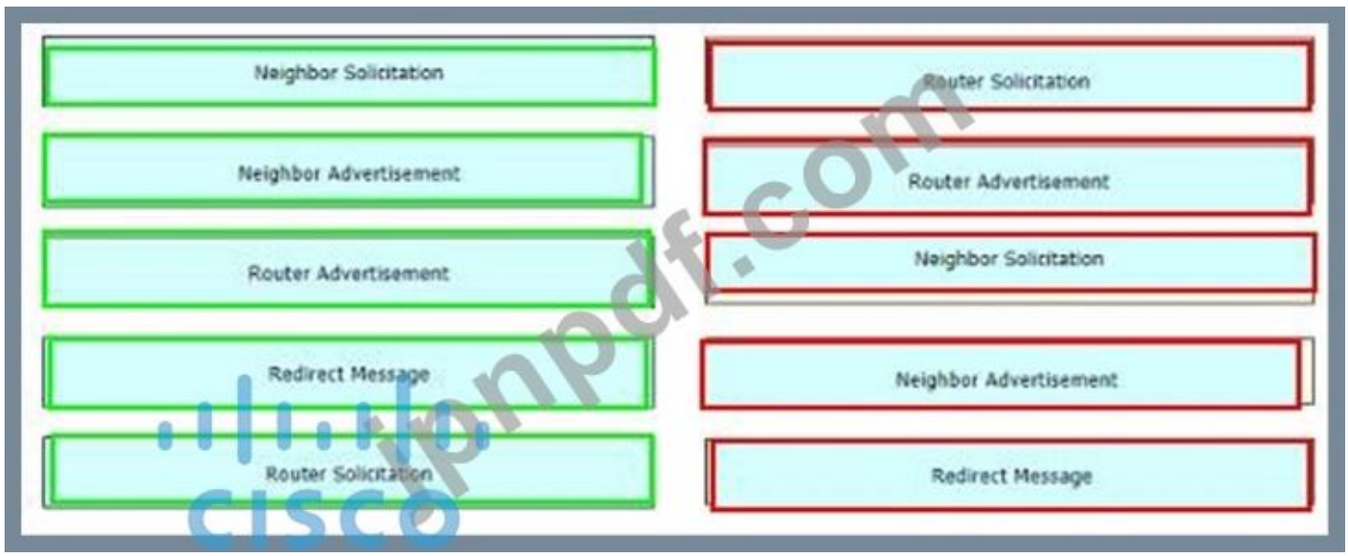


展示を参照してください。クライアント サーバーではありますが、show コマンドではサーバー上の IPv6 DHCP バインディングが表示されません。どのアクションで問題が解決しますか?

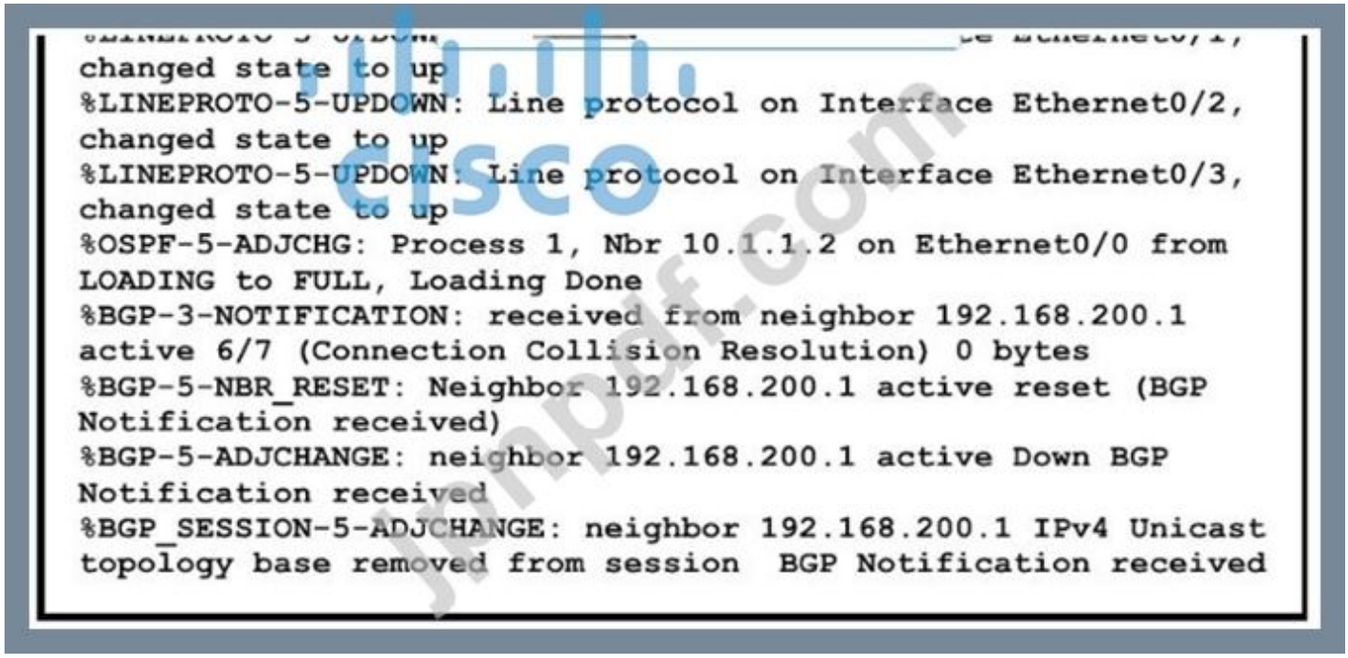
A. インターレース e0/0 に IPv6 アドレスを手動で割り当てる DHCP クライアントとして H1 を設定します。
B. 不正な DHCP サーバーからの IPv6 アドレスを回避するように、承認された DHCP サーバーを構成します。
C. リース期限が切れた後、R1 が IPv6 アドレスを削除したため、DHCP リース時間を延長します。
D. R1 の DHCP プールに 2001:DBB:BAD:C0DE::/64 プレフィックスを使用します。
Answer: D (メーッセージを残す**)**

最新問題**: 23**
左側の ICMPv6 近隣探索メッセージを右側の正しいパケット タイプにドラッグ アンド ドロップします。

Answer:



最新問題**: 24**
展示を参照してください。



展示を参照してください。エンジニアは、ルーターのログ メッセージにイベントがいつ発生したかに関する情報が含まれていないことに気付きました。ログ機能を詳細なレベルで改善するためにサービス タイム スタンプを有効にする場合、エンジニアはどのアクションを実行する必要がありますか?

A. msec オプションを構成します

B. タイムゾーン オプションを構成します

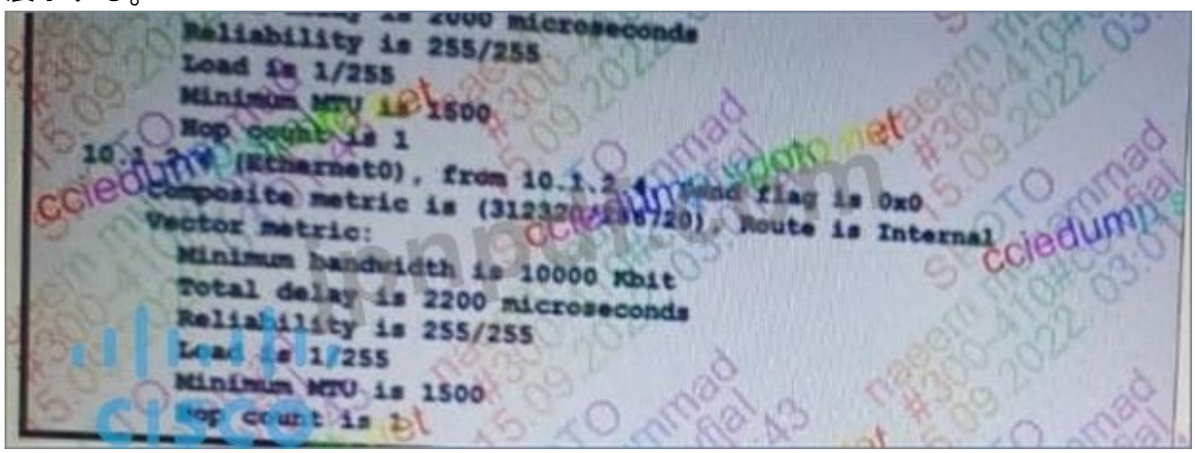
C. デバッグ稼働時間オプションを構成します

D. tog uptime オプションを構成します

Answer: D (メーッセージを残す**)**

最新問題**: 25**

展示する。



ネットワークは EIGR 等コスト バランシング用に設定されていますが、サーバ宛てのトラフィックはロード バランシングされていません。....問題は解決しましたか？

A. R4 E0/1 で 2200

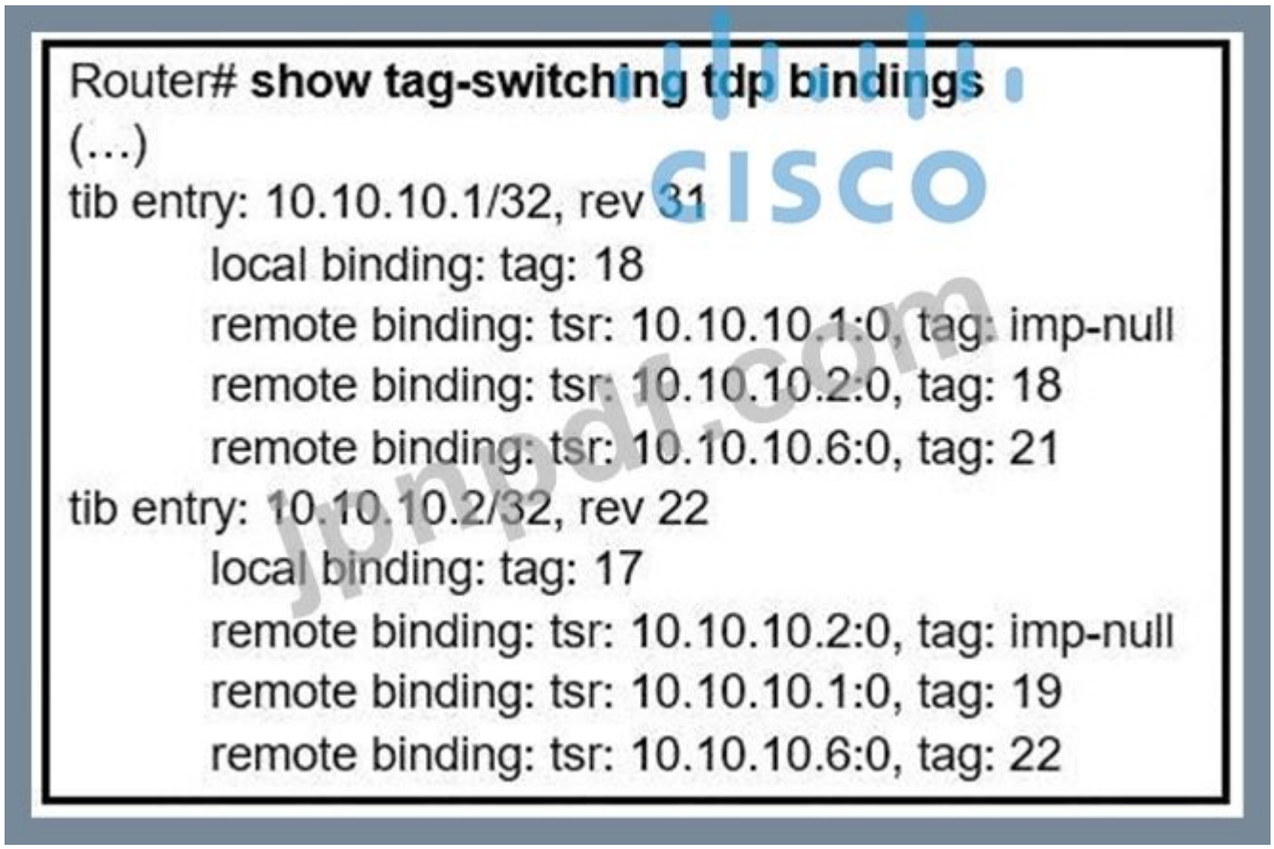
B. 120/on R3 E0/1

C. R4 E0/1 で 120

D. 208 oon R3 E0/0

Answer: B (メーッセージを残す)

最新問題: **26**
展示を参照してください。



MPLS VPN クラウドでは imp-null タグは何を表しますか?
A. ラベルをポップします
B. ラベルを面付けします
C. EXP ビットを含めます
D. EXP ビットを除外します
Answer: (解答を表示する)
説明
imp-null (暗黙的ヌル) タグは、パケットを転送する前にタグ スタックからタグ エントリをポップするように上流ルータに指示します。
注: Pop は、最上位の MPLS ラベルを削除することを意味します

最新問題: **27**
展示を参照してください。

エンジニアは、サマリー ルートを使用せずに R1 と R2 の間に EIGRP を設定する必要があります。どの構成で問題が解決しますか?

A)

```
R1(config)#router eigrp 1
R1(config-router)#no auto-summary
```

B)

```
R2 (config)#router eigrp 1
R2 (config-router)#no auto-summary
```

C)

```
R2 (config)#router eigrp 1
R2 (config-router)#auto-summary
```

D)

```
R1(config)#router eigrp 1
R1(config-router)#auto-summary
```

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: A (メーッセージを残す**)**

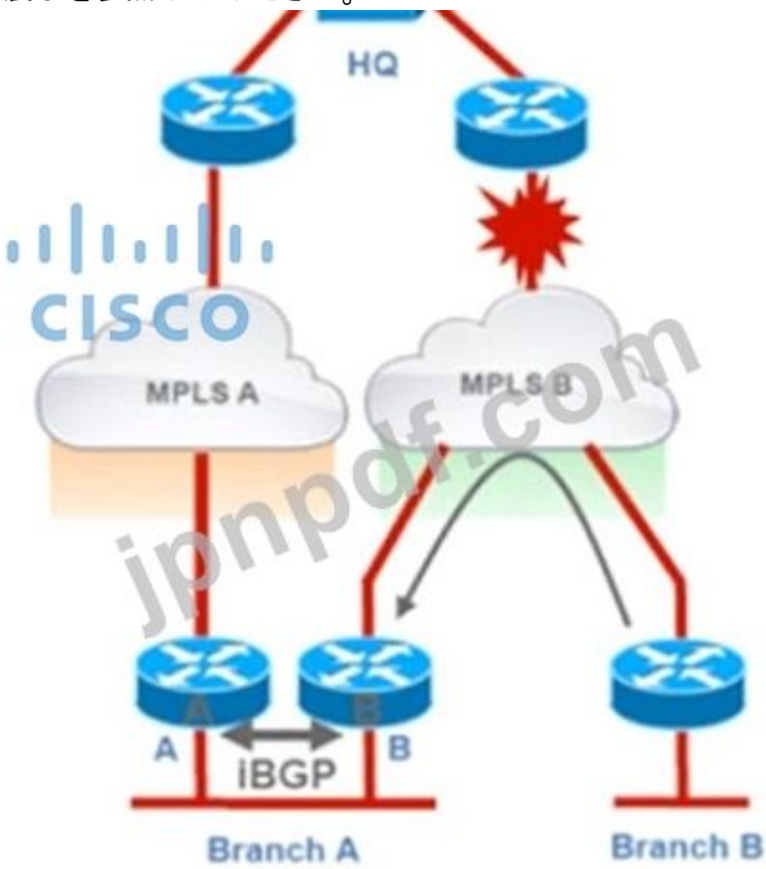
最新問題**: 28**
エンジニアがどの VPN に属しているかを識別できるように、IP アドレスを拡張するために MPLS VPN のどのコンポーネントが使用されますか?
A. VPNv4 アドレス ファミリ

B. RD
C. RT
D. 自民党
Answer: B (メーッセージを残す**)**
説明

- Specify the correct route distinguisher used for that VPN. This is used to extend the IP address so that you can identify which VPN it belongs to.

```
rd <VPN route distinguisher>
```

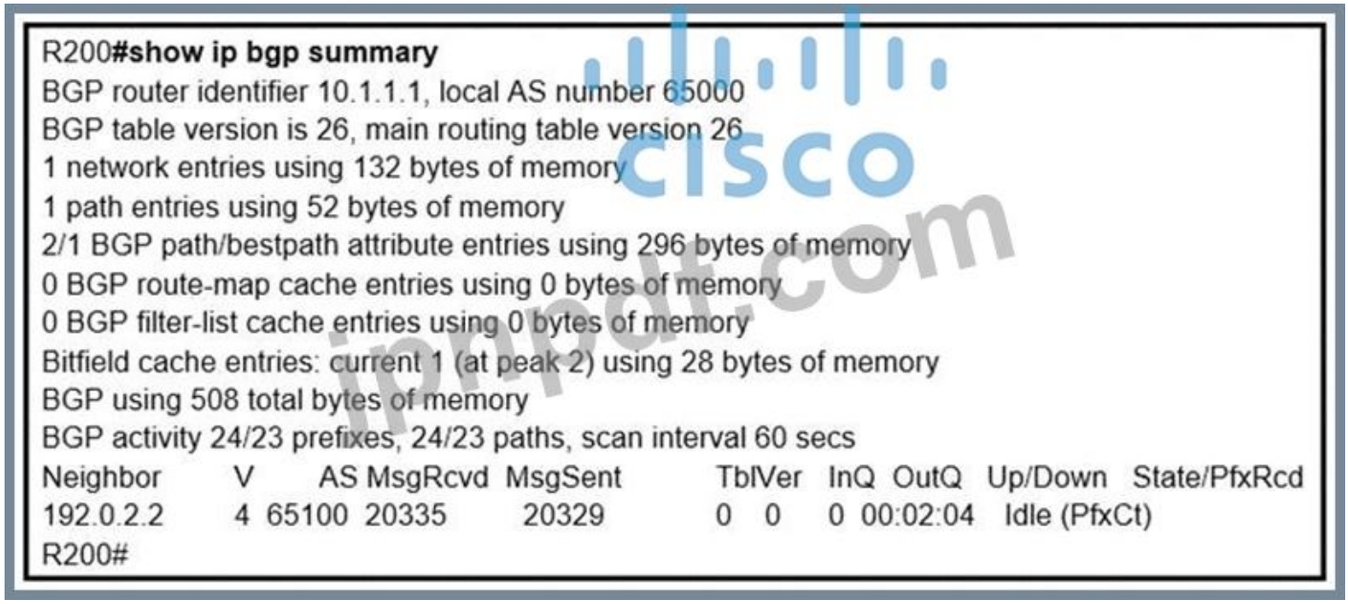
最新問題**: 29**
展示を参照してください。



トラブルシューティングを行い、ブランチ B が本社に到達するために MPLS B ネットワークのみを使用するようにします。この要件を達成するアクションはどれですか?
A. ブランチ A ルーターに AS パス フィルターを導入して、ローカル プレフィックスのみが BGP にアドバタイズされるようにします。
B. ブランチ B で MPLS B ネットワークから受信したすべての HQ プレフィックスのローカル プリファレンスを、MPLS A ネットワークで使用されるローカル プリファレンスよりも高くします。
C. ブランチ A の MPLS B ネットワーク接続の先頭に AS パスを追加し、ブランチ A から MPLS B ネットワークに向かう HQ アドバタイズメントが 3 回先頭に追加されるようにします。
D. ブランチ B で MPLS B ネットワークから受信したすべての HQ プレフィックスの重みを、MPLS A ネットワークで使用される重みよりも高く変更します。

Answer: A (メーッセージを残す**)**
重みを変更するか、ローカル優先度を増やすか、または AS パスの先頭に追加する場合は、MPLS B を MPLS A よりも優先させることしかできません。
ただし、MPLS B がダウンしている場合は、この質問の要件を満たさない MPLS A が使用されます。
AS パス フィルタリングを使用する場合のみ、特定の AS からのプレフィックスを拒否し、ブランチ B が MPLS A を使用して HQ に到達しないようにできます。

最新問題**: 30**
展示を参照してください。



BGP ネイバーがアイドル状態のままになるのはどのような状況ですか?
A. BGP ピアからプレフィックスを受信しない場合
B. プレフィックスが最大制限に達した場合
C. プレフィックス リストが受信方向に適用される場合
D. プレフィックスが最大制限を超えている場合
Answer: (解答を表示する**)**
説明
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/25160-bgp-maximum-prefix.html#

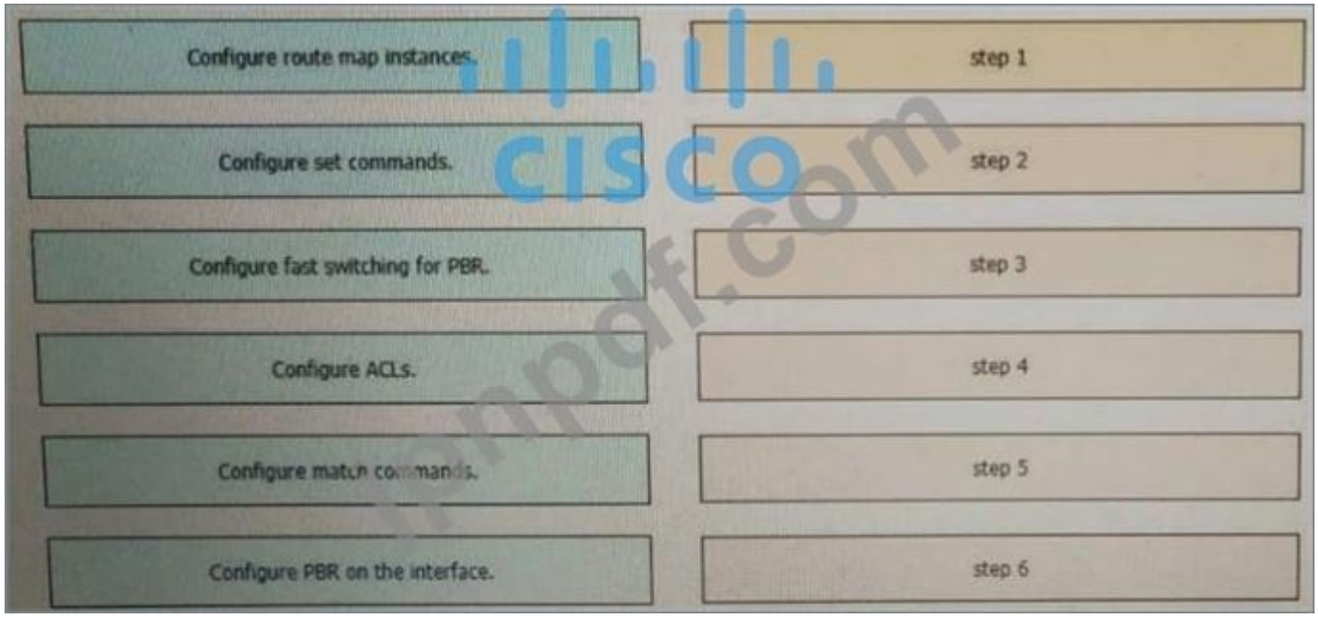
最新問題**: 31**

```
R1(config) # do show running-config | section line|username
username cisco secret 5 $1$yb/o$L3G5cXODxpYMSJ70PzEyo0
line con 0
 logging synchronous
line vty 0 4
 login local
 transport input telnet
R1(config) # logging console 7
R1(config) # do debug aaa authentication
R1(config) #
```

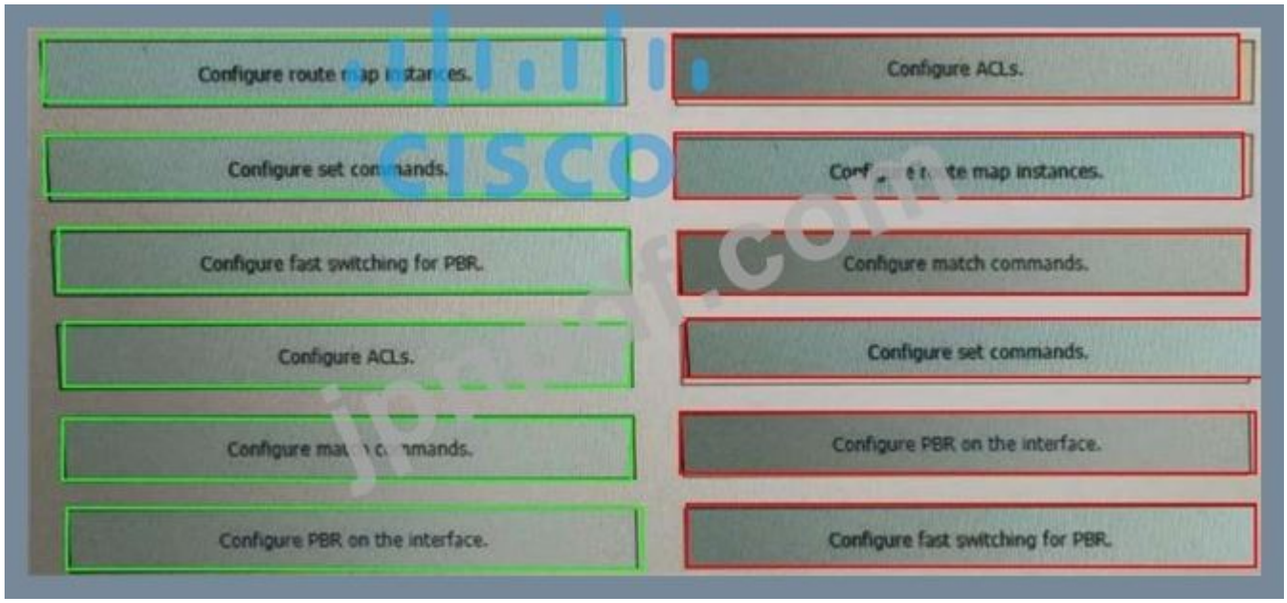
展示を参照してください。コンソールに接続している管理者には、リモート ユーザーがログインするときにデバッグ メッセージが表示されません。
リモート ログインに対してデバッグ メッセージが確実に表示されるようにするアクションはどれですか?

A. Transport input ssh 設定コマンドを入力します。
B. 端末監視実行コマンドを入力します。
C. ロギング コンソール デバッグ コンフィギュレーション コマンドを入力します。
D. aaa new-model コンフィギュレーション コマンドを入力します。
Answer: C (メーッセージを残す**)**
セクション: インフラストラクチャ サービス

最新問題: **32**
左側のアクションを右側の正しい順序にドラッグ アンド ドロップして、通常のルーティング パスに基づいたパケット転送を回避するポリシーを構成します。

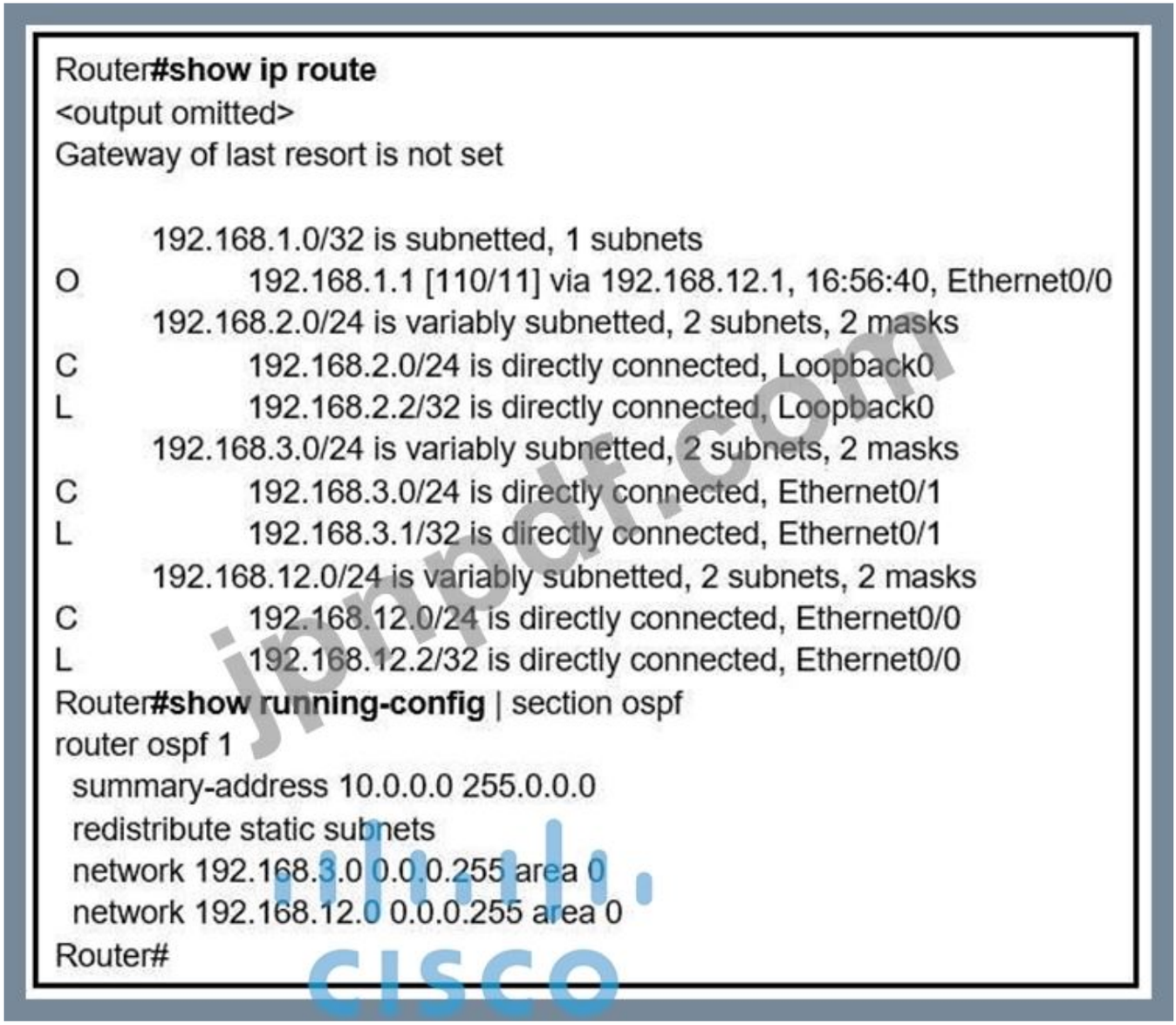


Answer:



最新問題: **33**

展示を参照してください。エンジニアは OSPF でネットワーク 10.0.0.0/8 のサマリー ルートを生成しようとしていますが、サマリー ルートがルーティング テーブルに表示されません。概要ルートが欠落しているのはなぜですか?

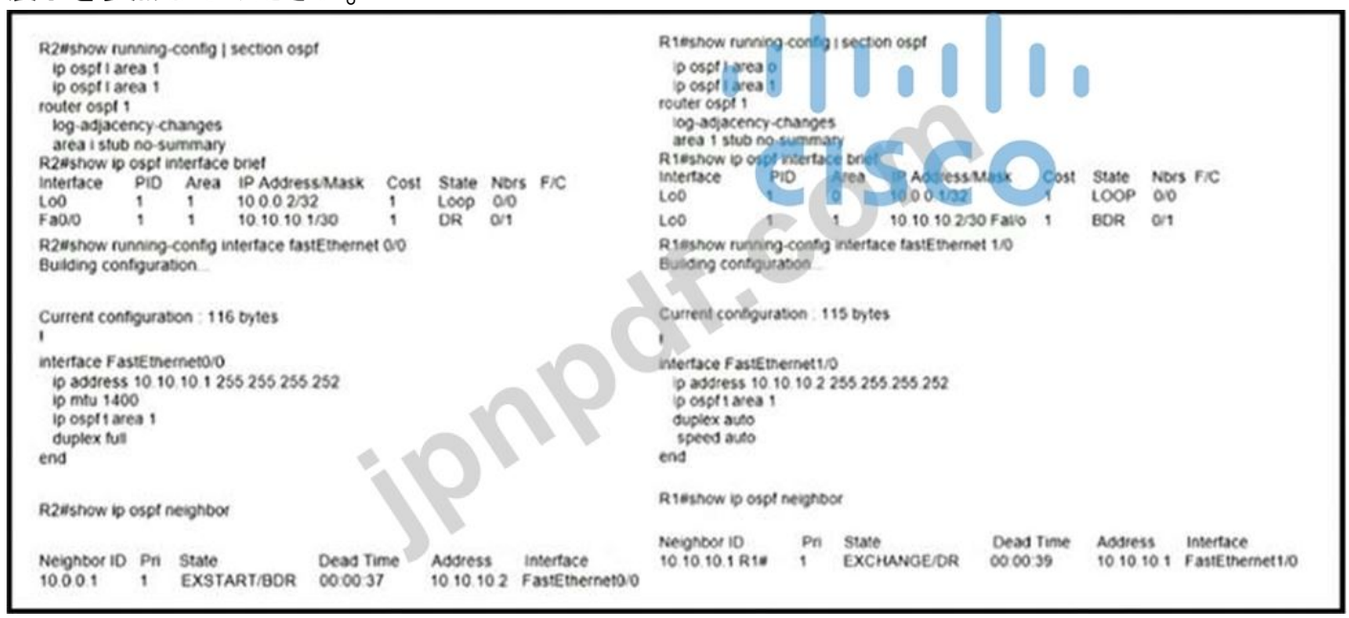


A. summary-address コマンドは、エリア間のプレフィックスを要約するためにのみ使用されます。
B. サマリー ルートは OSPF データベースでのみ表示され、ルーティング テーブルでは表示されません。
C. 10.0.0.0/8 内のサブネットのルートがないため、要約ルートは生成されません。
D. サマリー ルートはこのルーターでは表示されませんが、同じエリア内の他の OSPF ルーターでは表示されます。
Answer: C (メーッセージを残す**)**
セクション: レイヤ 3 テクノロジー

最新問題**: 34**
展示を参照してください。
セキュリティ監査の後、管理者はルート リフレクタに ACL を実装しました。ネットワーク内のどのルーターからも RR に到達できなくなりました。問題を解決する 2 つのアクションはどれですか? (2つお選びください。)
A. ACL で ICMPv6 近隣探索トラフィックを許可します。
B. Ethernet0/1 インターフェイス上でリンクローカル アドレスを設定します。

C. デフォルト ルートのネクスト ホップをデフォルト ゲートウェイのリンクローカル アドレスに変更します。
D. ACL エントリ 80 を削除します。
E. デフォルト ゲートウェイで ND プロキシ機能を有効にします。
Answer: A,D (メーッセージを残す**)**

最新問題**: 35**
展示を参照してください。



R1 と R2 の間の OSPF 隣接関係を復元するアクションはどれですか?
A. R1 Fa1/0 の IP MTU を 1500 に変更します
B. R1 Fa1/0 の IP MTU を 1300 に変更します
C. R2 Fa0/0 の IP MTU を 1300 に変更します
D. R2 Fa0/0 の IP MTU を 1500 に変更します
Answer: D (メーッセージを残す**)**

最新問題**: 36**

展示を参照してください。ネットワーク エンジニアは、スイッチ S1 から Telnet を使用して R3 にリモート アクセスできません。どのアクションで問題が解決しますか?

A. R3 にトランスポート入力 Telnet コマンドを追加します。

B. スイッチ上で ssh -l admin 10.0.0.1 コマンドの使用を許可します。

C. R3 の exec コマンドを介した受信接続を許可します。

D. スイッチにログイン管理コマンドを追加します。

Answer: (解答を表示する**)**

最新問題**: 37**

MPLS レイヤ 3 VPN の 2 つの機能は何ですか? (2つお選びください。)

A. イーサネット リンク/サイト間の透過的なポイントツーマルチポイント接続に使用されます。

B. ノード セグメント ID を持つパケットは、宛先までの最短パスとともに転送されます。

C. 顧客のトラフィックは、MPLS ネットワークで転送されるときに VPN ラベルにカプセル化されます。

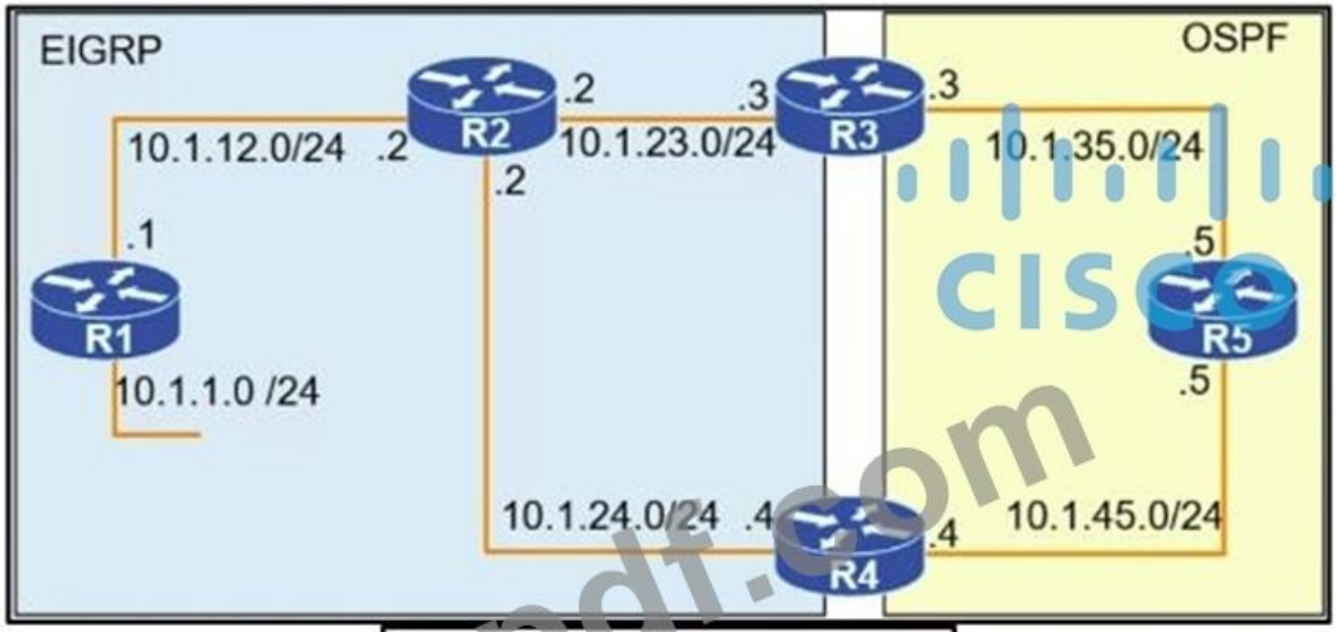
D. LDP および BGP は疑似回線シグナリングに使用できます。

E. BGP は、PE ノード間で顧客の VPNv4 ルートを通知するために使用されます。

Answer: C,E (メーッセージを残す**)**

最新問題**: 38**

展示を参照してください。




```
R1
router eigrp 1
 redistribute connected
 network 10.1.12.1 0.0.0.0
 default-metric 1000000 10 255 1 1500

R3
router eigrp 1
 network 10.1.23.3 0.0.0.0
!
router ospf 1
 redistribute eigrp 1 subnets
 network 10.1.35.3 0.0.0.0 area 0
```

R5 からネットワーク 10.1.1.0 /24 に到達できるようにするために、ネットワーク管理者は R3 上の OSPF に EIGRP を再配布しますが、R4 が 10.1.1.0/ に到達するために R5 を経由する ..... パスを使用していることに気付きます。24ネットワーク。R5 から 10.1.1.0/24 ネットワークへの到達可能性を維持しながら問題を解決するアクションはどれですか?

A. OSPF の R5 の R4 に向けた送信配布リストを適用します。

B. 外部 EIGRP のアドミニストレーティブ ディスタンスを 90 に変更します。

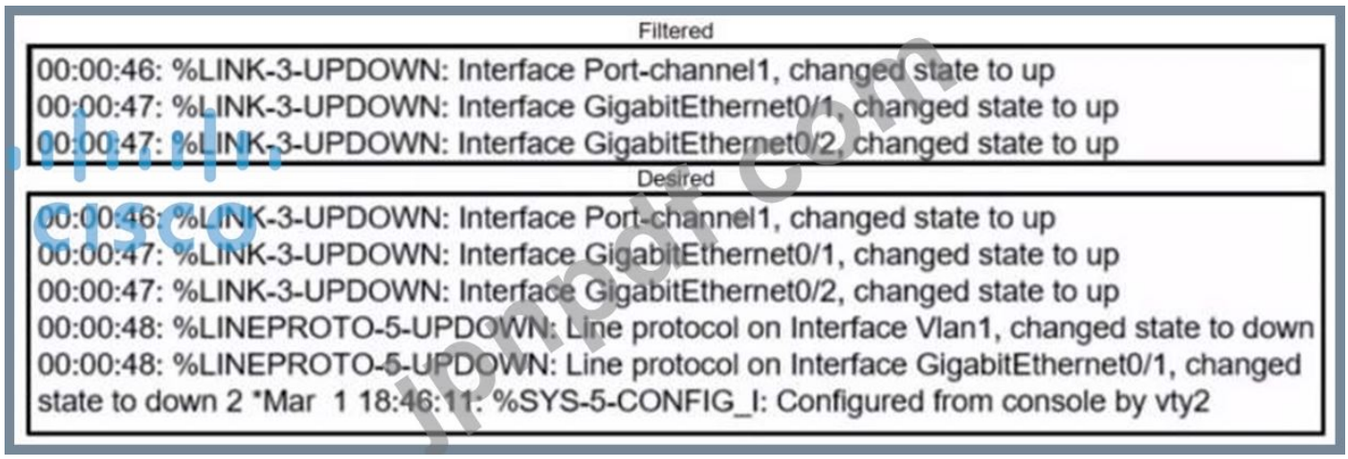
C. R5 で OSPF のアドミニストレーティブ ディスタンスを 200 に変更します。

D. OSPF を R4 の EIGRP に再配布します

Answer: B (メーッセージを残す**)**

最新問題**: 39**

展示を参照してください。



展示品をご参照ください。エンジニアは重大度に基づいてメッセージをフィルタリングし、ログ メッセージを最小限に抑えました。フィルタを適用した後、エンジニアは、必要なメッセージもフィルタリングされていることに気付きました。問題を解決するためにエンジニアはどのアクションを実行する必要がありますか?

A. syslog レベル 4 を構成します。

B. syslog レベル 5 を構成します。

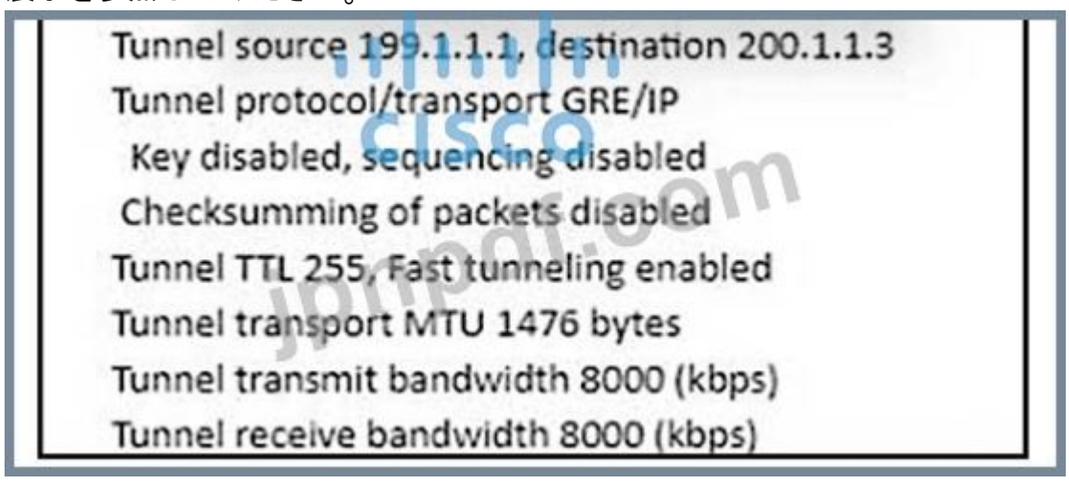
C. syslog レベル 2 を構成します。

D. syslog レベル 3 を構成します。

Answer: B (メーッセージを残す**)**

最新問題**: 40**

展示を参照してください。



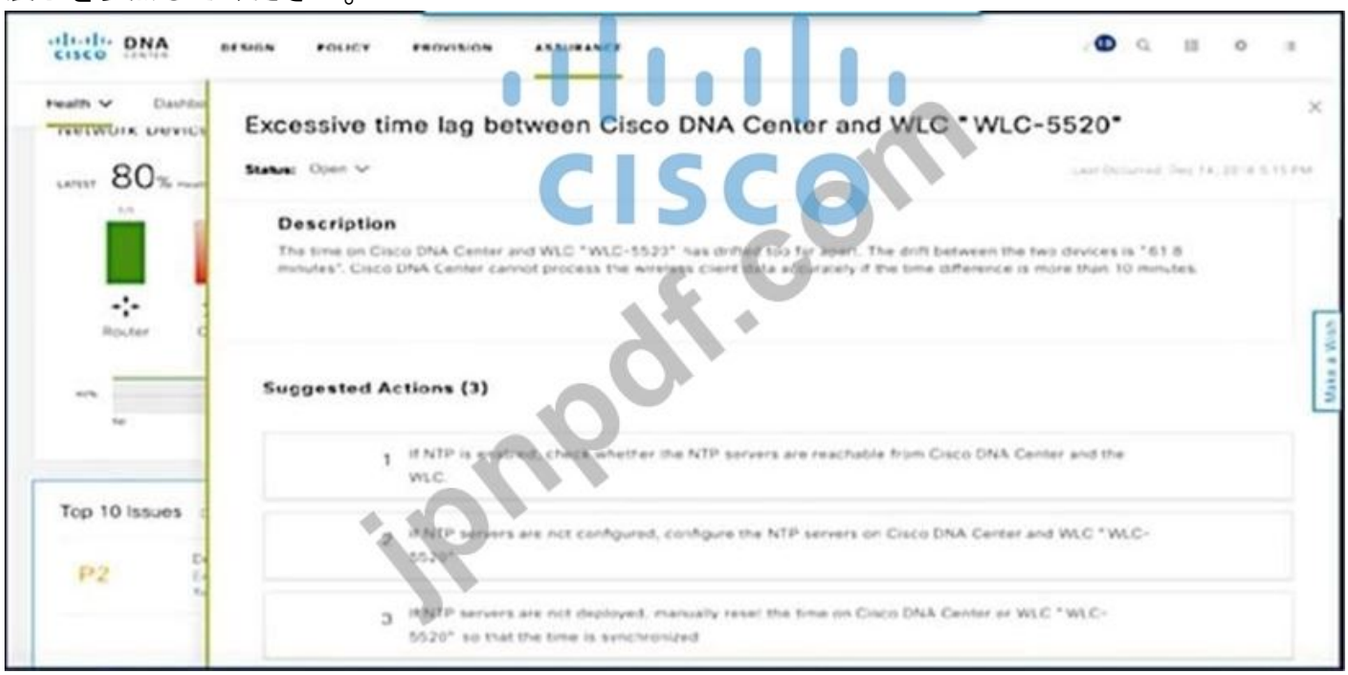
エンジニアは、R1 とリモート サイトの間にポイントツーポイント GRE VPN を確立する必要があります。どの構成がリモート サイトのタスクを達成しますか?

A. インターフェイス トンネル 1
トンネルソース 199.1.1.1
トンネル宛先 200.1.1.3
IPアドレス 192.168.1.3 255.255.255.0

B. インターフェイス トンネル 1
トンネルソース 200.1.1.3

トンネルの宛先 199.1.1.1
IPアドレス 192.168.1.1.255.255.255.0
C. インターフェイス トンネル 1
トンネルソース 200.1.1.3
トンネルの宛先 199.1.1.1
IPアドレス 192.168.1.3.255.255.255.0
D. インターフェイス トンネル
トンネルソース 199.1.1.1
トンネル宛先 200.1.1.3
IPアドレス 192.168.1.1.255.255.255.0
Answer: C (メーッセージを残す**)**

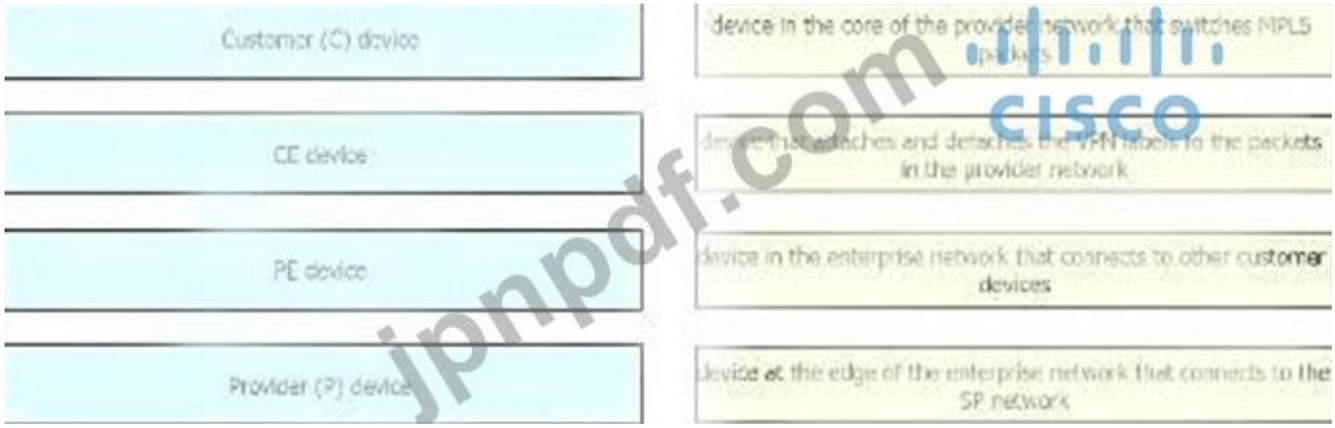
最新問題**: 41**
展示を参照してください。



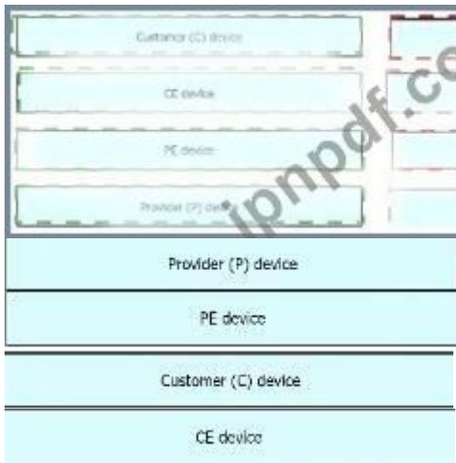
NTP は、ネットワーク インフラストラクチャと Cisco DNA Center 全体にわたって設定されます。NTP の問題は、17:15 に Cisco DNA Center で報告されました。どのアクションで問題が解決しますか?
A. WLC と NTP サーバ間の到達可能性を確認して解決します。
B. NTP サーバーをリセットして、すべてのデバイスの同期の問題を解決します。
C. Cisco DNA Center と NTP サーバ間の到達可能性を確認して解決します。
D. WLC で NTP を確認して設定し、Cisco DNA Center と同期します
Answer: D (メーッセージを残す**)**
Cisco DNA Center とデバイス間の過度のタイムラグ :Cisco DNA Center とデバイスの IP アドレス間の時間差が大きく離れています。時間差が 3 分を超える場合、CiscoDNA Center はデバイス データを正確に処理できません。

最新問題**: 42**

左側の MPLS VPN デバイス タイプを右側の定義にドラッグ アンド ドロップします。

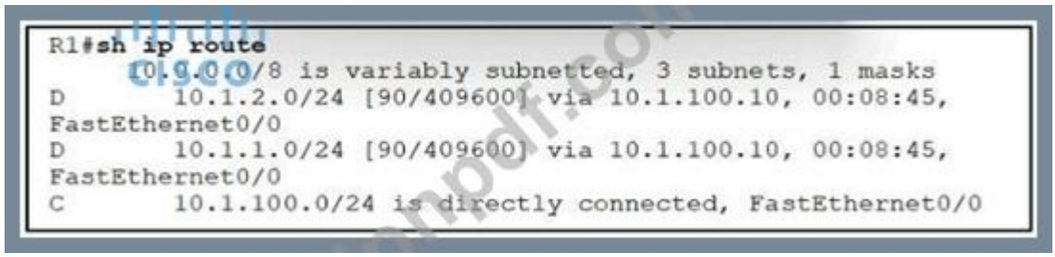


Answer:



最新問題**: 43**

展示を参照してください。



```
R1#sh ip route
     10.0.0.0/8 is variably subnetted, 3 subnets, 1 masks
D       10.1.2.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
D       10.1.1.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
```

R1 が 10.0.0.0/8 を受信するように要約が設定されていますが。より具体的なルートが R1 によって受信されます。

Fast Ethernet0/0 インターフェイス経由で R1 に接続されているネイバーから 10.0.0.0/8 サマリー ルートをどのように受信する必要がありますか?

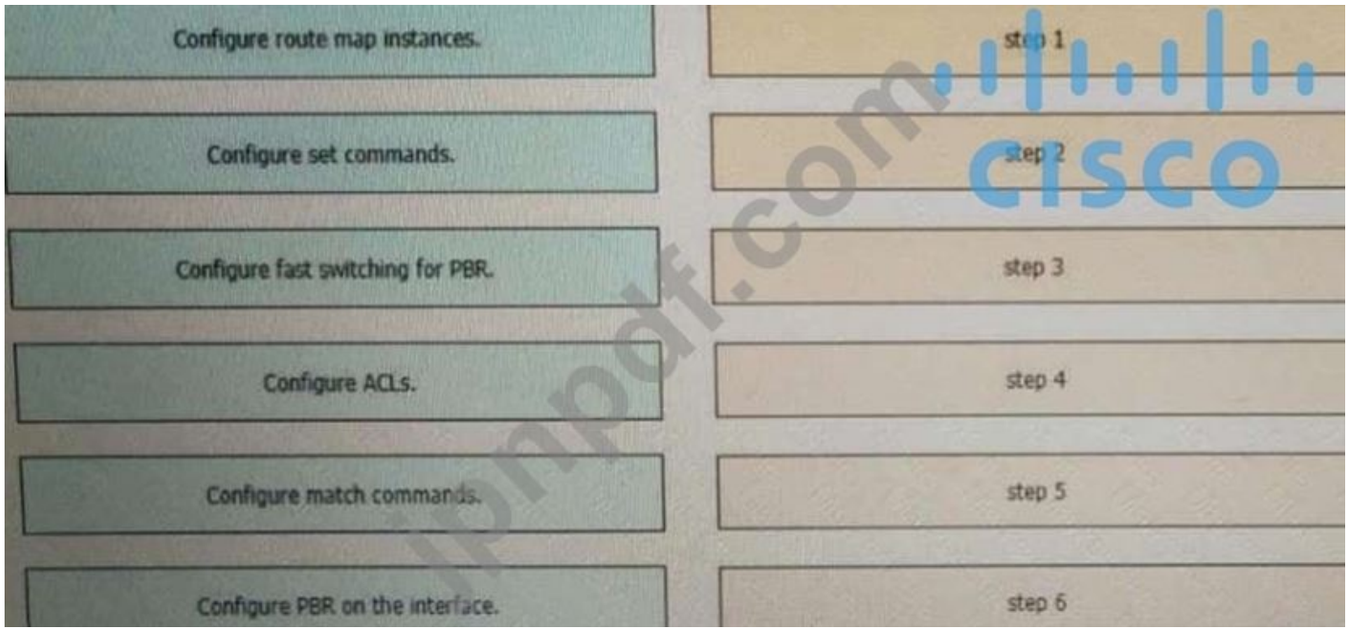
A. R1 は、ファスト イーサネット 0/0 インターフェイスで ip summary-address eigrp <AS 番号> 10.0.0.0.255.0.0.0 コマンドを設定する必要があります。

B. 要約条件が満たされていません。Router 10 1 100.10 には、null 0 を指す 10 0.0.0/8 のルートが必要です。

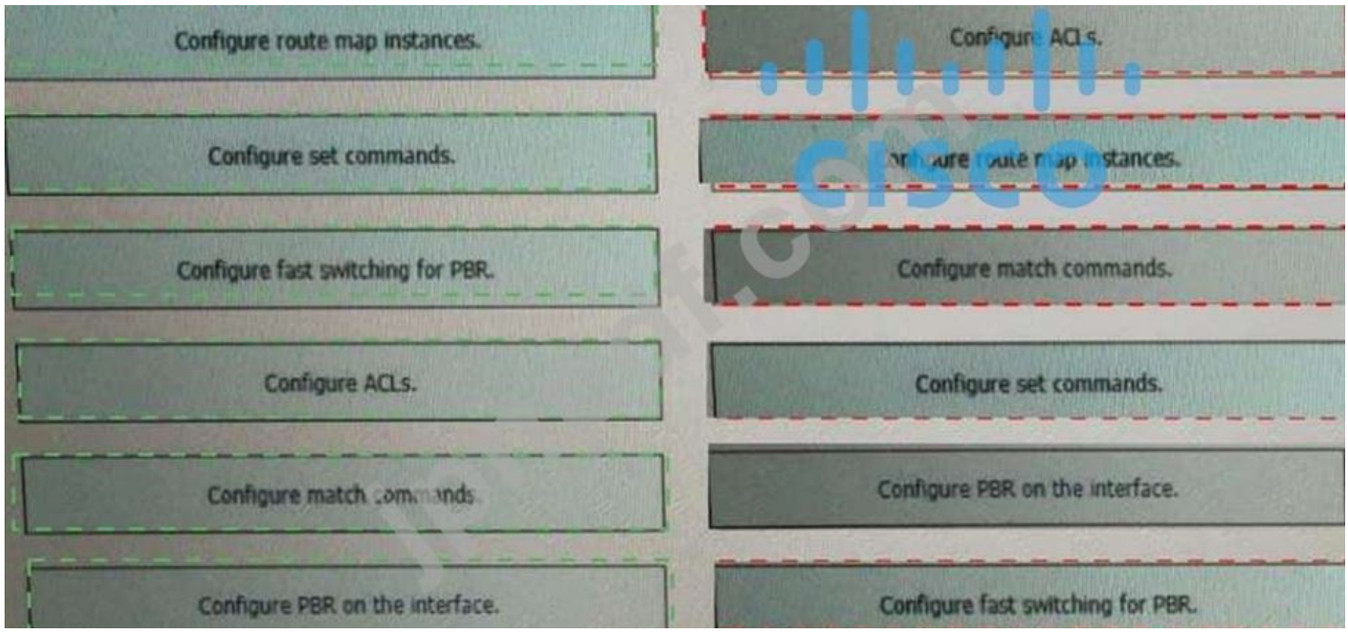
C. 集約条件を満たしていません。ネットワーク 10.1.100.0/24 を次のように変更する必要があります。172.16.0.0/24。

D. R1 は、ファスト イーサネット 0/0 インターフェイスで ip summary-address eigrp <AS 番号> 10.0.0.0 0.0.0.255 コマンドを設定する必要があります。
Answer: D (メーッセージを残す**)**

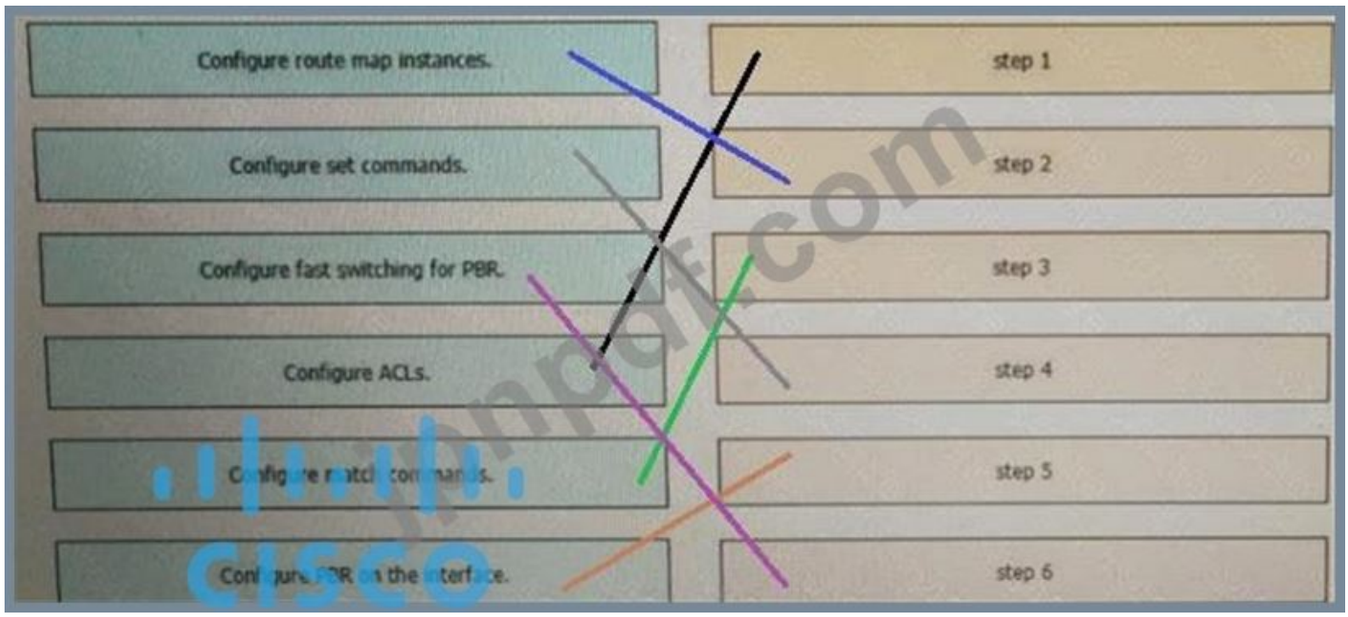
最新問題**: 44**
左側のアクションを右側の正しい順序にドラッグ アンド ドロップして、通常のルーティング パスに基づいたパケット転送を回避するポリシーを構成します。



Answer:



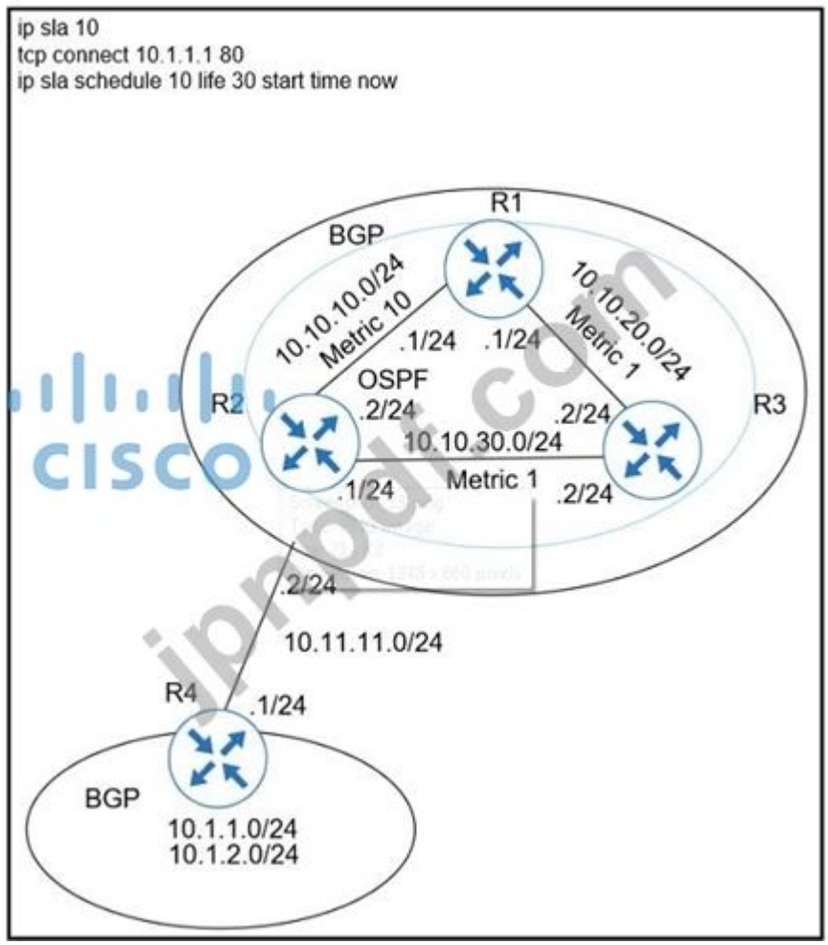
説明



https://community.cisco.com/t5/networking-documents/how-to-configure-pbr/ta-p/3122774

最新問題**: 45**

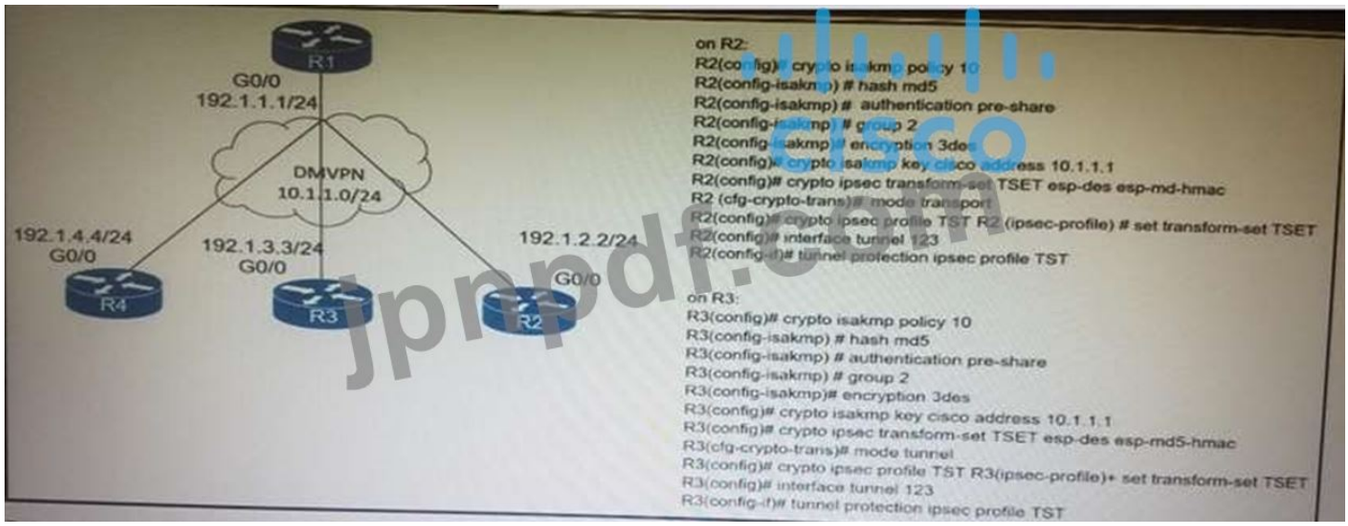
展示を参照してください。



ユーザは、導入前に IP アドレス 10.1.1.1 上の非 SLA ホスト Web サーバが HTTP セッションを受け入れるかどうかをテストするために IP SLA プローブを設定しました。プローブが失敗しています。プローブを成功させるために、ネットワーク管理者はどのアクションを推奨する必要がありますか?

A. IP sla スケジュール頻度を永久に変更します。
B. tcp 接続に制御無効化オプションを追加します。
C. ip slaSchedule コマンドを再発行します。
D. ホストの icmp-echo コマンドを追加します。
Answer: C (メーッセージを残す**)**

最新問題**: 46**
展示を参照してください。



IPsec を適用した後、エンジニアは DMVPN トンネルがダウンし、スポークツースポークとハブの両方が確立されていないことを観察しました。問題を解決した 2 つのアクションはどれですか? (2つお選びください。)
A. R2 および R3 に暗号 isakmp キーのシスコ アドレス 0.0.0.0 を設定します。
B. R3 でモード トンネルからモード トランスポートへのモードを設定します。
C. R2 でモードをトランスポート モードからトンネル モードに変更します。
D. crypto isakmp キー Cisco アドレス 10.1.1.1 を削除します。R2とR3で。
Answer: D (メーッセージを残す**)**

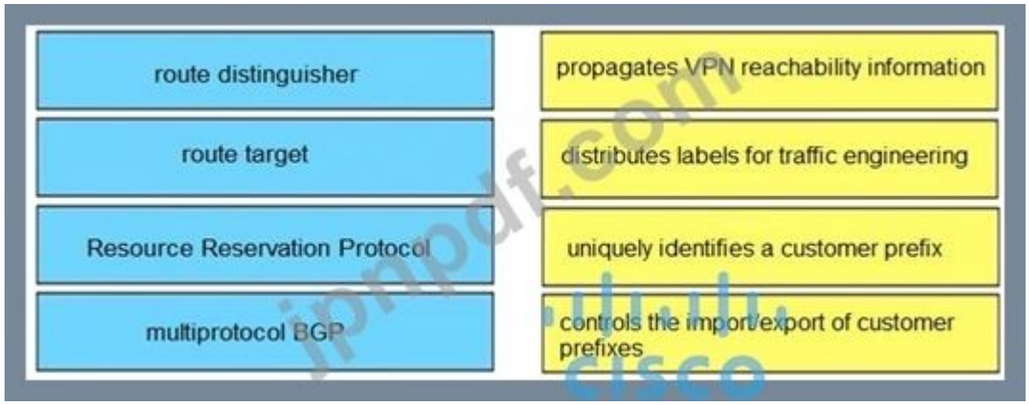
最新問題**: 47**
展示を参照してください。

```
R1#show ip ssh
SSH Disabled – version 1.99
%Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size: 1024 bits
IOS Keys in SECSH format (ssh-rsa, base64 encoded) : NONE
R1#
```

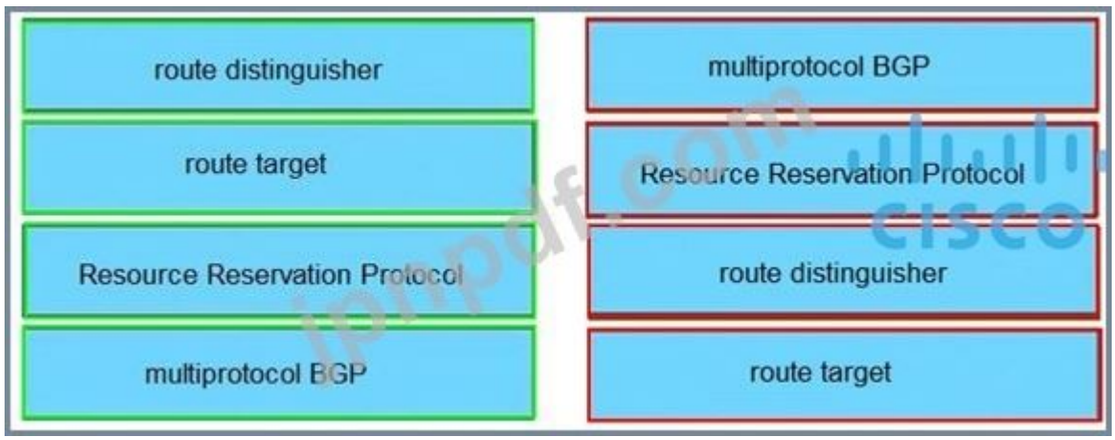
エンジニアは SSH を使用してデバイスに接続しようとしていますが、接続できません。エンジニアは、トラブルシューティング時にコンソールを使用して接続し、表示された出力を確認します。デバイス上で SSH を有効にするには、設定モードでどのコマンドを使用する必要がありますか?

A. ip ssh 無効なし
B. 暗号鍵生成 rsa
C. ip ssh バージョン 2
D. ip ssh 有効化
Answer: (解答を表示する**)**

最新問題: **48**
左側の MPLS VPN の概念を右側の適切な説明にドラッグ アンド ドロップします。

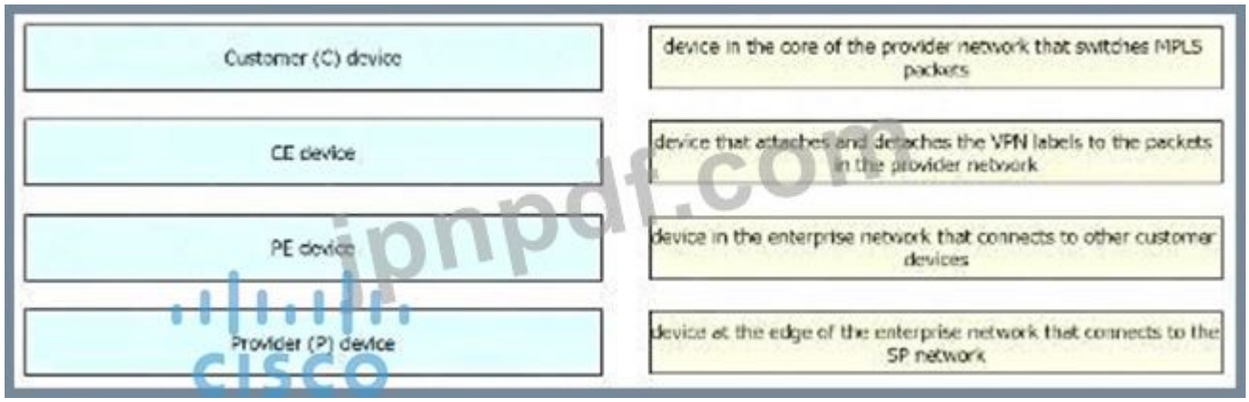


Answer:



最新問題: **49**

左側の MPLS VPN デバイス タイプを右側の定義にドラッグ アンド ドロップします。



Answer:

最新問題**: 50**

R2 にはローカルに発信されたプレフィックス 192.168.130.0/24 があり、次の構成があります。

```
ip prefix-list test seq 5 permit 192.168.130.0/24
!
route-map OUT permit 10
match ip address prefix-list test
set as-path prepend 65000
```

ルート マップ OUT コマンドが、neighbor 1.1.1.1 ルート マップ OUT out コマンドを使用して eBGP ネイバー R1 (1.1.1.1) に適用されると、結果はどうなりますか?

A. R1 は 192.168.130.0/24 を 1 AS ホップではなく 2 AS ホップと認識します。

B. R1 は 192.168.130.0/24 以外のルートを受け入れません

C. R1 は 192.168.30.0/24 宛てのトラフィックを転送しません。

D. ネットワーク 192.168.130.0/24 は R1 テーブルでは許可されていません

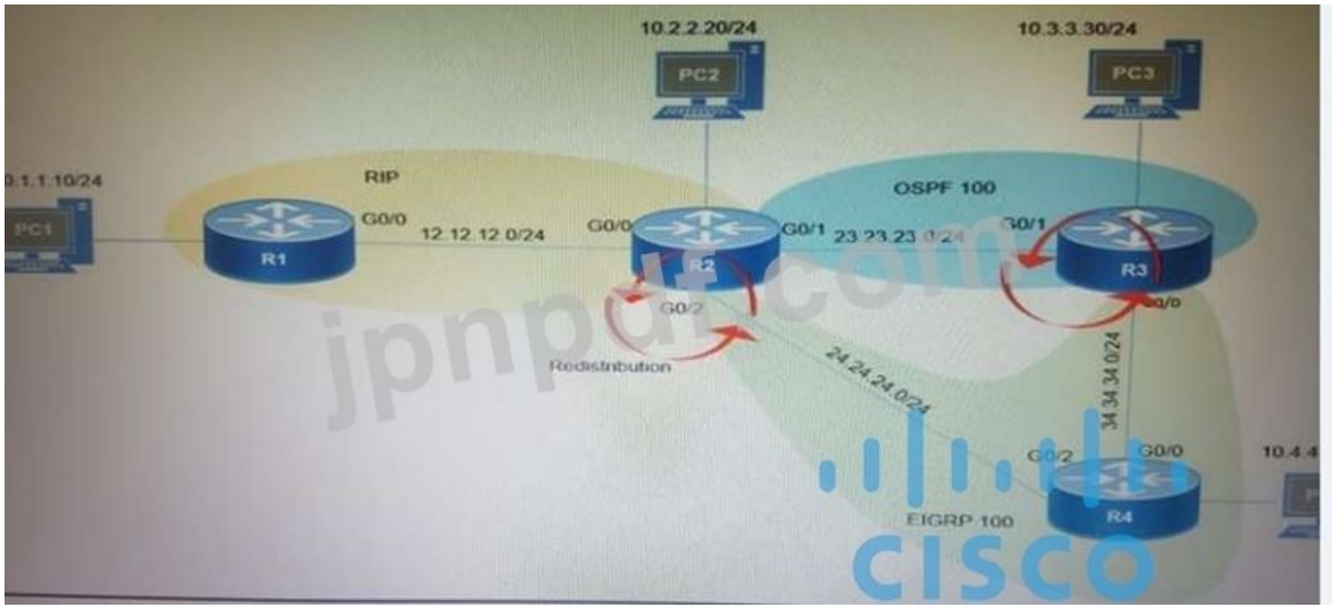
Answer: A (メーッセージを残す**)**

セクション: レイヤ 3 テクノロジー

説明/参照:

最新問題**: 51**

展示を参照してください。



ルーティング プロトコル間で再配布が有効になると、PC2、PC3、および PC4 は PC1 に到達できなくなります。すべての PC にアクセスできるように問題を解決するために、エンジニアはどのようなアクションを実行できますか?

A. R2 のプロセスでアドミニストレーティブ ディスタンス 100 を設定します。

B. OSPF から EIGRP に再配布されるときにプレフィックス 10.1.1.0/24 をフィルタリングします。

C. R2 上で直接接続されたインターフェイスを再配布します。

D. RIP から EIGRP に再配布されるときに、プレフィックス 10.1.1.0/24 をフィルタリングします。

Answer: C (メーッセージを残す**)**

最新問題**: 52**

展示を参照してください。

```
L     172.1.12.3/32 is directly connected, Ethernet0/0
C     172.1.13.0/24 is directly connected, Ethernet0/1
L     172.1.13.3/32 is directly connected, Ethernet0/1
O     192.168.1.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O     192.168.2.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O     192.168.3.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
O     192.168.4.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
      192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.5.0/24 is directly connected, Loopback0
L       192.168.5.1/32 is directly connected, Loopback0
      192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.6.0/24 is directly connected, Loopback1
L       192.168.6.1/32 is directly connected, Loopback1
```

サンフランシスコとボストンのルーターは、直接リンクが稼働しているにもかかわらず、相互に接続するために低速リンクを選択しています どの構成が問題を解決しますか?

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: (解答を表示する**)**

最新問題**: 53**
展示を参照してください。

エンジニアは、サマリー ルートを使用せずに R1 と R2 の間に EIGRP を設定する必要があります。どの構成で問題が解決しますか?

A.
```
R1(config)#router eigrp 1
R1(config-router)#no auto-summary
```

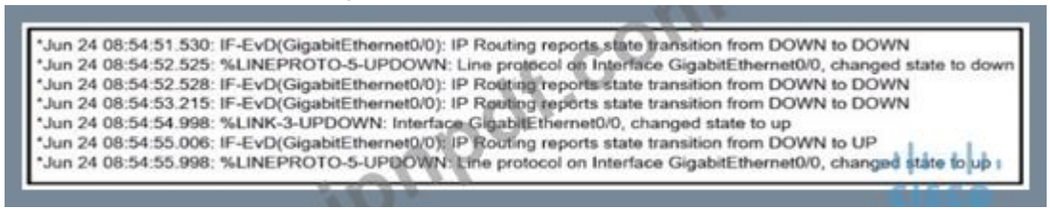
B.
```
R1(config)#router eigrp 1
R1(config-router)#auto-summary
```

C.
```
R2 (config)#router eigrp 1
R2 (config-router)#auto-summary
```

D.
```
R2 (config)#router eigrp 1
R2 (config-router)#no auto-summary
```

Answer: D (メーッセージを残す)

最新問題: **54**
展示を参照してください。



R1 は GigabitEthernet0/0 経由で R2 に接続されていますが、R2 は R1 に ping できません。どのようなアクションをとれば問題が解決しますか?

A. ルーターに設定されているルート ダンプニングを修正します。
B. SFP モジュールはサポートされていないため、交換します。
C. インターフェイスで構成された IP イベント ダンプニングを修正します。
D. 失敗した IP SLA プローブを修正します。

Answer: C (メーッセージを残す)

The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping.

最新問題: **55**
展示を参照してください。

EIGRP ネイバー隣接関係の問題のトラブルシューティング中に、ネットワーク エンジニアは、隣接ルータに接続されているインターフェイスが EIGRP プロセスに参加していないことに気づきました。どのアクションで問題が解決しますか?

A. network コマンドをネットワーク 172.16.0.1 0.0.0.0 に設定します。

B. EIGRP アドレス ファミリ vrf CLIENT1 でネットワーク コマンドを設定します。

C. インターフェイス FastEthernet0/3 で EIGRP メトリックを設定します

D. EIGRP アドレス ファミリ ipv4 でネットワーク コマンドを設定します。

Answer: B (メーッセージを残す)

説明

ルーター eigrp 1

！

アドレスファミリー ipv4 vrf CLIENT1

ネットワーク 172.16.0.0 0.0.0.255

自動要約なし

自律システム 1

出口アドレスファミリー

最新問題**: 56**

R1 と R2 は eBGP ネイバーとして設定されており、R1 は AS100 にあり、R2 は AS200 にあります。R2 は、次のネットワークを R1 にアドバタイズしています。

R1 のネットワーク管理者は、マスクが 23 より低い 172-16.0.0/16 メジャー ネットワークのすべてのサブネットが入ってくるのをブロックして、コンバージェンスを改善する必要があります。R1 でのタスクを達成できる設定セットはどれですか?

A. ip プレフィックス リスト PL-1 拒否 172.16.0.0/16 ファイル 23
ip プレフィックス リスト PL-1 許可 0.0.0.0/0 ファイル 32
！
ルーター bgp 100
ネイバー 192.168.100.2 リモート-as200
ネイバー 192.168.100.2 プレフィックスリスト PL-1

B. ip プレフィックス リスト PL-1 拒否 172.16.0.0/16 ge 23
ip プレフィックス リスト PL-1 許可 0.0.0.0/0 ファイル 32
！
ルーター bgp 100
ネイバー 192.168.100.2 リモート-as200
ネイバー 192.168.100.2 プレフィックスリスト PL-1

C. アクセスリスト 1 拒否 172.16.0.0 0.0.254.255
アクセスリスト 1 はすべてを許可します
！
ルーター bgp 100
ネイバー 192.168.100.2 リモート-as200
ネイバー 192.168.100.2 配布リスト 1 インチ

D. ip プレフィックス リスト PL-1 拒否 172.16.0.0/16
ip プレフィックス リスト PL-1 許可 0.0.0.0/0
！
ルーター bgp 100
ネイバー 192.168.100.2 リモート-as200
ネイバー 192.168.100.2 プレフィックスリスト PL-1

Answer: A (メーッセージを残す**)**

説明

23 未満のマスクを持つ 172.16.0.0/16 メジャー ネットワークのすべてのサブネットの受信をブロック」すると、172.16.16.0/20 がブロックされます。

最初のプレフィックス リスト ｢ip prefix-list PL-1deny 172.16.0.0/16 le 23｣は、｢72.16.0.0/16 の範囲内にあり、かつ /23 以下のサブネット マスクを持つすべてのネットワーク｣が拒否されることを意味します。。
2 番目のプレフィックス リスト ｢ip prefix-list PL-1mit 0.0.0.0/0 le 32｣は、他のすべてのプレフィックスを許可することを意味します。

最新問題: **57**
展示を参照してください。

左側の資格情報を右側のリモート ログイン情報にドラッグ アンド ドロップして、vtys へのログイン試行の失敗を解決します。頻度とスケジュールを定義することにより、すべての認証情報が SLA を満たすわけではありません

Answer:

Explanation:

vty 0:

+シスコ

+0csic

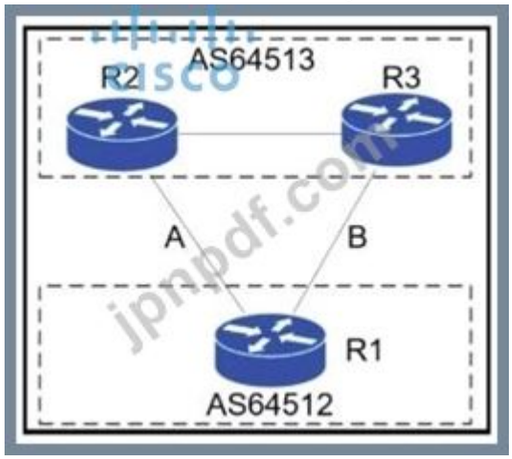
vty 1:

+ ユーザー名なし

+ パスワードなし

コマンド「aaaAuthenticationlogindefaultnone」は、コンソール/VTY/AUX 経由でデバイスにアクセスするときに認証が必要ないことを意味するため、あるインターフェイスで別のログイン認証方法が指定されていない場合（「loginauthentication...」コマンド経由）、ユーザー名やパスワードを必要とせずにアクセスできるようになります。この場合、VTY 1 は別の認証ログイン方法を指定していないため、デフォルトの方法 (この場合は「なし」) を使用します。

最新問題: **58**
展示を参照してください。



AS64512 のネットワーク エンジニアは、メンテナンス中に BGP セッションを閉じずにリンク A からインバウンド トラフィックとアウトバウンド トラフィックを削除し、リンク A 上に ASN へのバックアップ リンクが残るようにする必要があります。R1 上のどの BGP 構成がこの目標を達成しますか?

A)

```
route-map link-a-in permit 10
 set weight 200
route-map link-a-out permit 10
 set as-path prepend 64512
route-map link-b-in permit 10
 set weight 100
route-map link-b-out permit 10
```

B)

```
route-map link-a-in permit 10
 set weight 200
route-map link-a-out permit 10
route-map link-b-in permit 10
 set weight 100
route-map link-b-out permit 10
  set as-path prepend 64512
```

C)

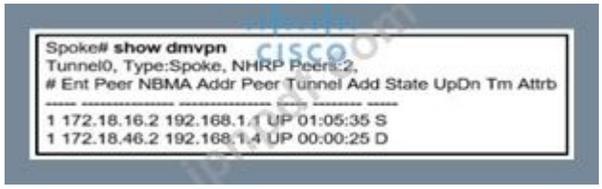
```
route-map link-a-in permit 10
 set local-preference 200
route-map link-a-out permit 10
route-map link-b-in permit 10
route-map link-b-out permit 10
 set as-path prepend 64512
```

D)

```
route-map link-a-in permit 10
route-map link-a-out permit 10
 set as-path prepend 64512
```

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: **59**
展示を参照してください。



エンジニアはスポーク ルータ上で DMVPN を設定しました。DMVPN ネットワーク内の別のスポーク ルータの WAN IP アドレスは何ですか?

A. 172.18.46.2

B. 192.168.1.4

C. 172.18.16.2

D. 192.168.1.1

Answer: (解答を表示する**)**

説明

出力から、2 つの NHRP ピアがあることがわかります。NBMA アドレスを持つ最初のもの 172.18.16.2 と Static (S) の 「属性」(Attrb) から、それがハブ デバイスであると推測できます。

したがって、2 番目のスポーク デバイスは、ダイナミック (D) 属性を持つ残りのスポーク デバイスである必要があります。

--> S - 静的、D - 動的、I - 不完全

N - NATed、L - ローカル、X - ソケットなし

Ent --> 同じ NBMA ピアを持つ NHRP エントリの数

NHS ステータス: E --> 応答待ち、R --> 応答中、W --> 待機中

アップダウン時間 --> トンネルのアップタイムまたはダウンタイム

インターフェイス: トンネル 1、IPv4 NHRP 詳細

タイプ:スポーク、NHRP ピア:2、

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb

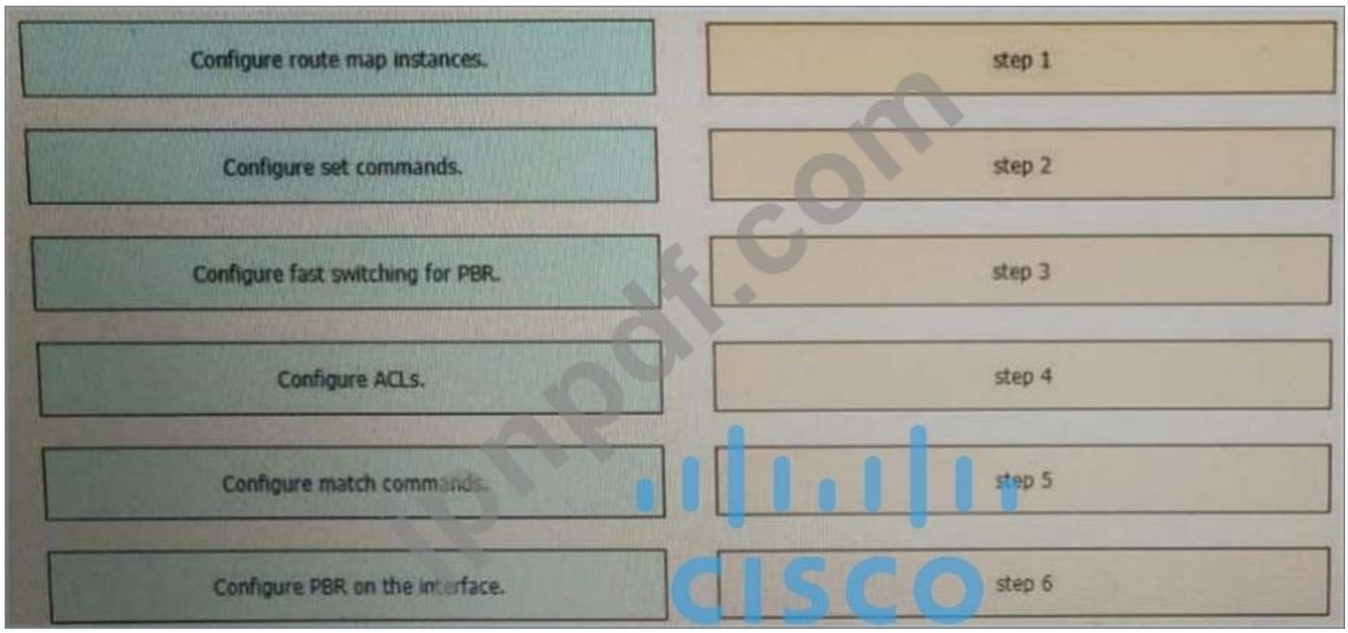
----- --------------- --------------- ----- -------- -- ---

1 44.44.44.4 192.168.100.254 上り 00:03:40 S

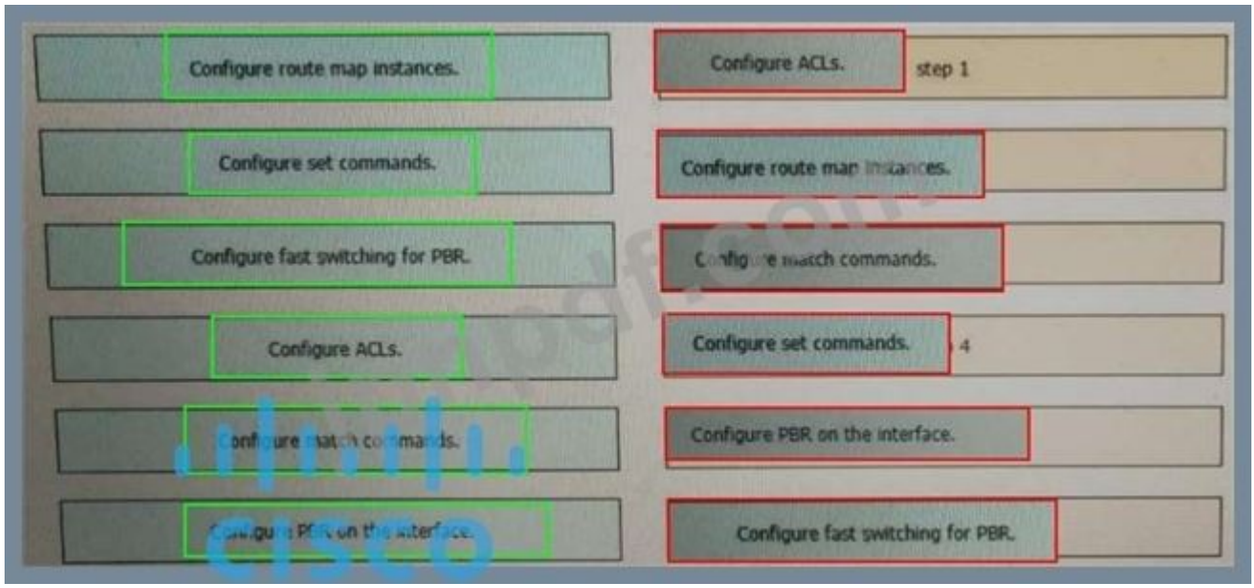
1 12.12.12.2 192.168.100.2 アップ 00:03:20 D

最新問題**: 60**

左側のアクションを右側の正しい順序にドラッグ アンド ドロップして、通常のルーティング パスに基づいたパケット転送を回避するポリシーを構成します。

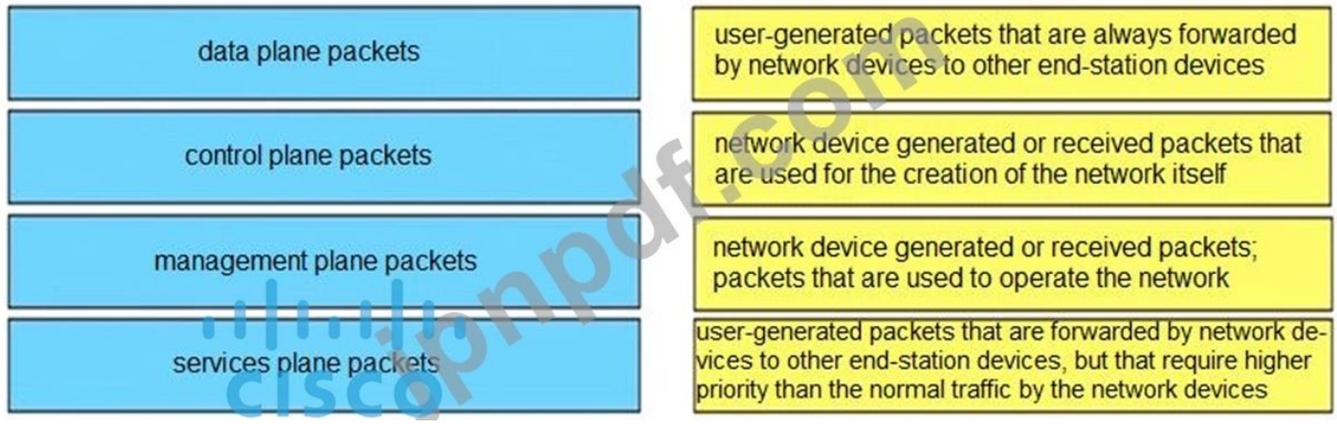


Answer:

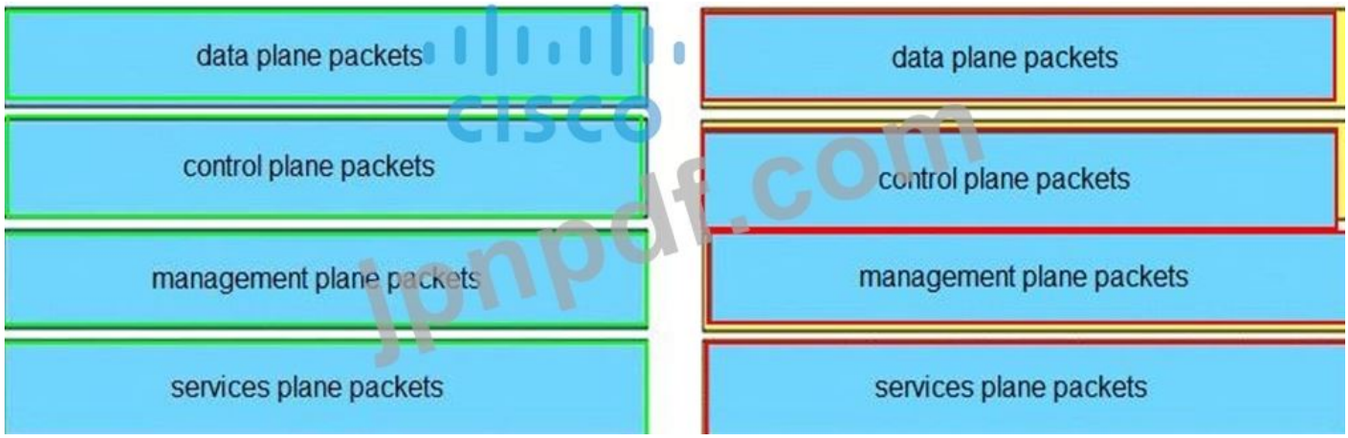


最新問題: **61**

左側のパケット タイプ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: **62**
展示を参照してください。

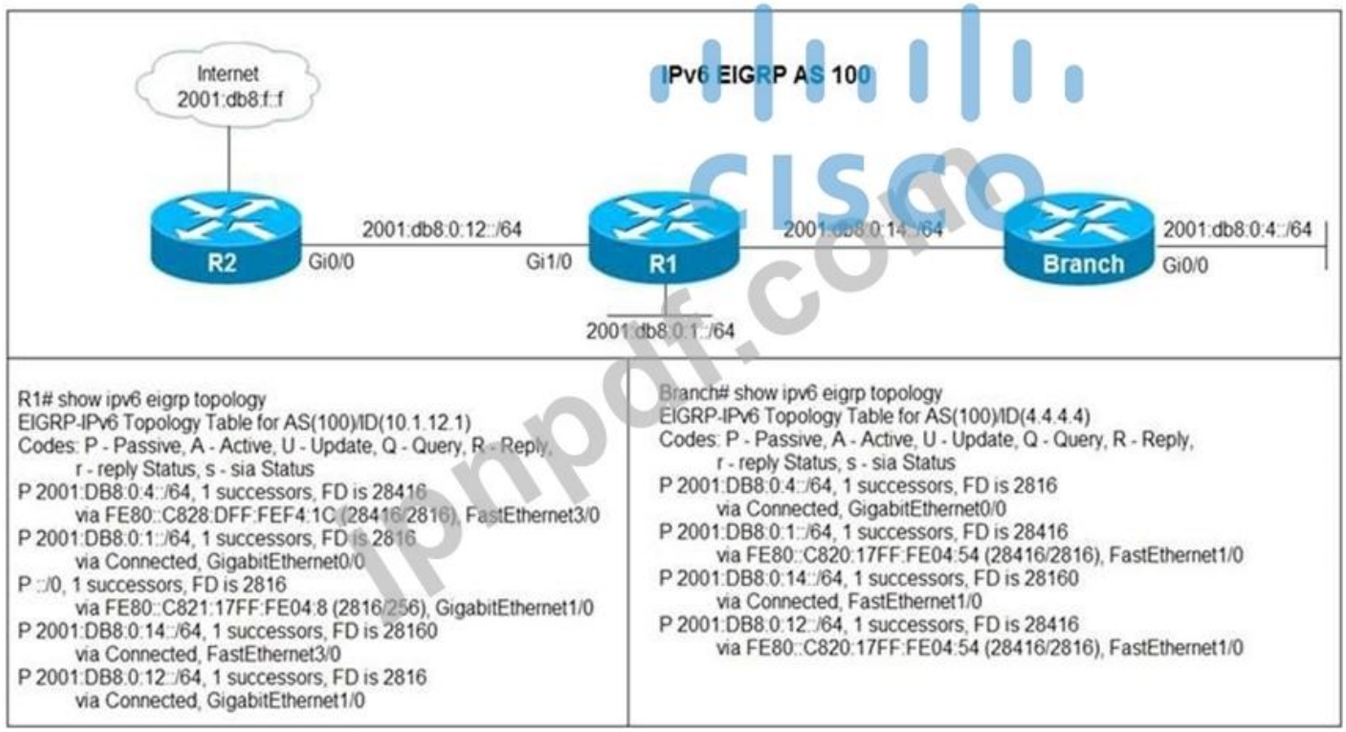
```
R1(config)#ip prefix-list EIGRP seq 10 permit 10.0.0.0/8
R1(config)#ip prefix-list EIGRP seq 20 deny 0.0.0.0/0 le 32
R1(config)#router eigrp 10
R1(config-router)#distribute-list prefix EIGRP in Ethernet0/0

R1#show ip route eigrp | include 10.
D EX 10.0.0.0/8 [170/2665332] via 192.168.10.1, 00:00:10,
Ethernet0/0
```

エンジニアは、ネットワーク 10 のプレフィックスの大部分を許可する代わりにフィルタリングするプレフィックス リスト フィルタを適用します。どのアクションで問題が解決しますか?
A. コマンドを変更します。Ip prefix-list EIGRP seq 10許可 10.0.0.0/8 le 32 コマンドを変更します。
B. ip prefix-list EIGRP seq 10 allowed 10.0.0.0/8 le 9 コマンドを変更します。
C. ip prefix-list EIGRP seq 20 allowed 10.0.0.0/8 ge 9 コマンドを変更します。
D. Ip prefix-list EIGRP seq 20 allowed 0.0.0.0/0 le 32 コマンドを変更します。
Answer: D (メーッセージを残す**)**

最新問題: **63**
IPv6 ソース ガードの 2 つの機能とは何ですか? (2つお選びください。)
A. IPv6 近隣探索とは独立して動作します。
B. 不明な送信元または未割り当てのアドレスからのトラフィックを拒否します。

C. 正規のトラフィックを許可するために、データが設定されたバインディング テーブルを使用します。
D. 近隣探索パケットの特定のパターンを検査することでトラフィックを拒否します。
E. 特定の送信元の DHCP パケットを検査することで、特定のトラフィックをブロックします。
Answer: B,C (メーッセージを残す**)**
セクション: さまざまな質問

最新問題**: 64**
展示を参照してください。



2001:db8:0:4::/64 のブランチ ネットワーク内のユーザーは、インターネットにアクセスできないと報告しています。この問題を解決するには、IPv6 ルータ EIGRP 100 コンフィギュレーション モードでどのコマンドを発行しますか?
A. R1 で eigrp stub コマンドを発行します。
B. R2 で no neighbors stub コマンドを発行します。
C. R2 で eigrp コマンドを発行します。
D. R1 で no eigrp stub コマンドを発行します。
Answer: D (メーッセージを残す**)**

最新問題**: 65**
メンテナンス期間中に、金曜日から日曜日の夜の時間帯にのみ、内部ネットワーク (Eth0/0) からネットワーク外部への Telnet 接続を許可する Telnet 関連の設定を管理者が誤って削除してしまいました。どの構成で問題が解決しますか?

A.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range changewindow
!
time-range changewindow
periodic Friday Saturday Sunday 22:00 to 05:00
```

B.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range changewindow
!
time-range changewindow
periodic 22:00 to 05:00
```

C.

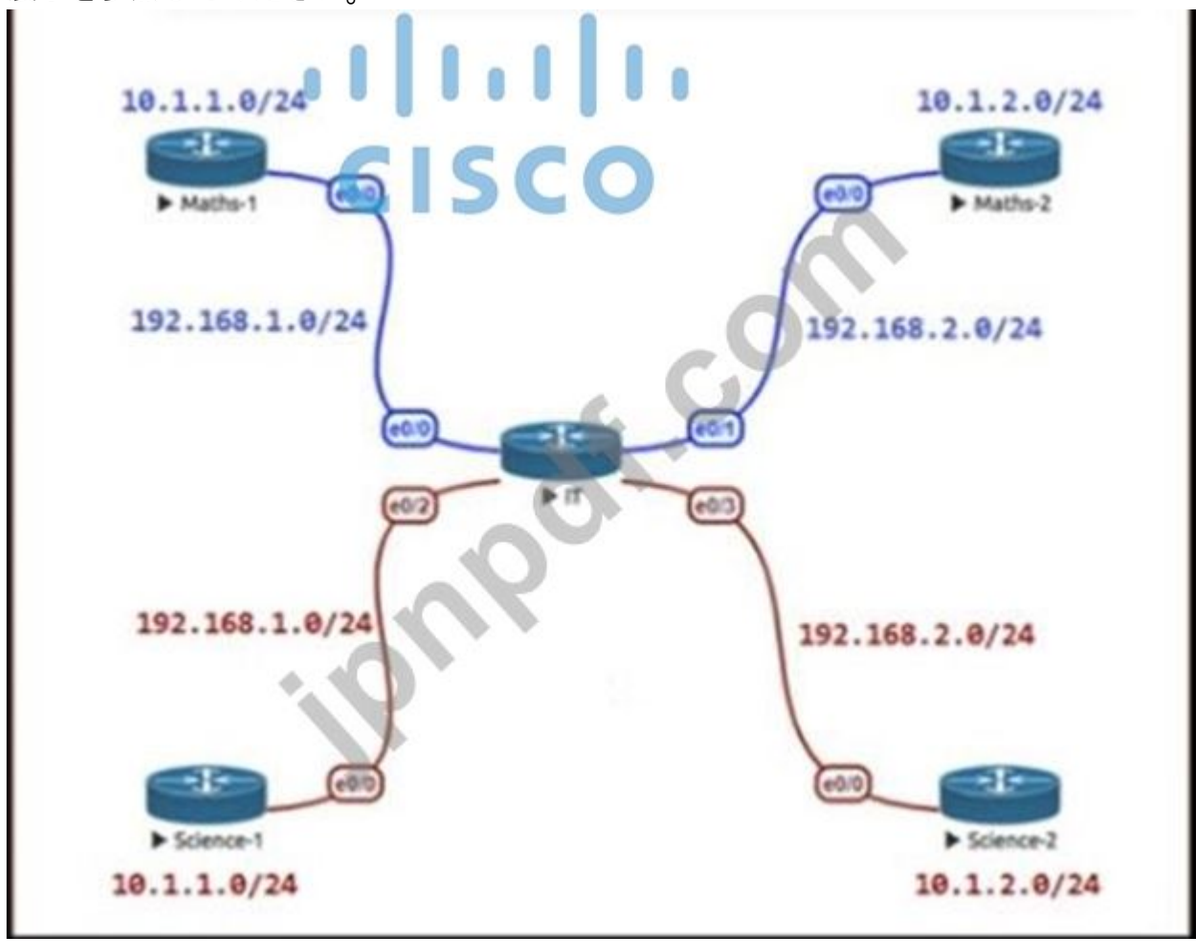
```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range changewindow
!
time-range changewindow
periodic Friday Saturday Sunday 22:00 to 05:00
```

D.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range changewindow
!
time-range changewindow
```

Answer: A (メーッセージを残す)

最新問題: **66**
展示を参照してください。



数学部門と科学部門は企業を通じてつながります。IT ルーターですが、数学部門のユーザーは科学部門にアクセスできてはなりません (逆も同様) どの構成でこのタスクを実行できますか?

A. VRF 定義 科学
！
インターフェースE0/2
IPアドレス 192.168.1.1 255.255.255.0
いいえ、閉じません
！
インターフェースE0/3
IPアドレス 192.168.2.1 255.255.255.0
いいえ、閉じません

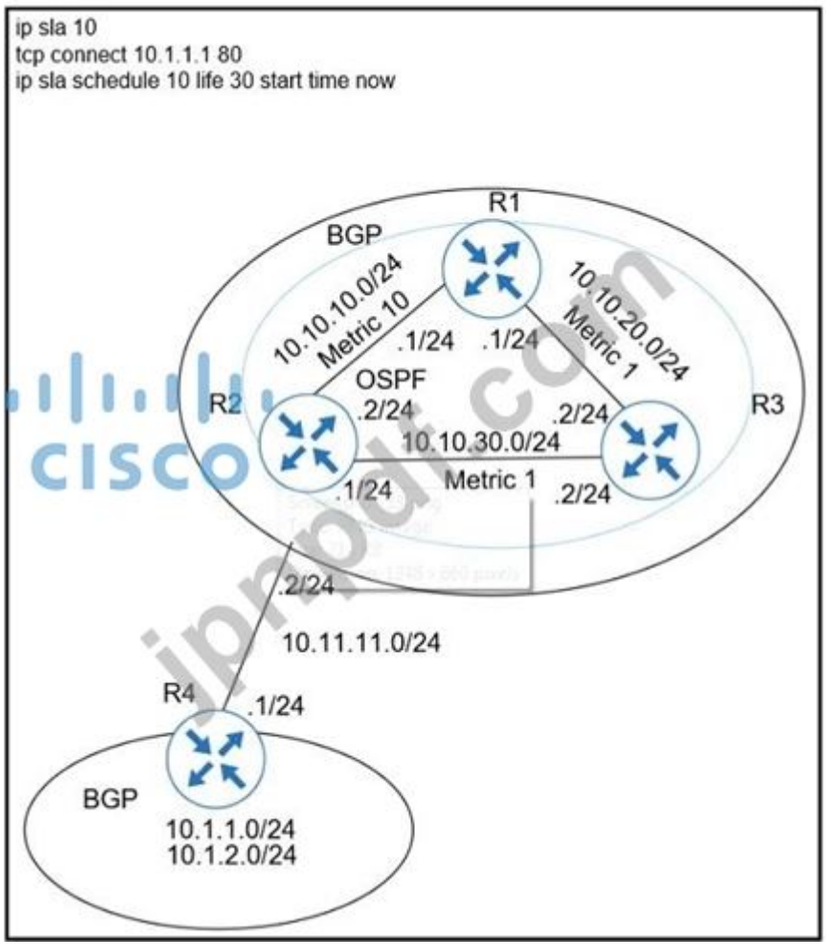
B. VRF 定義 科学
アドレスファミリー IPv4
！
インターフェースE0/2
IPアドレス 192.168.1.1 255.255.255.0
VRF 転送科学

いいえ、閉じません
！
インターフェースE0/3
IPアドレス 192.168.2.1 255.255.255.0
VRF 転送科学
いいえ、閉じません
C. VRF 定義 科学
アドレスファミリー IPv4
！
インターフェースE0/2
VRF 転送科学
IPアドレス 192.168.1.1 255.255.255.0
いいえ、閉じません
！
インターフェースE0/3
VRF 転送科学
IPアドレス 192.168.2.1
D. VRF 定義 科学
アドレスファミリー IPv4
！
インターフェースE0/2
IPアドレス 192.168.1.1 255.255.255.0
いいえ、閉じません
！
インターフェースE0/3
IPアドレス 192.168.2.1 255.255.255.0
いいえ、閉じません
Answer: C (メーッセージを残す**)**

最新問題**: 67**
左側の MPLS VPN デバイス タイプを右側の定義にドラッグ アンド ドロップします。

Answer:

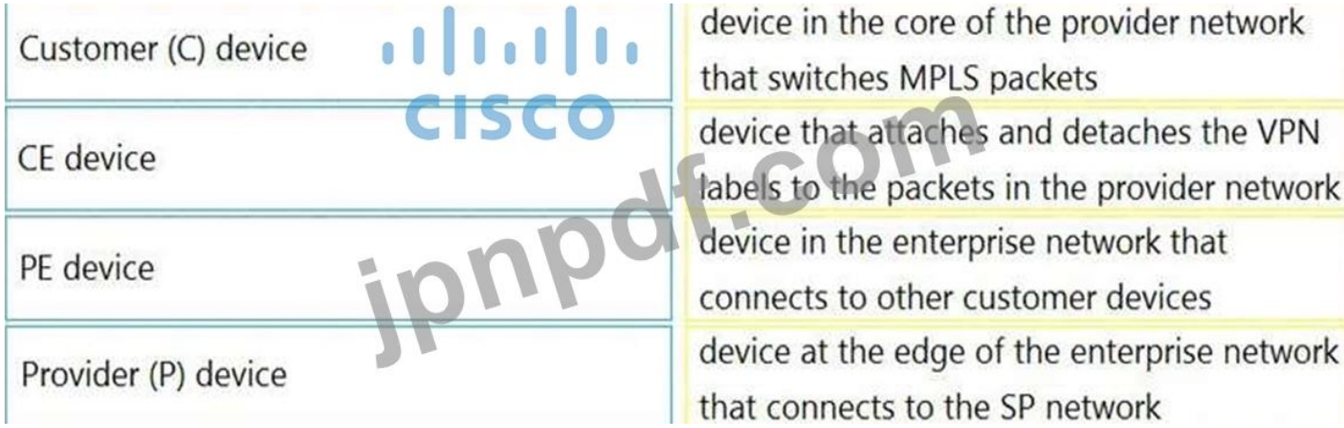
最新問題: **68**
展示を参照してください。



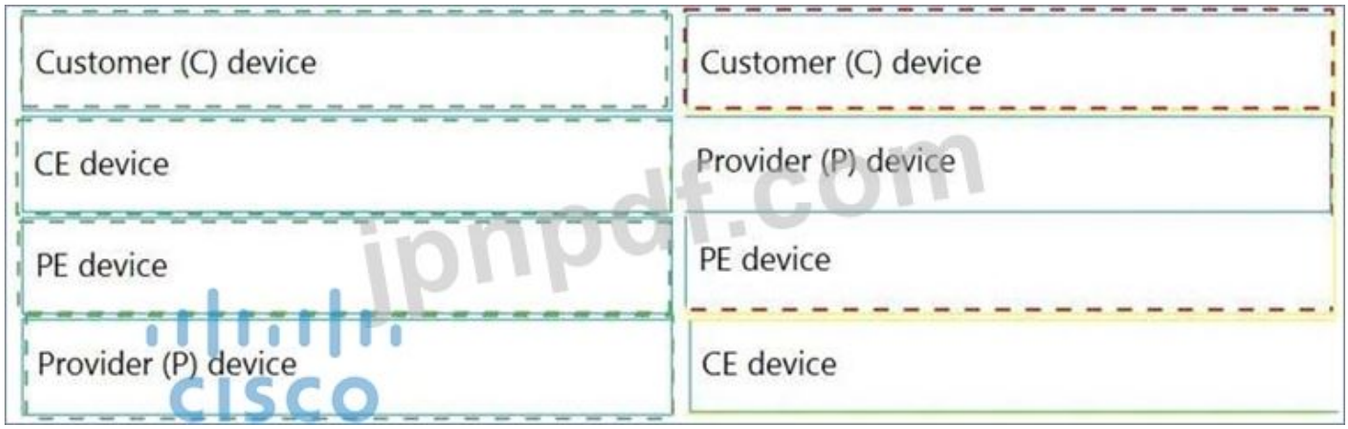
ユーザは、導入前に IP アドレス 10.1.1.1 上の非 SLA ホスト Web サーバが HTTP セッションを受け入れるかどうかをテストするために IP SLA プローブを設定しました。プローブが失敗しています。プローブを成功させるために、ネットワーク管理者はどのアクションを推奨する必要がありますか?
A. TCP 接続に制御無効オプションを追加します。
B. ip sla skill コマンドを再発行します。
C. ホストの icmp-echo コマンドを追加します。
D. IP sla スケジュール頻度を永久に変更します。
Answer: A (メーッセージを残す**)**

最新問題: **69**

MPLS VPN デバイス タイプを左側から右側の定義にドラッグ アンド ドロップします。

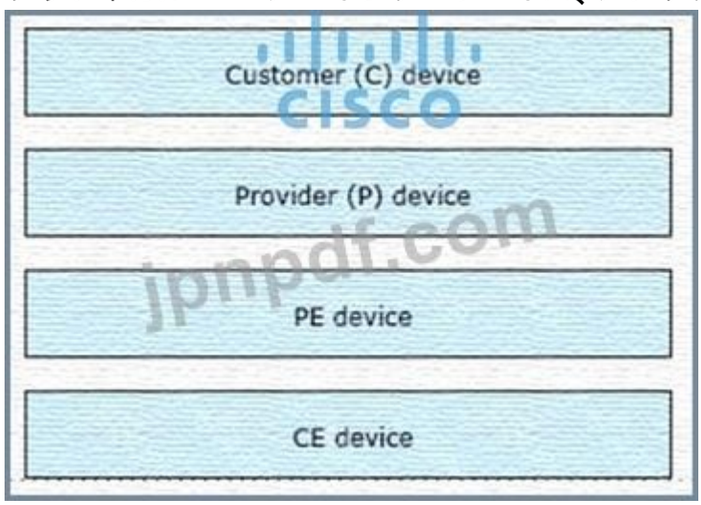


Answer:



説明

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



最新問題: **70**

展示を参照してください。

```
access-list 1 permit 1.1.1.0 0.0.0.255
!
route-map FILTER1 deny 10
match ip address 1
!
router eigrp 1
distribute-list route-map FILTER1 in
```

展示を参照してください。1.1.1.0/24 をフィルタリングしながら、近隣からのルートを復元するアクションはどれですか?

A. アクセス リストを許可ではなく拒否するように変更します。

B. アクセス リストに 2 行目を追加して、すべてを許可します。

C. アクセス リストを拒否するのではなく許可するようにルート マップを変更します。

D. ルート マップ許可 20 に 2 番目のシーケンスを追加します。

Answer: D (メーッセージを残す)

最新問題**: 71**

展示する：

どのアクションが認証の問題を解決しますか?

A. TACACS+ サーバーでユーザー名を設定します。

B. TACACS+ サーバーで UDP ポート 1812 を許可するように設定します。

C. ルーターが到達できるように TCP ポート 49 を構成します。

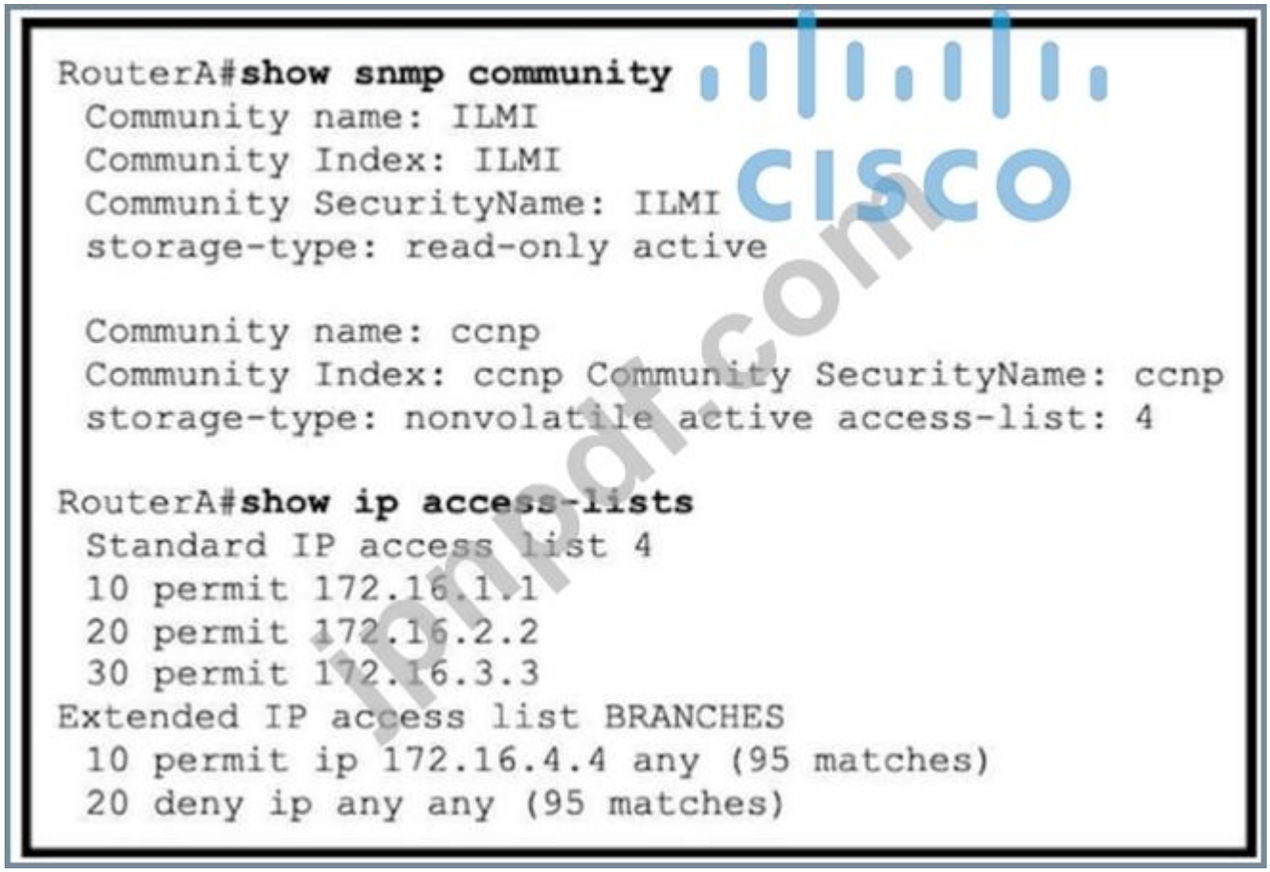
D. TACACS+ サーバーとルーター間で同じパスワードを設定します。

Answer: D (メーッセージを残す)

説明

出力の最後の行から、結果が 無効な AUTHEN パケット」であることがわかります。したがって、ユーザー名またはパスワードに問題が発生しました。

最新問題: **72**
展示を参照してください。



IP アドレス 172.16 4 4 の SNMP サーバーがホスト ルーター A にアクセスできない」を参照してください。ルーター A のどの設定コマンドが問題を解決しますか?
A. SNMP サーバー コミュニティ ccnp
B. SNMP サーバー ホスト 172.16.4.4 ccnp
C. アクセスリスト 4 許可 172.16.4.0 0.0.0.3
D. アクセスリスト 4 はホスト 172.16.4.4 を許可します
Answer: B (メーッセージを残す**)**

最新問題: **73**
展示を参照してください。

2001:db8:0:4::/64 のブランチ ネットワーク内のユーザーは、インターネットにアクセスできないと報告しています。この問題を解決するには、IPv6 ルータ EIGRP 100 コンフィギュレーション モードでどのコマンドを発行しますか?

A. R1 で eigrp stub コマンドを発行します。
B. R2 で no eigrp stub コマンドを発行します。
C. R1 で no eigrp stub コマンドを発行します。
D. R2 で eigrp stub コマンドを発行します。
Answer: C (メーッセージを残す**)**

最新問題**: 74**
IPv6 ND インスペクションに関する正しい記述はどれですか?
A. レイヤ 3 隣接テーブル内のステートレス自動構成アドレスのバインディングを学習し、保護します。
B. レイヤ 2 近隣テーブル内のステートレス自動構成アドレスのバインディングを学習し、保護します。
C. レイヤ 3 隣接テーブル内のステートフル自動構成アドレスのバインディングを学習し、保護します。
D. レイヤ 2 隣接テーブル内のステートフル自動構成アドレスのバインディングを学習し、保護します。
Answer: B (メーッセージを残す**)**
IPv6 ND インスペクションは、レイヤ 2 ネイバー テーブル内のステートレス自動構成アドレスのバインディングを学習し、保護します。IPv6 ND インスペクションは、信頼できるバインディング テーブル データベースを構築するために近隣探索メッセージを分析し、有効なバインディングを持たない IPv6 近隣探索メッセージはドロップされます。IPv6 から MAC へのマッピングが検証可能であれば、近隣探索メッセージは信頼できると見なされます。
この機能は、重複アドレス検出 (DAD)、アドレス解決、デバイス検出、および近隣キャッシュに対する攻撃など、近隣探索メカニズムに固有の脆弱性の一部を軽減します。

最新問題**: 75**

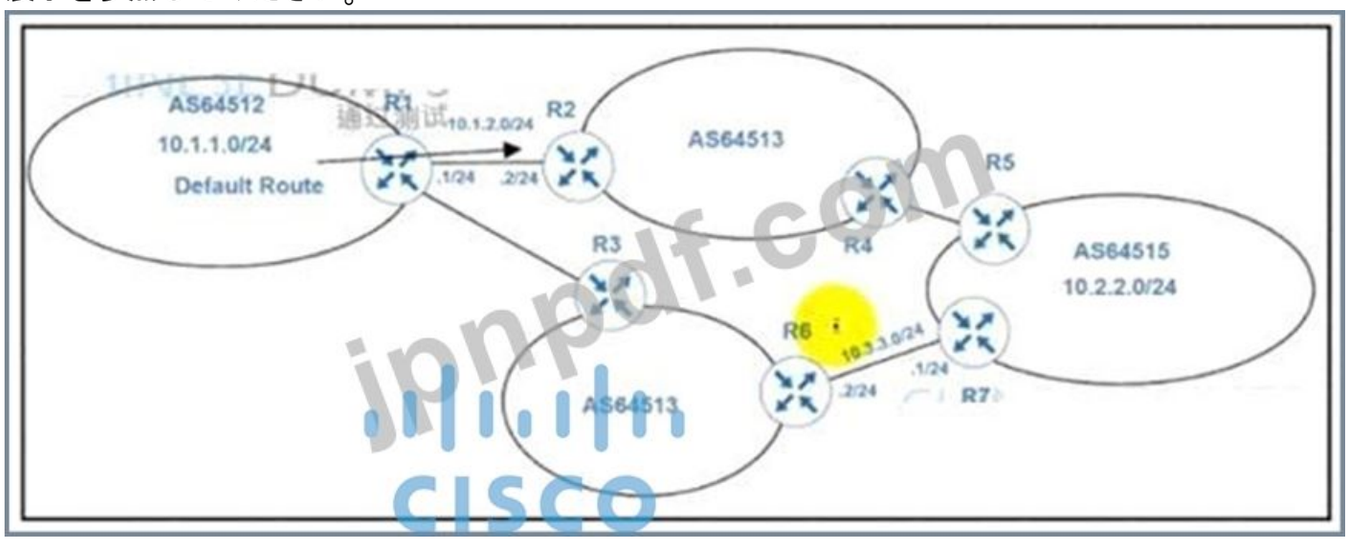
VRF-Lite セットアップ実装によるルート識別子の役割は何ですか?
A. VRF-Lite セットアップのマルチキャスト配信を有効にして、IGP ルーティング プロトコル機能を強化します。
B. IP アドレスを拡張して、どの VFP インスタンスに属しているかを識別します。
C. VRF-Lite セットアップのマルチキャスト配信を有効にして、EGP ルーティング プロトコル機能を強化します。
D. 2 つ以上の VRF インスタンス間のルートのインポートとエクスポートを管理します。
Answer: (解答を表示する**)**

最新問題: **76**
展示を参照してください。

エンジニアが DMVPN を設定し、R2 および R3 でハブ ロケーション プレフィックス 10.1.1.0724 を受信します。R3 プレフィックス 10 1.3.0/24 は R2 では受信されません。R2 プレフィックス 10.1,2.0/24 は R3 で受信されません。どのアクションが問題を留保しますか?
A. スプリット ホライズンにより、スポーク ルータ間でルートがアドバタイズされなくなります。これは、R1 のトンネル インターフェイスでコマンド no ip split-horizon eigrp 10 を使用して無効にする必要があります。
B. スポークツースポーク接続がありません。DMVPN 設定を変更して、R2 と R3 間のトンネル接続と、show ip eigrp neighbors コマンドを使用して確認したネイバー関係を有効にする必要があります。

C. スプリット ホライズンにより、スポーク ルータ間でルートがアドバタイズされなくなります。これは、R1 の Gi0/0 インターフェイスで no ip split-horizon eigrp 10 コマンドを使用して無効にする必要があります。
D. スポークツースポーク接続がありません。R2 と R3 の間に手動でネイバー関係を設定し、show ip eigrp neighbors コマンドの使用を確認して、DMVPN 設定を変更する必要があります。
Answer: A (メーッセージを残す**)**
説明
このトポロジでは、ハブ ルータは、そのトンネル インターフェイス上で R2 スポーク ルータからアドバタイズメントを受信します。ここでの問題は、同じトンネル インターフェイス上で R3 スポークとの接続も存在することです。スプリット ホライズンを無効にしない場合、ハブは R2 から R3 へ、またはその逆へのルートを中継しません。これは、同じインターフェイス トンネル上でこれらのルートを受信したため、その同じインターフェイスをアドバタイズして戻すことができないためです (スプリット ホライズン ルール)。したがって、スポークが相互に認識していることを確認するために、ハブ ルータで splithorizon を無効にする必要があります。

最新問題**: 77**
展示を参照してください。



エンジニアは、プライマリ パスとして R3 AS64513 経由で 10.2.2.0/24 に到達し、R2 AS64513 経由でデフォルト ルート経由のバックアップ ルートに到達するように R1 上の PBR を設定する必要があります。すべての BGP ルートは R1 のルーティング テーブルにあります。ただし、静的デフォルト ルートは BGP ルートをオーバーライドします。どの PBR 構成が目的を達成しますか?

```
access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
!
route-map PBR permit 10
 match ip address 100
 set ip next-hop 10.3.3.1

access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
!
route-map PBR permit 10
 match ip address 100
 set ip next-hop recursive 10.3.3.1

access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!
route-map PBR permit 10
 match ip address 100
 set ip next-hop recursive 10.3.3.1

access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!
route-map PBR permit 10
 match ip address 100
 set ip next-hop 10.3.3.1
```

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: A (メーッセージを残す**)**

最新問題**: 78**
展示を参照してください。エンジニアは、ハブ ルータ R6 とブランチ ルータ R1、R2、および R3 の間にマルチポイント GRE トンネルを確立する必要があります。R1 でこのタスクを実行できる構成はどれですか?

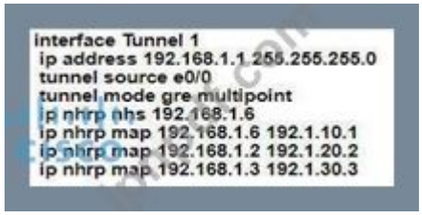
A)

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/1
 tunnel mode gre multipoint
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.6
```

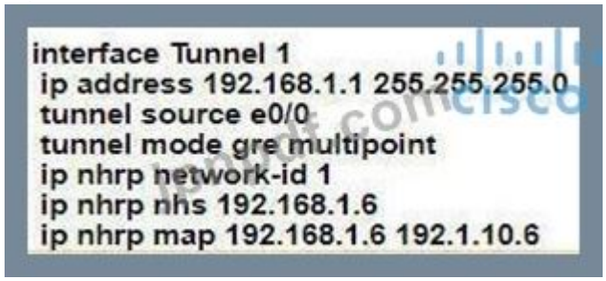
B)

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/1
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.1
 ip nhrp map 192.168.1.2 192.1.20.2
 ip nhrp map 192.168.1.3 192.1.30.3
```

C)

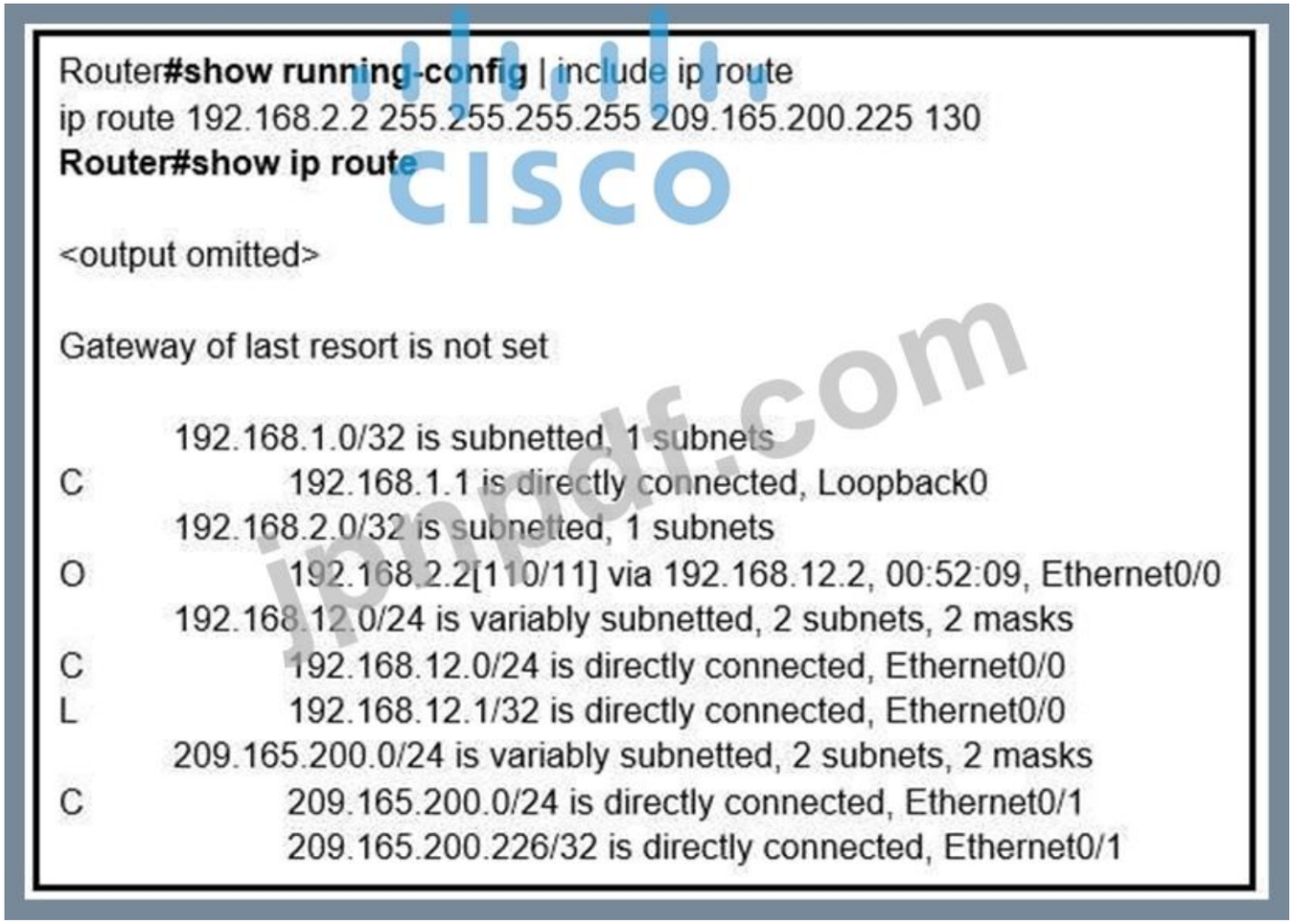


D)



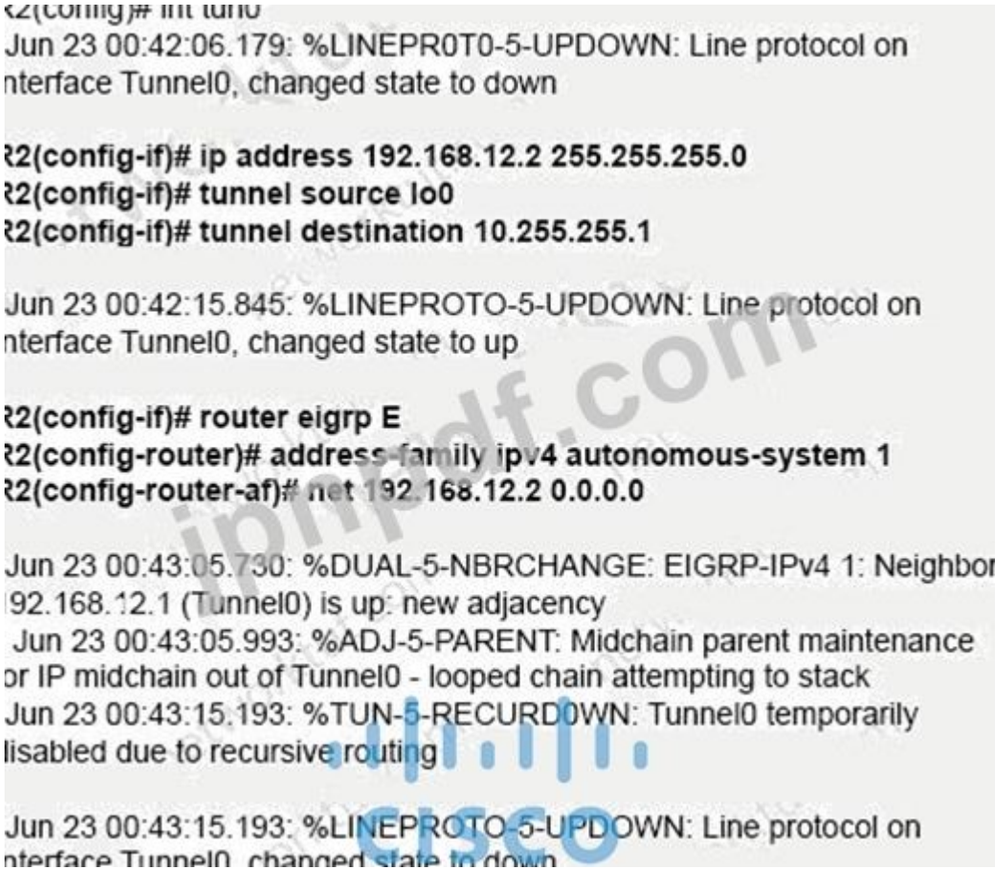
A. オプション B
B. オプション C
C. オプション A
D. オプション D
Answer: D (メーッセージを残す**)**

最新問題**: 79**
展示を参照してください。エンジニアはルーターに静的ルートを設定しますが、宛先へのルートを確認すると、別のネクストホップが選択されます。
その理由は何でしょうか?



A. 動的ルーティング プロトコルは常に静的ルートよりも優先されます。
B. OSPF ルートのメトリックがスタティック ルートのメトリックよりも低いです。
C. スタティック ルートに設定された AD は、OSPF の AD よりも上位です。
D. 静的ルートの構文が無効であるため、ルートは考慮されません。
Answer: C (メーッセージを残す**)**
セクション: レイヤ 3 テクノロジー

最新問題**: 80**
展示を参照してください。



管理者は、リモート ルータへの EIGRP ネイバーを確立するために GRE トンネルを設定しています。もう一方のトンネル エンドポイントはすでに構成されています。図のように構成を適用すると、トンネルがフラッピングを開始しました。どのアクションで問題が解決しますか?

A. Tunnel0 インターフェイス ネットマスクを使用するようにネットワーク コマンドを変更します。

B. R2 からトンネルを介して Loopback0 インターフェイスをアドバタイズします

C. トンネル宛先に一致するルートのトンネル経由での送信を停止します。

D. /31 ネットマスクを使用して、両方のルーターの Tunnel0 上の IP ネットワークを再アドレス指定します。

Answer: C (メーッセージを残す)

この質問では、トンネル IP アドレス 192.168.12.2 を反対側にアドバタイズしています。もう一方の端が EIGRP アドバタイズメントを受信すると、EIGRP 経由でトンネルの反対側に到達できることがわかります。

つまり、トンネル自体を経由してトンネルの宛先に到達します -> これにより、「再帰ルーティング」エラーが発生します。

注: このエラーを回避するには、トンネル インターフェイス上のトンネル宛先 IP アドレスを相手側にアドバタイズしないでください。

再帰的ルーティングの優れたリファレンス: https://networklessons.com/cisco/ccie-routing-switching/gretunnel- recursive-routing-error

最新問題**: 81**

エンジニアは、ホップ 10.1.1.1 のルーター上にデフォルトの静的ルートを作成します。エンジニアが検査したところ、ルータに Red と Blue の 2 つの VRF があることがわかりました。ネクスト ホップは両方の VRF で有効であり、割り当てられた各 VRF に存在します。どの構成で接続が実現しますか?

A)
```
ip route vrf BLUE 0.0.0.0 255.255.255.255 10.1.1.1
ip route vrf RED 0.0.0.0 255.255.255.255 10.1.1.1
```

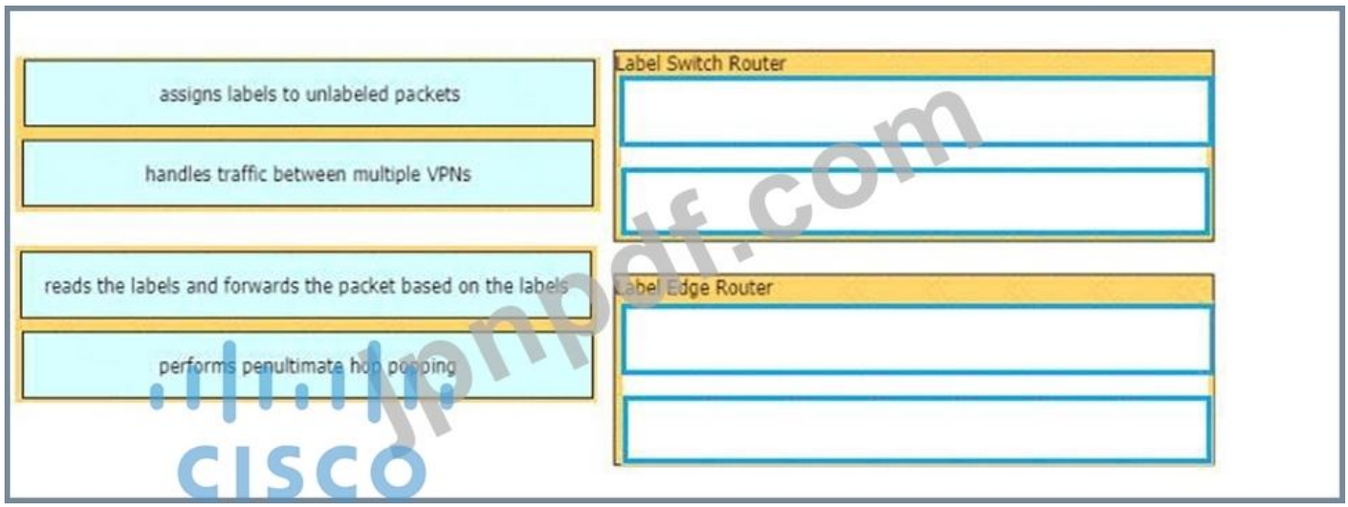
B)
```
ip route vrf Red 0.0.0.0 0.0.0.0 10.1.1.1
ip route vrf Blue 0.0.0.0 0.0.0.0 10.1.1.1
```

C)
```
ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

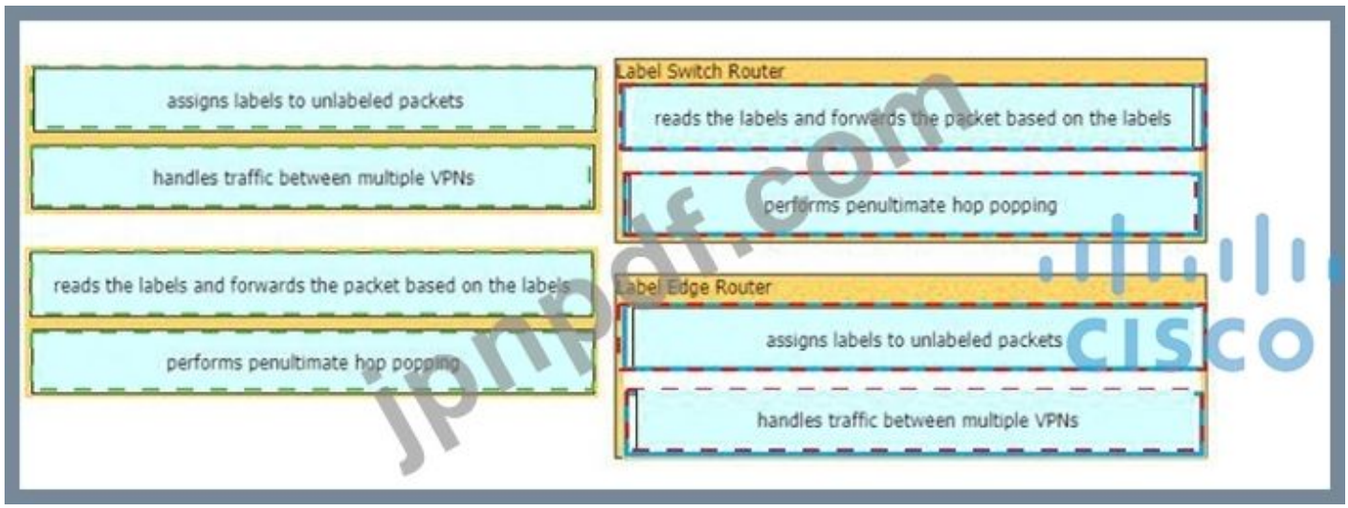
D)
```
ip route vrf Red 0.0.0.0 255.255.255.255 10.1.1.1
ip route vrf Blue 0.0.0.0 255.255.255.255 10.1.1.1
```

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: (解答を表示する**)**

最新問題: **82**
左側の操作を、右側の操作が実行される場所にドラッグ アンド ドロップします。



Answer:



説明

ラベル スイッチ ルーター 1. ラベルを読み取り、ラベルに基づいてパケットを転送します。

2.PHPを実行する

ラベル エッジ ルーター: 1 ラベルとラベルのないパケットを割り当てます。

2. 複数の VPN 間のトラフィックを処理します

最新問題: **83**

展示を参照してください。

展示を参照してください。R1 は SP1 をプライマリ パスとして使用します。ネットワーク エンジニアは、R1 から生成されたすべての SSH トラフィックを SP2 に強制する必要があります。どの構成でそのタスクを達成できますか?

A.

```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.20.20.1
!
interface Gig0/1
 ip policy route-map PBR_SSH
```

B.

```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.10.10.1
!
ip local policy route-map PBR_SSH
```

C.

```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.20.20.1
!
ip local policy route-map PBR_SSH
```

D.

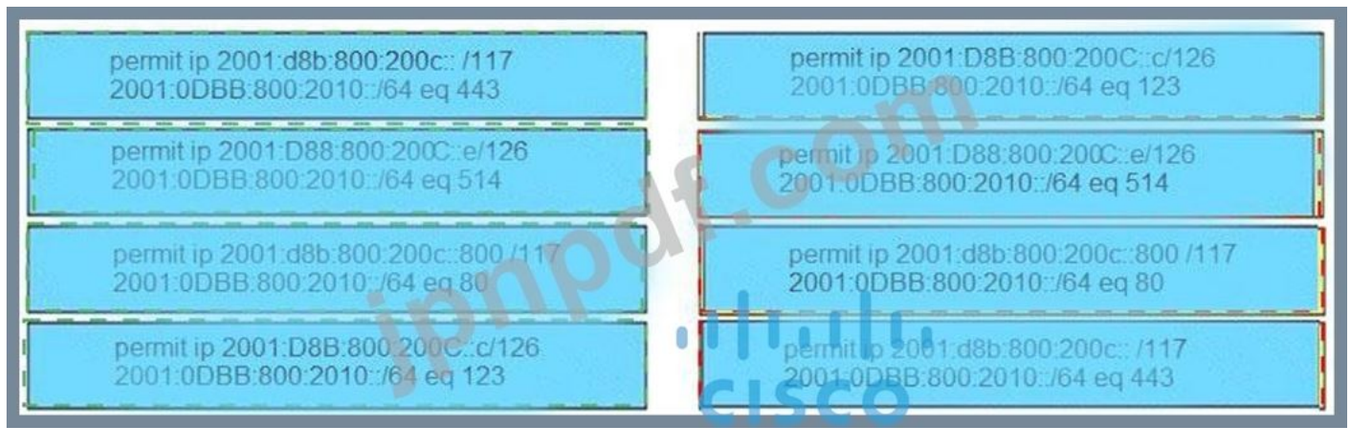
```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.20.20.1
!
interface Gig0/0
 ip policy route-map PBR_SSH
```

Answer: (解答を表示する)

最新問題: **84**
サービス プロバイダーが LVPN MPLS アプリケーションを利用するには、どの 2 つのコンポーネントが必要ですか? (2つお選びください。)
A. P ルーターは、PE ルーターに対する MP-iBGP 用に構成する必要があります
B. P ルーターは RSVP を使用して設定する必要があります。
C. PE ルーターは、他の PE ルーターとの MP-iBGP 用に構成する必要があります
D. CE に接続するには、MP-eBGP 用に PE ルーターを設定する必要があります
E. P ルーターと PE ルーターは、LDP または RSVP で構成されている必要があります
Answer: C,E (メーッセージを残す)
MPLSネットワークプロトコル
+ IGP: コア側およびコア側リンク上の OSPF、EIGRP、IS-IS+ コア側および/またはコア側リンク上の RSVP および/またはLDP ->
+ PE デバイス上の MP-iBGP (MPLS サービス用)、MP-BGP: マルチプロトコル ボーダー ゲートウェイ プロトコル、MPLS L3 VPN に使用 -> 。

最新問題: **85**
左側のアドレスを右側の適切な IPv6 フィルターの目的にドラッグ アンド ドロップします。

Answer:



説明
同じ回答が以下ですでに更新されています。

HTTP と HTTPs はそれぞれ TCP ポート 80 と 443 で実行されるため、それらを覚えておく必要があります。

Syslog は UDP ポート 514 で実行され、NTP は UDP ポート 123 で実行されるため、それらを覚えていれば、一致する答えを簡単に見つけることができます。ただし、2001:d88:800:200c::c/126 の範囲は 2001:d88:800:200c:0:0:0:c から 2001:d88:800:200c:0 までであるため、この質問にはタイプミスがある可能性があります。:0:0:f (合計 4 つのホスト)。ホスト 2001:0D88:0800:200c::1f はカバーされません。2001:D88:800:200c::e/126 も同様で、範囲は次のとおりです。

2001:d88:800:200c:0:0:0:c から 2001:d88:800:200c:0:0:0:f はホスト 2001:0D88:0800:200c::1c をカバーしません

。

最新問題: **86**

左側の操作を、右側の操作が実行される場所にドラッグ アンド ドロップします。

Answer:

最新問題: **87**

展示を参照してください。

Cisco DNA Center Assurance ダッシュボードの AP ステータスには、アクセス スイッチ インターフェイス G1/0/14 からの物理接続の問題がいくつか示されています。物理接続の問題を解決するための診断データを生成するコマンドはどれですか?

A. テスト ケーブル診断 TDR インターフェイス GigabitEthernet1/0/14

B. ケーブル診断 TDR インターフェイス GigabitEthernet1/0/14 を確認します。

C. ケーブル診断 TDR インターフェイス GigabitEthernet1/0/14 を表示します。

D. ケーブル診断 TDR インターフェイス GigabitEthernet1/0/14 を確認します。

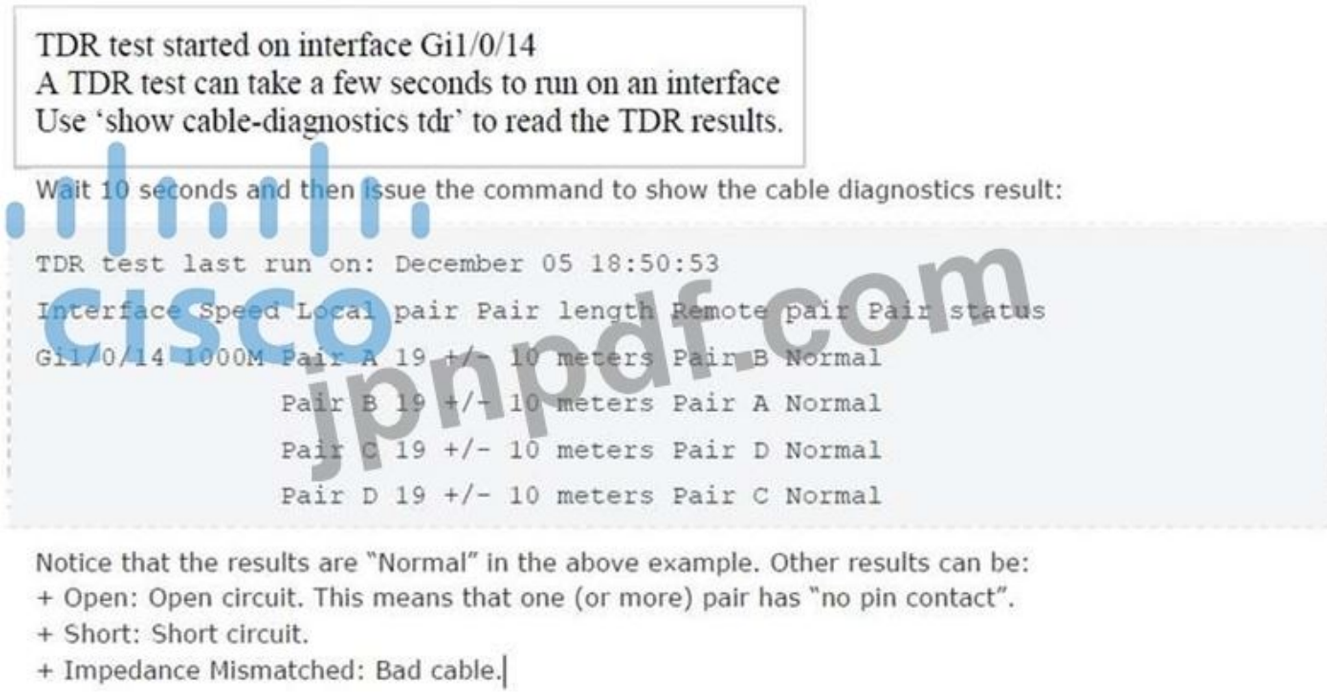
Answer: A (メーッセージを残す**)**

タイムドメイン反射率計 (TDR) 機能を使用すると、ケーブルに障害があるときにケーブルがオープンかショートかを判断できます。

TDR テストを開始するには、次の作業を実行します。

ステップ 1 「TDR テストの開始」testcable-diagnostics tdr {interface {interface-number}} ステップ 2 「TDR テスト カウンタ情報の表示」showcable-diagnostics tdr {interfaceinterface-number}

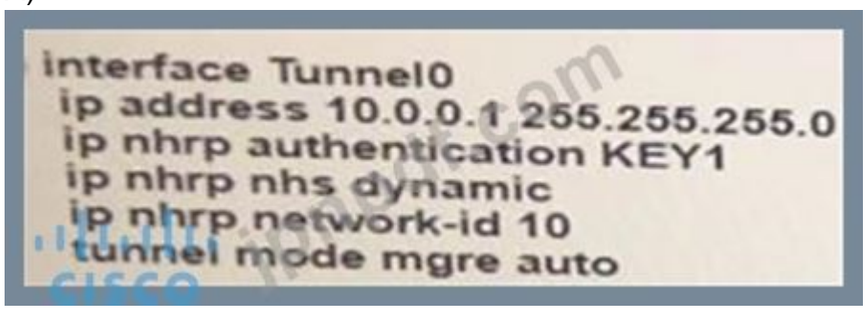
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/16-11/configuration_guide/int_hw/b_1611_int_and_hw_9600_cg/checking_port_status_and_connectivity.pdf



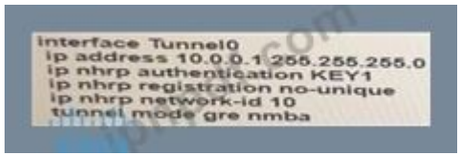
最新問題: **88**

ある会社は、インターネット上に 35 の支店を開設してビジネスを拡大しています。ネットワーク エンジニアは、ブランチ ルータで DMVPN を設定してハブ ルータに接続し、NHRP がスポーク ルータをマルチキャスト NHRP マッピングに安全に自動的に追加できるようにする必要があります。ハブ ルータでこの要件を満たす設定はどれですか?

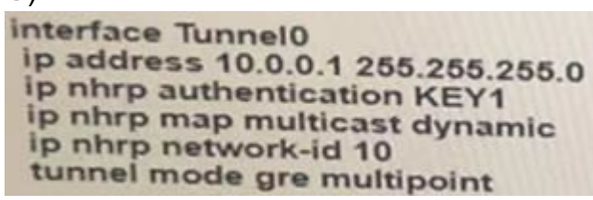
A)



B)



C)

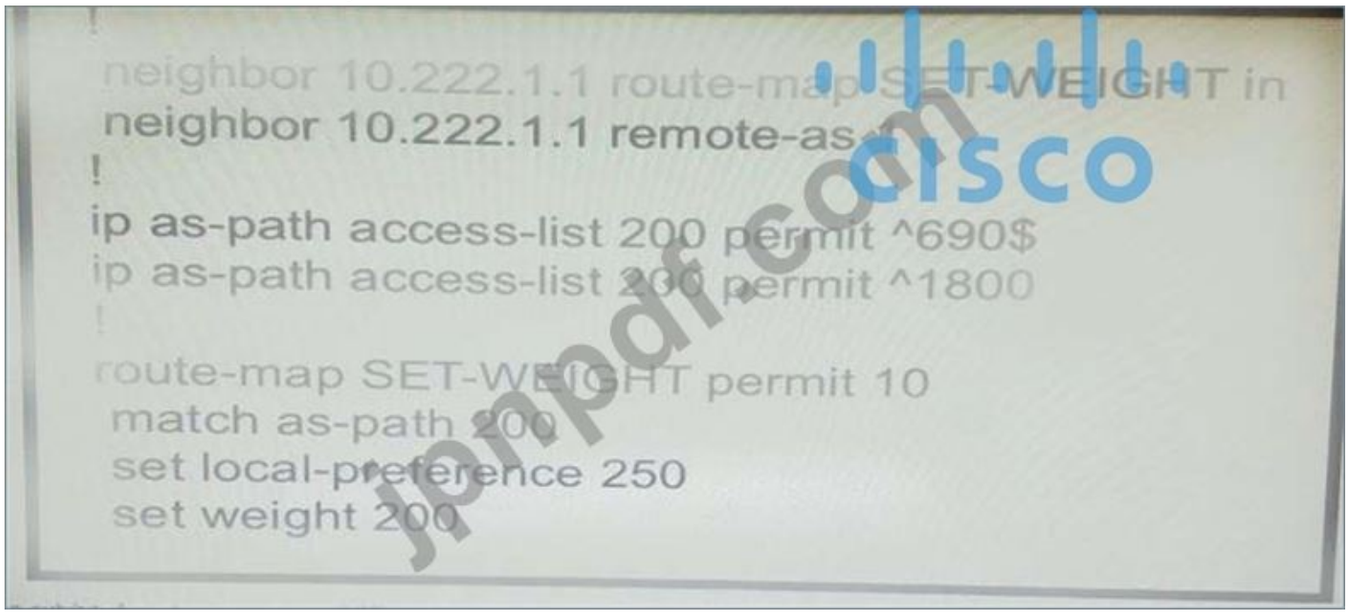


D)

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication KEY1
 ip nhrp map multicast 224.0.0.0
 ip nhrp network-id 10
 tunnel mode gre ipv4
```

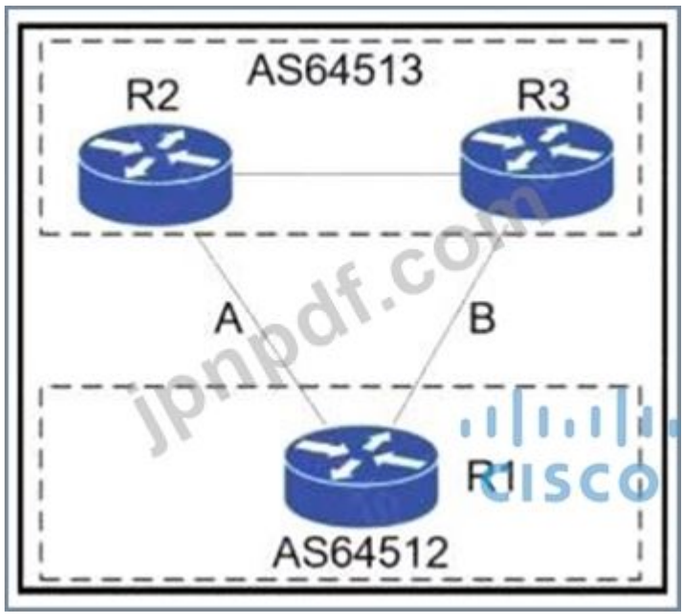
A. オプション A
B. オプション B
C. オプション C
D. オプション D
Answer: C (メーッセージを残す**)**
コマンド「ip nhrp map multicast Dynamic」を使用すると、NHRP がマルチキャスト NHRP マッピングにスポーク ルータを自動的に追加できます。

最新問題**: 89**
展示を参照してください。



AS 690 のルーターの複数のネイバーから BGP ルーティング アップデートを受信するルーター。ルーターが依然として AS 690 宛てのトラフィックを 10.222.1.1 以外のネイバーに送信する理由は何ですか?
A. 別の隣接ステートメントの重み値が 200 を超えています。
B. ローカル プリファレンス値は、ルート マップの重みと同じ値に設定する必要があります。
C. ルート マップが間違った方向に適用されています。
D. 別の近隣ステートメントのローカル優先値が 250 を超えています。
Answer: C (メーッセージを残す**)**

最新問題**: 90**
展示を参照してください。



AS64512 のネットワーク エンジニアは、メンテナンス中に BGP セッションを閉じずにリンク A からインバウンドおよびアウトバウンドのトラフィックを削除し、リンク A 上に ASN へのバックアップ リンクが存在するようにする必要があります。

R1 上のどの BGP 構成がこの目標を達成しますか?

A.

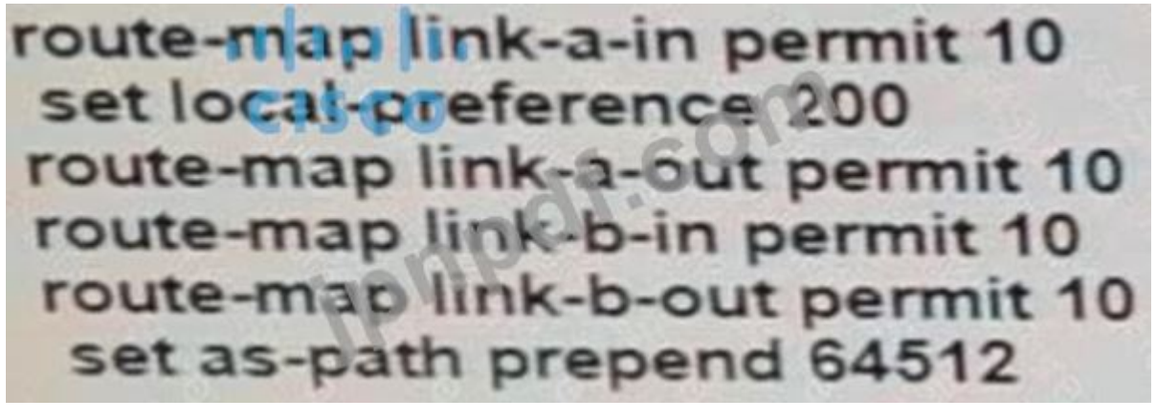
```
route-map link-a-in permit 10
 set weight 200
route-map link-a-out permit 10
route-map link-b-in permit 10
 set weight 100
route-map link-b-out permit 10
  set as-path prepend 64512
```

B.

```
route-map link-a-in permit 10
route-map link-a-out permit 10
 set as-path prepend 64512
route-map link-b-in permit 10
 set local-preference 200
route-map link-b-out permit 10
```

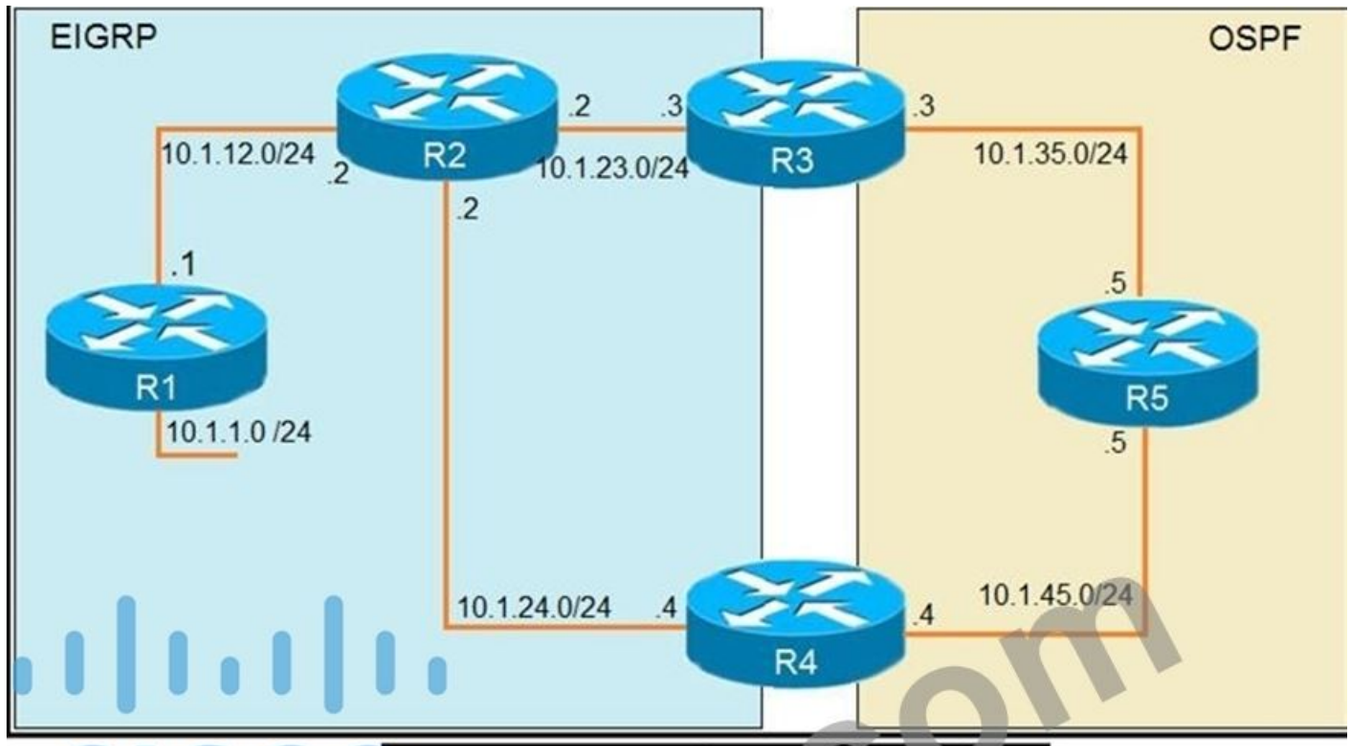
C.

```
route-map link-a-in permit 10
 set weight 200
route-map link-a-out permit 10
 set as-path prepend 64512
route-map link-b-in permit 10
 set weight 100
route-map link-b-out permit 10
```

D. 

Answer: B (メーッセージを残す)

最新問題: **91**
展示を参照してください。




```
R1
router eigrp 1
 redistribute connected
 network 10.1.12.1 0.0.0.0

R3
router ospf 1
 redistribute eigrp 1 subnets
 network 10.1.35.3 0.0.0.0 area 0

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500
!
router ospf 1
 network 10.1.45.4 0.0.0.0 area 0

R5#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

 1 10.1.35.3 80 msec 44 msec 20 msec
 2 10.1.23.2 44 msec 104 msec 64 msec
 3 10.1.24.4 44 msec 64 msec 40 msec
 4 10.1.45.5 24 msec 40 msec 20 msec
 5 10.1.35.3 92 msec 144 msec 148 msec
 6 10.1.23.2 108 msec 76 msec 80 msec
        <output truncuated>
```


R5 からのトレース ルートの出力には、ネットワーク内のループが示されています。このループを防ぐ構成はどれですか?

A)

```
R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
 match tag 1
!
route-map FILTER-TAG permit 20
```

B)

```
R3
router eigrp 1
 redistribute OSPF 1 route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
 network 10.1.24.4 0.0.0.0
!
route-map FILTER-TAG deny 10
 match tag 1
!
route-map FILTER-TAG permit 20
```

C)

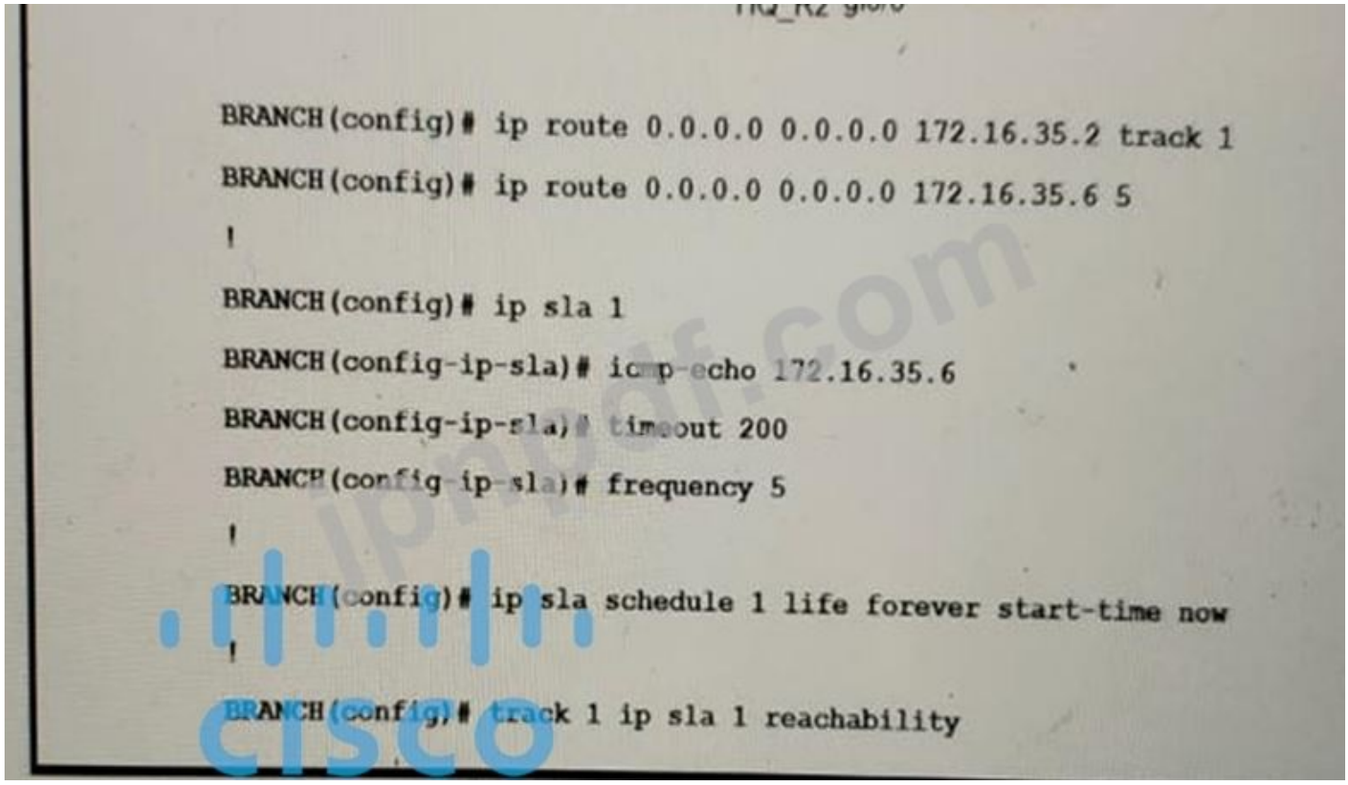
```
outer ospf 1
redistribute eigrp 1 subnets route-map SET-TAG

oute-map SET-TAG permit 10
set tag 1

4
outer eigrp 1
redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG

oute-map FILTER-TAG permit 10
match tag 1
```

D)

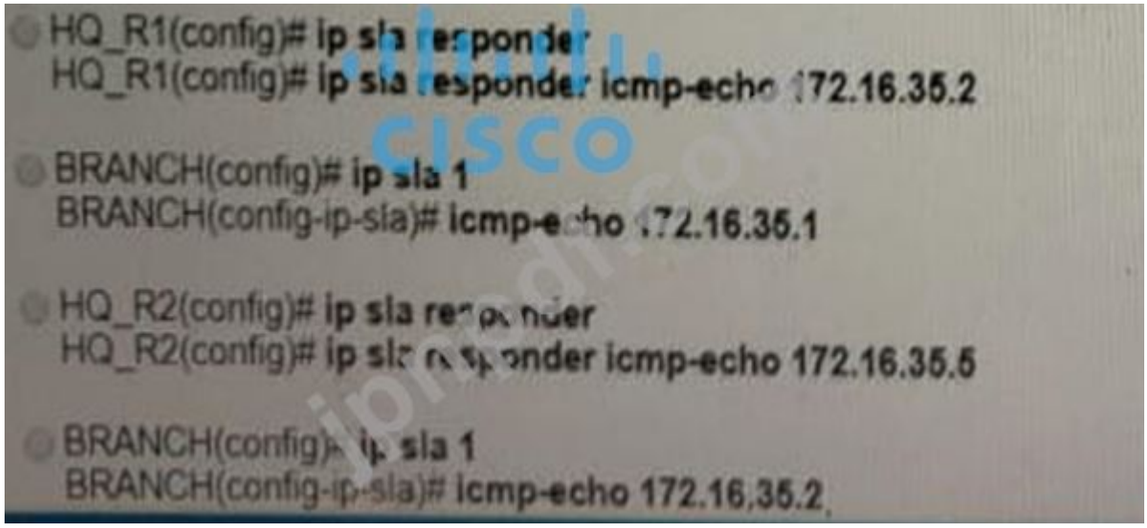
```
R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG deny 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
 match tag 1
```

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
ループの理由は、R2 が 10.1.1.1 宛てのパケットを R1 ではなく R4 に転送しているためです。これは、redistribute OSPF ステートメントで BW メトリックの値が大きく、遅延の値が 1 であるためです。そのため、R2 は 10.1.1.0/24 サブネットに対して R1 ではなく R4 を選択し、ループが発生します。ここで、R5 は R3 から 10.1.1.0/24 を学習し、同じルートを R4 にアドバタイズし、R4 は EIGRP に再配布します。OSPF で EIGRP を再配布中に R3 がタグ 1 を設定し、R4 が再配布中にタグ 1 を持つすべての OSPF ルートを拒否した場合、10.1.1.0/24 は EIGRP にアドバタイズしません。したがって、ループは壊れます。

最新問題: **92**
別紙を参照してください。

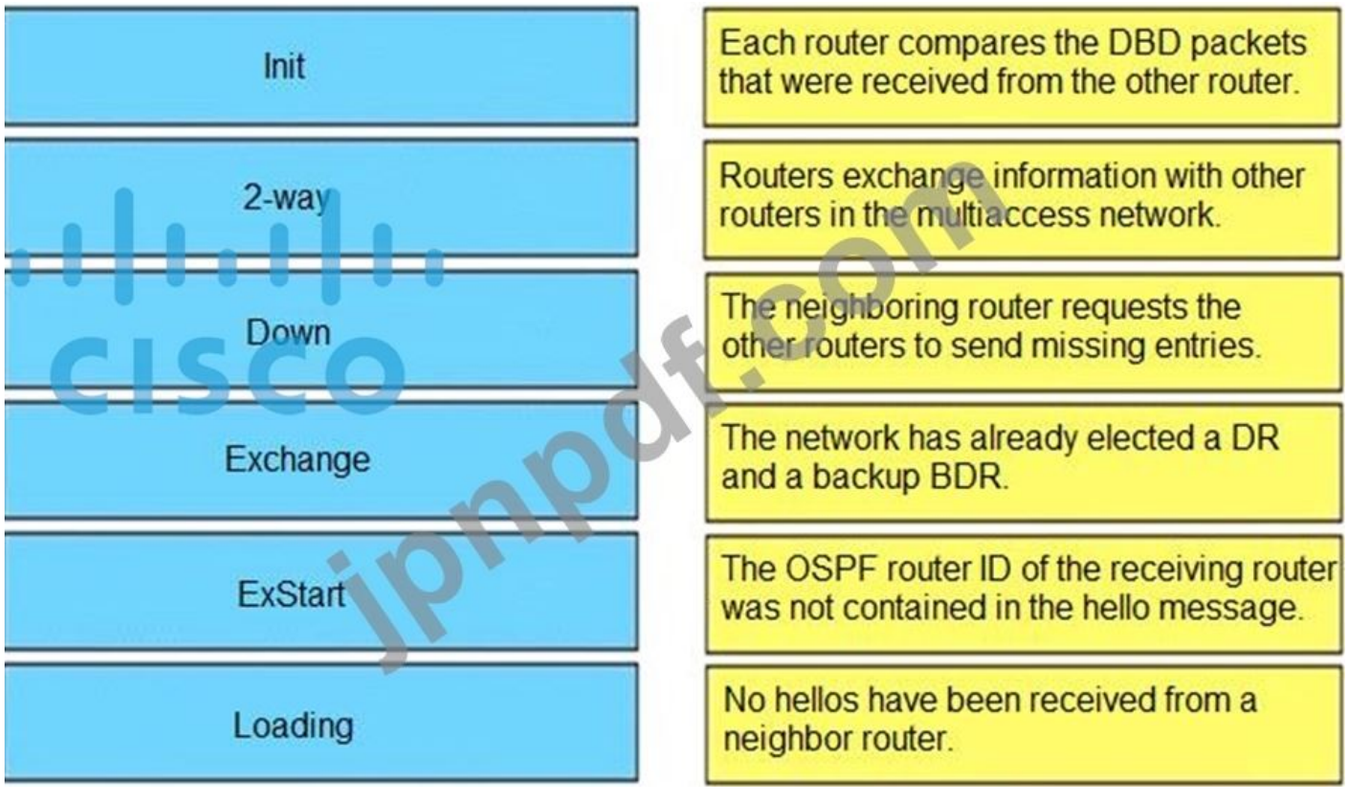


ブランチ ネットワークからのトラフィックは、パスが使用できない場合を除き、本社 R1 を経由してルーティングされる必要があります。エンジニアは、BRANCH ルータ上の HQ_R1 ルータへのインターフェイスをシャットダウンしてこの機能をテストしましたが、192.168.20.0/24 はブランチ ルータから到達できなくなりました。どの構成セットが問題を解決しますか?

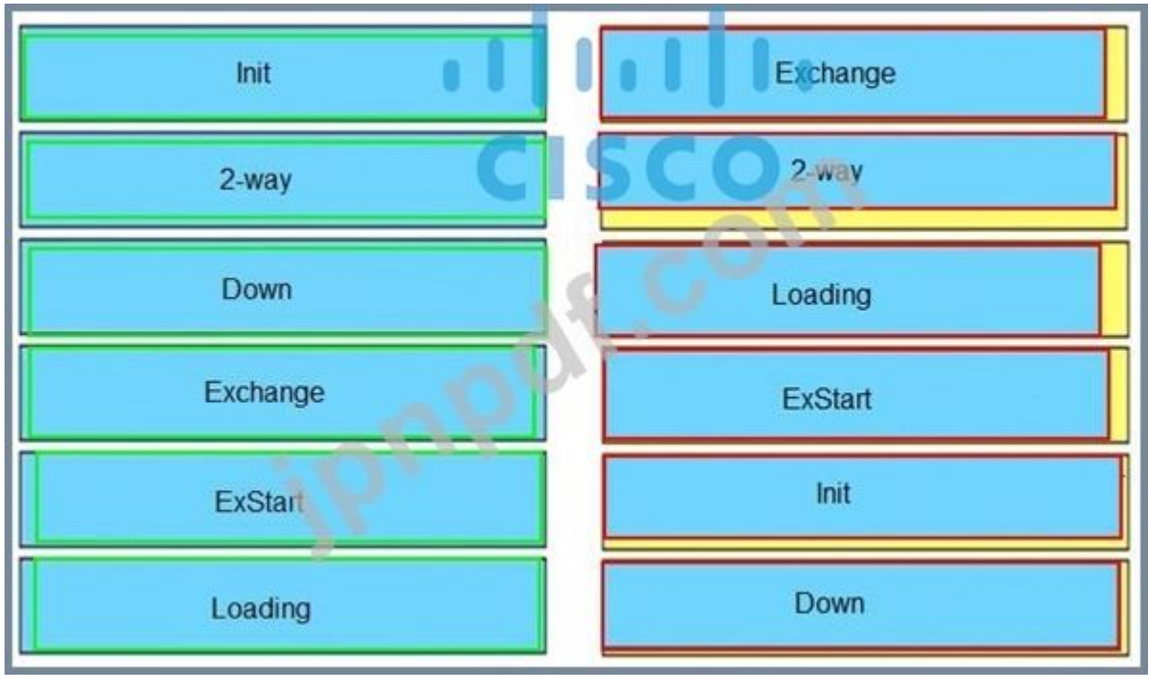


A. オプション B
B. オプション C
C. オプション D
D. オプション A
Answer: D (メーッセージを残す**)**

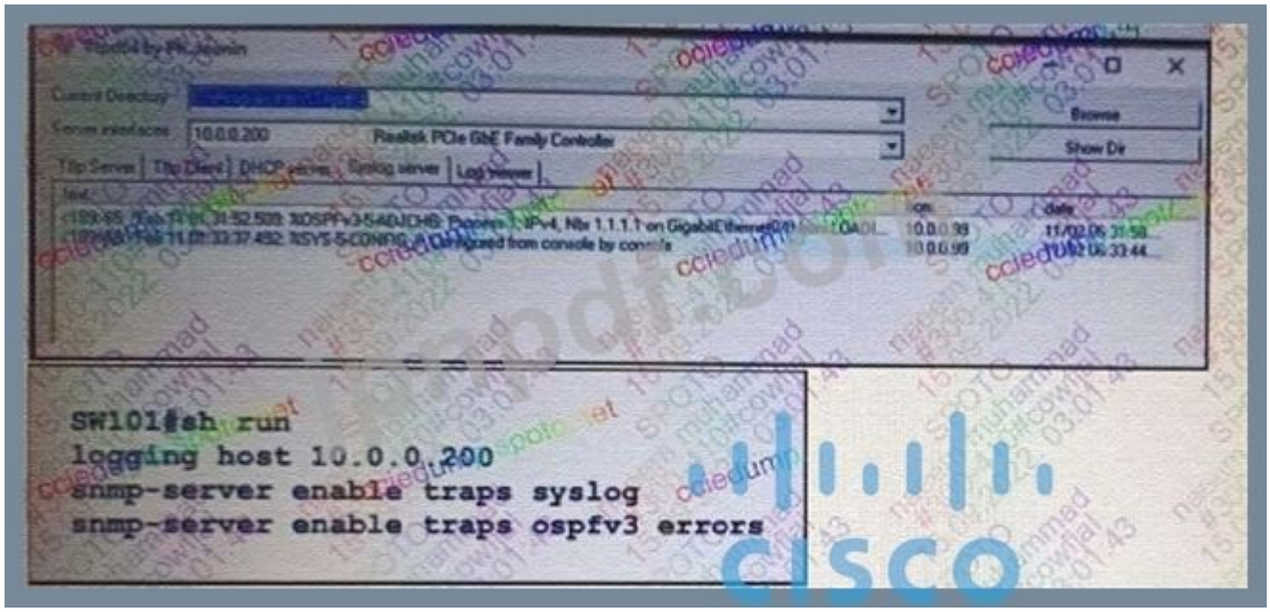
最新問題**: 93**
OSPF 隣接状態を左側から右側の正しい説明にドラッグ アンド ドロップします。



Answer:



最新問題: **94**
展示を参照してください。



エンジニアは、OSPFv3 インターフェイスの状態変更メッセージをサーバーに送信するように SW101 を設定します。ただし、一部の OSPFv3 エラーのみが記録されます。..を解決するのはどの組織ですか？

A. snmp-server-enable トラップ ospfv3 state-change restart-status-change
B. snmp サーバー有効トラップ ospfv3 状態変更 if-state-change
C. snmp-server-enable トラップ ospfv3 state-change if-state-change neighbors-state-change
D. snmp-server-enable トラップ ospfv3 状態変更ネイバー状態変更。
Answer: (解答を表示する**)**

最新問題: **95**
MPLS ネットワーク内のルート識別に関する記述は本当ですか?

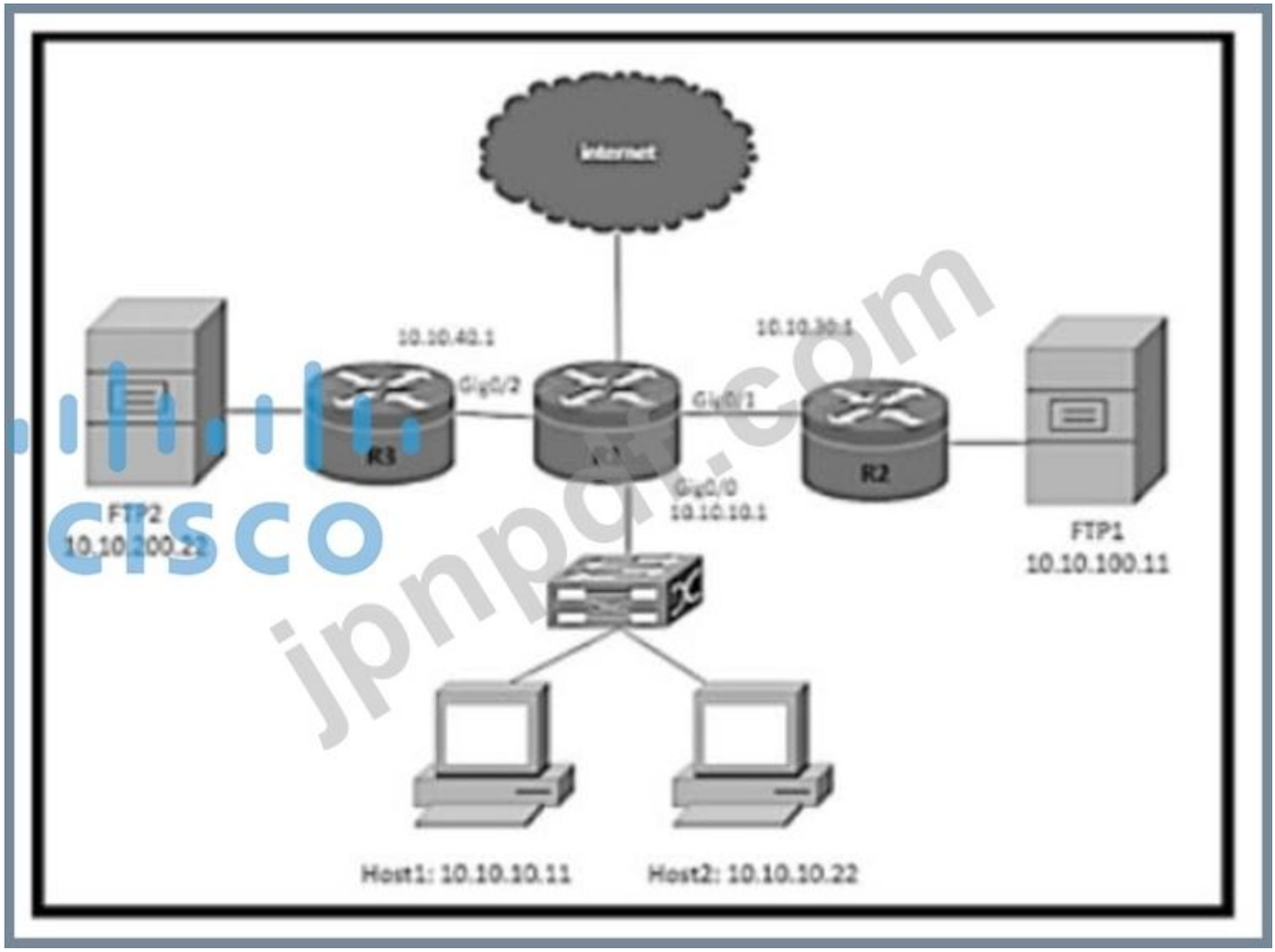
A. ルート識別は、どのプレフィックスがエッジ ルーターでインポートおよびエクスポートされるかを定義します。
B. ルート識別子により、ルーティング テーブルの複数のインスタンスがエッジ ルーター内で共存できます。
C. ルート識別により、MPLS ネットワーク全体で一意の VPNv4 アドレスが作成されます。
D. ルート識別はラベル バインディングに使用されます
Answer: B (メーッセージを残す**)**

最新問題**: 96**
エンジニアは、EIGRP ルートを要約し、特にループバックをアドバタイズするように Leak-map コマンドを設定しました
0、IP 10.1.1.1.255.255.255.252、サマリー ルート。設定を完了した後、顧客から、特定のループバック アドレスを持つ要約ルートを受信できないという苦情が寄せられました。どの 2 つの構成が問題を解決しますか? (2つお選びください。)

A. ルート マップ リーク ルート許可 10 を設定し、アクセス リスト 1 と一致します。
B. アクセス リスト 1 の許可 10.1.1.1.0.0.0.252 を設定します。
C. アクセス リスト 1 の許可 10.1.1.0.0.0.0.3 を設定します。
D. アクセス リスト 1 を設定し、ルート マップ Leak-Route で照合します。
E. ルートマップのリークルート許可 20 を設定します。
Answer: A,C (メーッセージを残す**)**

最新問題**: 97**
展示を参照してください。
管理者は、ISP1 に障害が発生したときに接続が ISP2 に切り替わらず、2 つの ISP 間でフラッピングしていることに気付きました。どのアクションで問題が解決しますか?
A. icmp-echo ステートメントに有効なsource-interface キーワードを含めます。
B. ISP1 ではなく ISP2 を介してデフォルト ルート上のトラック オブジェクト 1 を参照します。
C. ネクストホップと発信インターフェイスの両方を参照するように静的ルートを変更します。
D. ISP2 ルートのアドミニストレーティブ ディスタンスに一致するようにしきい値を変更します。
Answer: A (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-withdefault-routes-using-l.html

最新問題**: 98**
展示を参照してください。



展示を参照してください。R1 ルーティング テーブルには、FTP1 および FTP2 ファイル サーバーのプレフィックスが付いています。ネットワーク エンジニアは、次の要件に従って R1 を構成する必要があります。

Host1 は FTP1 ファイルサーバーを使用する必要があります。

Host2 は FTP2 ファイルサーバーを使用する必要があります。

R1 の要件を満たす構成はどれですか?

A.

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.40.1
route-map PBR_FTP permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.30.1
!
ip local policy route-map PBR_FTP
```

B.

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
interface GigabitEthernet 0/0
 ip policy route-map PBR_FTP
```

C.

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 any
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 any
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP  permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
interface GigabitEthernet 0/0
 ip policy route-map PBR_FTP
```

D.

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP  permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
ip local policy route-map PBR_FTP
```

Answer: B (メーッセージを残す)

最新問題: **99**
展示を参照してください。

198A:0:200C::1/64 からルータ 2 への Telnet トラフィックを拒否する設定はどれですか?

A)

B)

C)

D)

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**: 100**

```
OSPF: Send DBD to 10.100.1.2 on GigabitEthernet0/1 seq 0x9E6 opt
0x52 flag 0x7
   len 32
OSPF: Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1
[10]
OSPF: Send DBD to 10.100.1.2 on GigabitEthernet0/1 seq 0x9E6 opt
0x52 flag 0x7
   len 32
OSPF: Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1
[11]
%OSPF-5-ADJCHG: Process 1, Nbr 10.100.1.2 on GigabitEthernet0/1
from EXSTART to
   DOWN, Neighbor Down: Too many retransmissions
```

展示を参照してください。OSPF ネイバー関係が確立されない OSPF ネイバー隣接関係を復元するには何を設定する必要がありますか?

A. リモートルーター上の OSPF

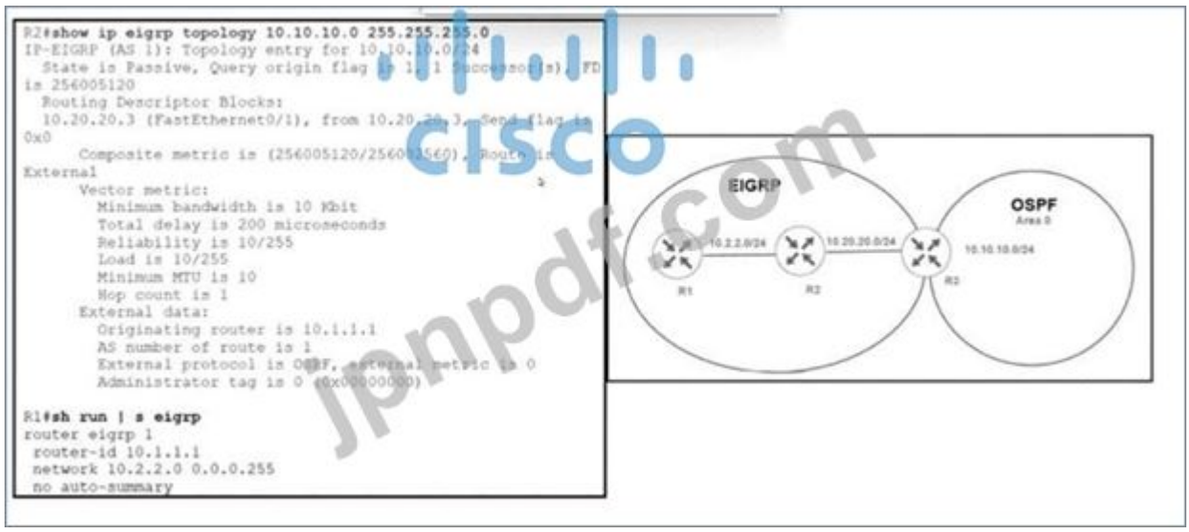
B. ルーター ID を使用します

C. hello タイマーの照合

D. 一致する MTU 値

Answer: (解答を表示する**)**

最新問題**: 101**



展示を参照してください。エンジニアは、プレフィックス 10.10.10.0/24 を OSPF から EIGRP に再配布するようにルータ R3 を設定しました。R1 はプレフィックスに接続していません。R1 でのプレフィックスの受信を有効にするアクションはどれですか?

A. R1 と R3 でルーター ID が重複しています。R1 はルーター ID を変更する必要があります。

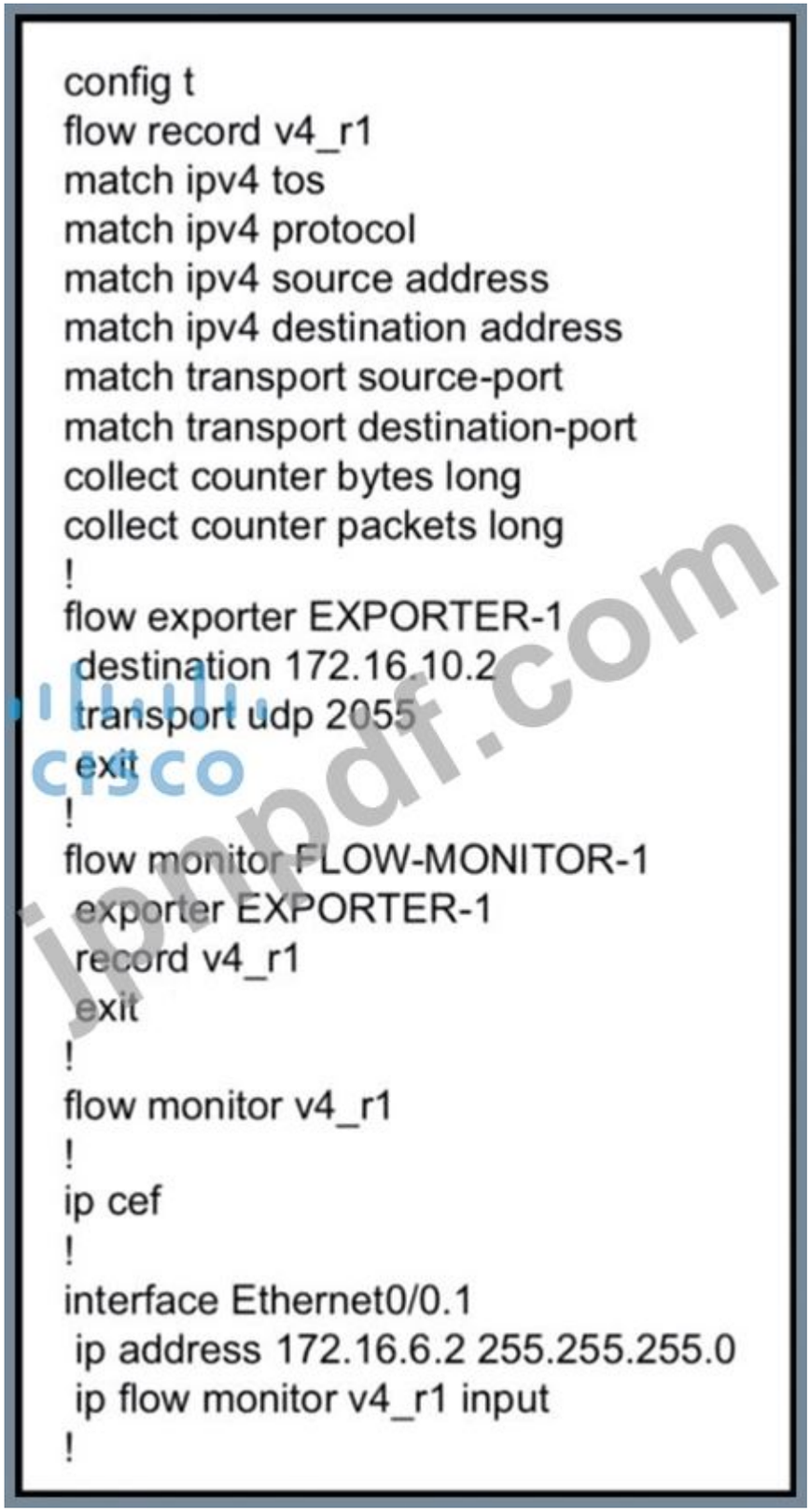
B. R1 ドキュメントには R2 との近隣関係がありません。EIGRP プロセスは R1 でクリアする必要があります。

C. R3 は、TTL 1 で 10.20.20 0'24 プレフィックスをアドバタイズしています。R3 は、このプレフィックスの TTL を 2 に設定する必要があります。

D. R1 は R3 のネクストホップ IP アドレスを受信していません。R2 は、EIGRP 内でネットワーク 10 20.20.0V24 を有効にする必要があります。

Answer: B (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。リモート サーバーが NetFlow データの受信に失敗しています どのアクションで問題が解決しますか?

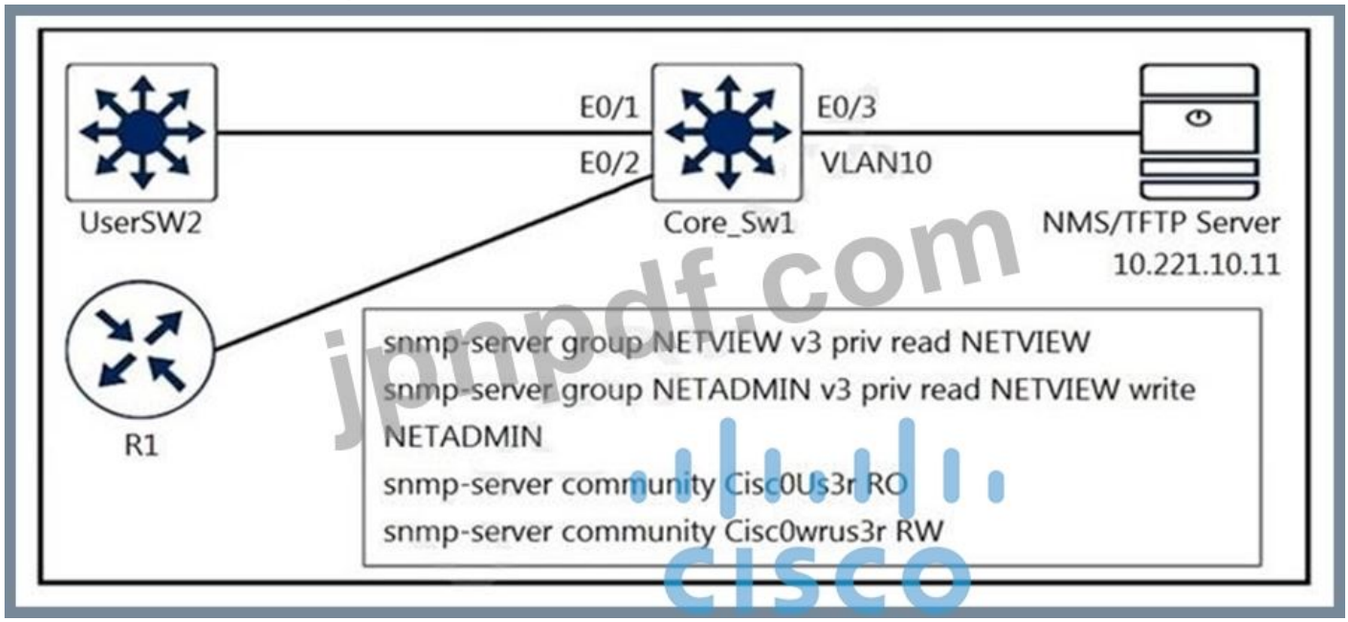
A. フロー トランスポート コマンド Transport udp 2055 を変更して、フロー モニタ プロファイルの下に移動します。

B. インターレース コマンドを Ip フロー モニター FLOW-MONITOR-1 入力に変更します。

C. フロー エクスポータ プロファイルの udp ポートを IP トランスポート udp 4739 に変更します。
D. フロー レコード コマンド レコード v4_r1 を変更して、フロー エクスポーター プロファイルの下に移動します。
Answer: B (メーッセージを残す**)**
展示を見ると、2 つのフロー モニタがあることがわかります。最初のモニタ FLOW-MONITOR-1」は正しく設定されていますが、2 番目のモニタ ｳ4_r1」は空のままであり、インターフェイス E0/0.1 がそれを使用しています。したがって、リモート サーバーは NetFlow データを受信しません。

最新問題: **103**
mGRE が使用されている場合、トンネルの反対側の NBMA アドレスを決定するためにどのプロトコルが使用されますか?
A. IPsec
B. NHRP
C. MP-BGP
D. OSPF
Answer: A (メーッセージを残す**)**

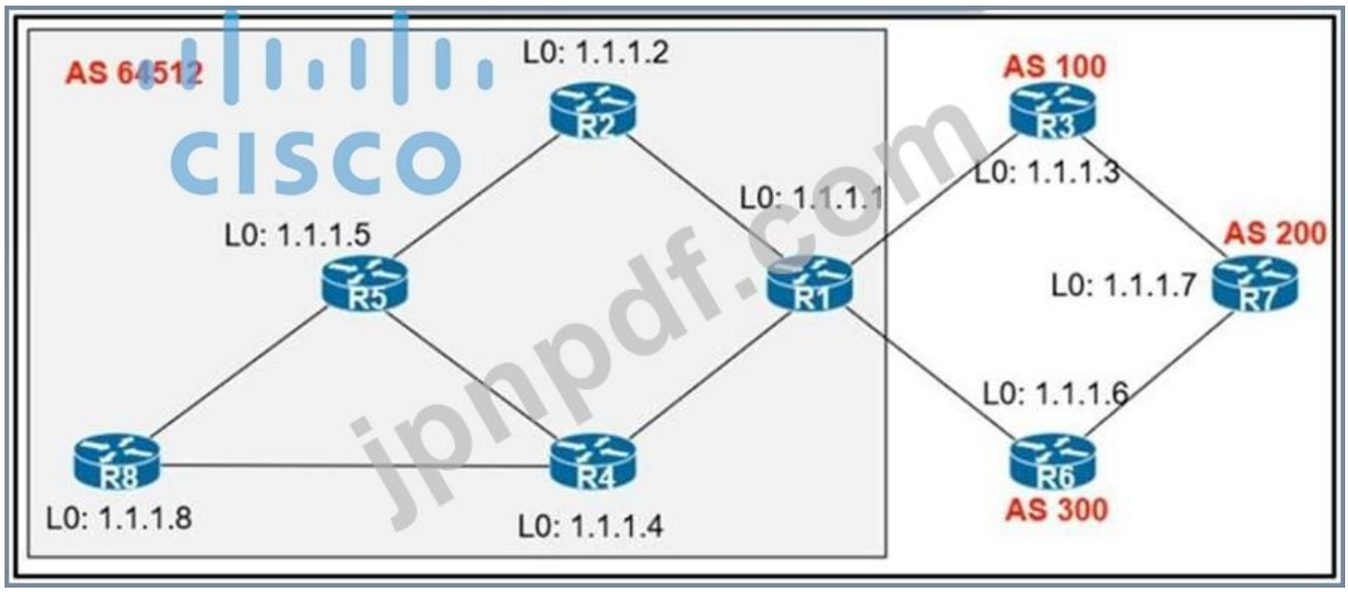
最新問題: **104**
展示を参照してください。



若手エンジニアがネットワーク デバイスに SNMP を設定しました。悪意のあるユーザーは、SNMP サーバーと TFTP サーバーを使用して、さまざまな設定をネットワーク デバイスにアップロードしました。未承認の NMS および TFTP サーバーからの変更を防止する設定はどれですか?
A. アクセスリスト 20 許可 10.221.10.11
B. アクセスリスト 20 許可 10.221.10.11
アクセスリスト 20 はすべてのログを拒否します
！
SNMP サーバー グループ NETVIEW v3 priv 読み取り NETVIEW アクセス 20

snmp サーバー グループ NETADMIN v3 priv 読み取り NETVIEW 書き込み NETADMIN アクセス 20
snmp サーバー コミュニティ Cisc0Us3r RO 20 snmp サーバー コミュニティ Cisc0wrus3r RW 20 snmp サーバー tftp-server-list 20
C. アクセスリスト 20 許可 10.221.10.11
アクセスリスト 20 はすべてのログを拒否します
D. アクセスリスト 20 許可 10.221.10.11
アクセスリスト 20 はすべてのログを拒否します
！
SNMP サーバー グループ NETVIEW v3 priv 読み取り NETVIEW アクセス 20
snmp サーバー グループ NETADMIN v3 priv 読み取り NETVIEW 書き込み NETADMIN アクセス 20
snmp サーバー コミュニティ Cisc0wrus3r RO 20 snmp サーバー コミュニティ Cisc0Us3r RW 20 snmp サーバー tftp-server-list 20
Answer: B (メーッセージを残す**)**

最新問題**: 105**
展示する：



エンジニアは R2 と R5 をルート リフレクタとして設定し、すべてのルートが eBGP ピアにアドバタイズするために R1 に送信されるわけではないことに気付きました。すべてのネットワークにわたる到達可能性を復元するには、すべてのルートをアドバタイズするルート リフレクタとしてどの iBGP ルーターを構成する必要がありますか?
A. R1 および R4
B. R1 および R5
C. R4 および R5
D. R2 および R5
Answer: C (メーッセージを残す**)**
R2 および R5 がルート リフレクタ (RR) である場合、R4 および R8 からのルートは R5 にアドバタイズされ、R5 は R2 にアドバタイズされます。ただし、R2 も RR であるため、R2 はそれらをドロップします。したがって、eBGP ピアにアドバタイズするためのルートの一部が R1 で欠落しています。

良い参考資料:
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/TECRST-2310.pdf ルート リフレクタ（RR）は完全に iBGP メッシュ化されている必要があるため、R1 と R1 の両方で RR を設定することはできません。R5.
トポロジ RR の中心にあるルーター、この場合は R4 と R5 を選択する必要があります。

最新問題: **106**
エンジニアは、DES による認証とデータの暗号化を使用して、管理サーバーに送信される SNMP 通知を構成しました。応答 PDU のエラーは、「UNKNOWNUSERNAME.WRONGDIGEST」として受信されます。どのアクションで問題が解決しますか?
A. SNMPv3 authPriv を使用して正しい認証パスワードを構成します。
B. SNMPv3 authNoPriv を使用して正しい認証パスワードを設定します。
C. SNMPv3 authNoPriv を使用して、正しい認証パスワードとプライバシー パスワードを構成します。
D. SNMPv3 authPriv を使用して、正しい認証パスワードとプライバシー パスワードを構成します。
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp- snmpv3.html

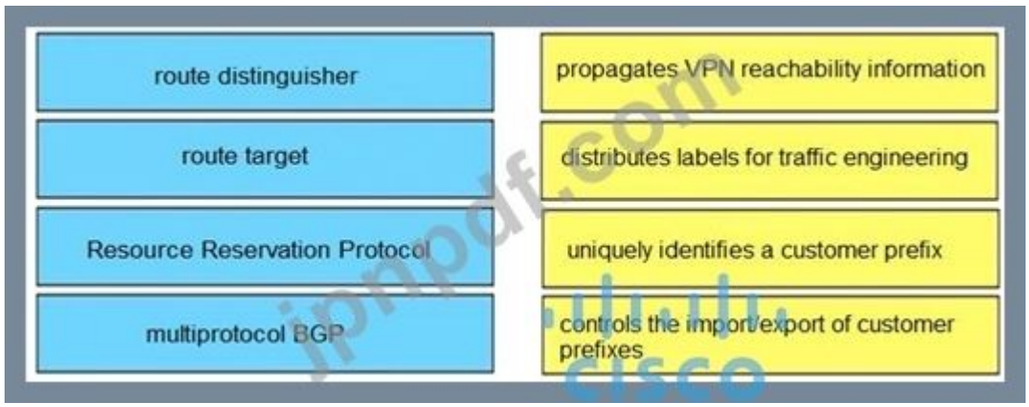
最新問題: **107**
展示を参照してください。

```
R2# show ip ospf neighbor
R2#
R2# debug ip ospf hello

*Feb 22 23:46:58.699: OSPF-1 HELLO Et1/1: Rcv hello from
10.255.255.1 area 0 10.0.23.1
*Feb 22 23:46:58.703: OSPF-1 HELLO Et1/1: Mismatched hello
parameters from 10.0.23.1
*Feb 22 23:46:58.703: OSPF-1 HELLO Et1/1: Dead R 30 C 20, Hello
R 10 C 10 Mask R 255.255.255.0 C 255.255.255.0
```

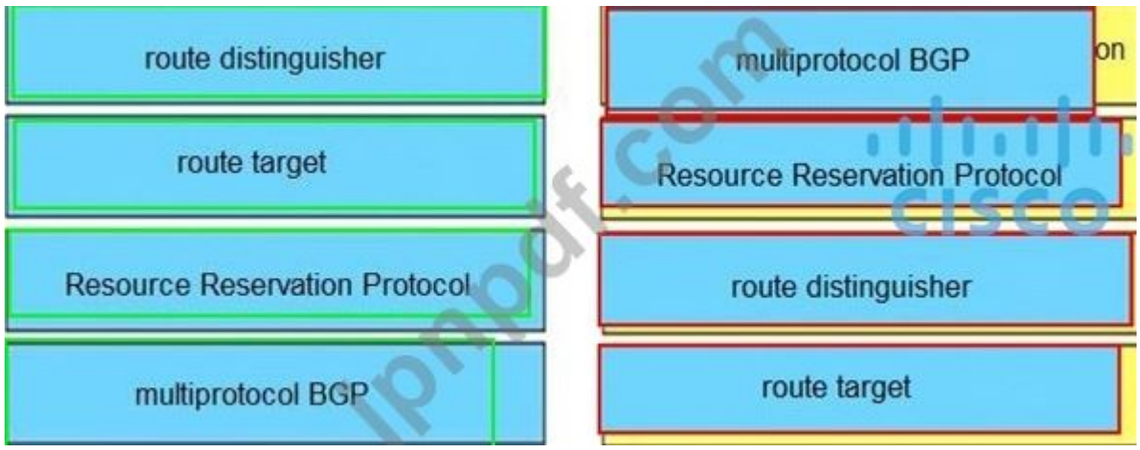
接続されているルータは OSPF ネイバーとして表示されません。どのアクションで問題が解決しますか?

A. R2 デッド タイマーを 20 に変更します。
B. R1 hello タイマーを 20 に変更します。
C. R1 デッド タイマーを 20 に変更します。
D. R2 hello タイマーを 20 に変更します。
Answer: C (メーッセージを残す**)**

最新問題**: 108**
左側の MPLS VPN の概念を右側の適切な説明にドラッグ アンド ドロップします。



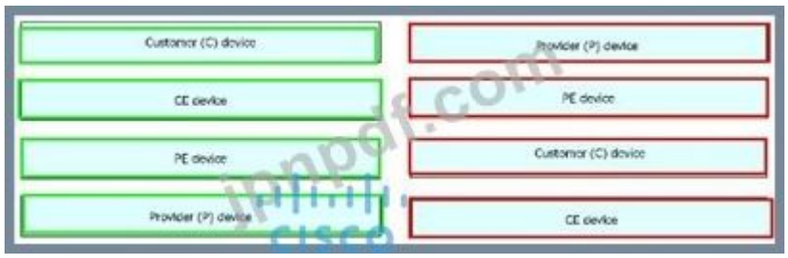
Answer:



参照：
https://www.rogerperkin.co.uk/featured/route-distinguisher-vs-route-target/

最新問題**: 109**
左側の MPLS VPN デバイス タイプを右側の定義にドラッグ アンド ドロップします。

Answer:



最新問題**: 110**

左側のアドレスを右側の適切な IPv6 フィルターの目的にドラッグ アンド ドロップします。

Answer:

説明

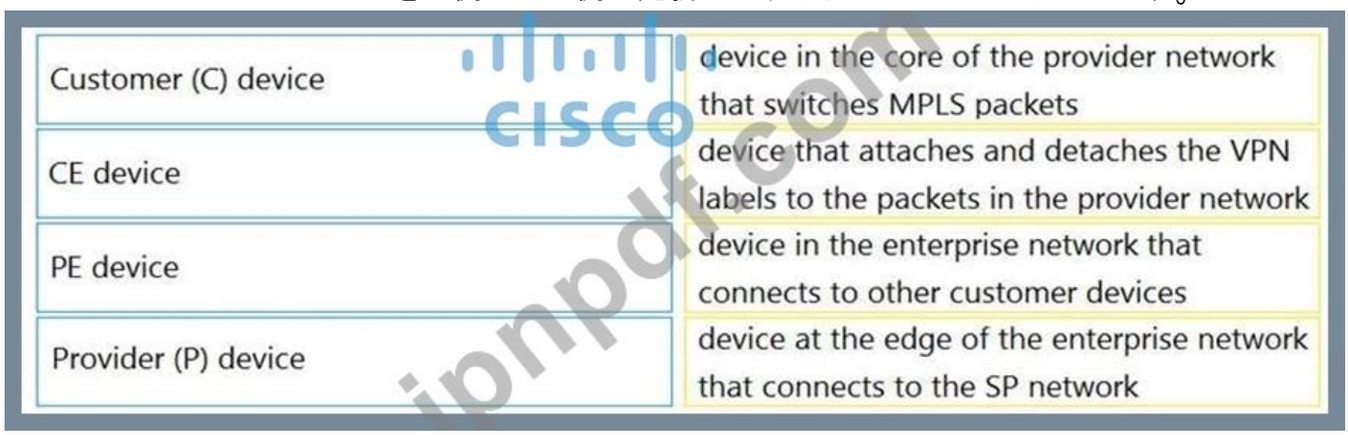
同じ回答が以下ですでに更新されています。

HTTP と HTTPs はそれぞれ TCP ポート 80 と 443 で実行されるため、それらを覚えておく必要があります。

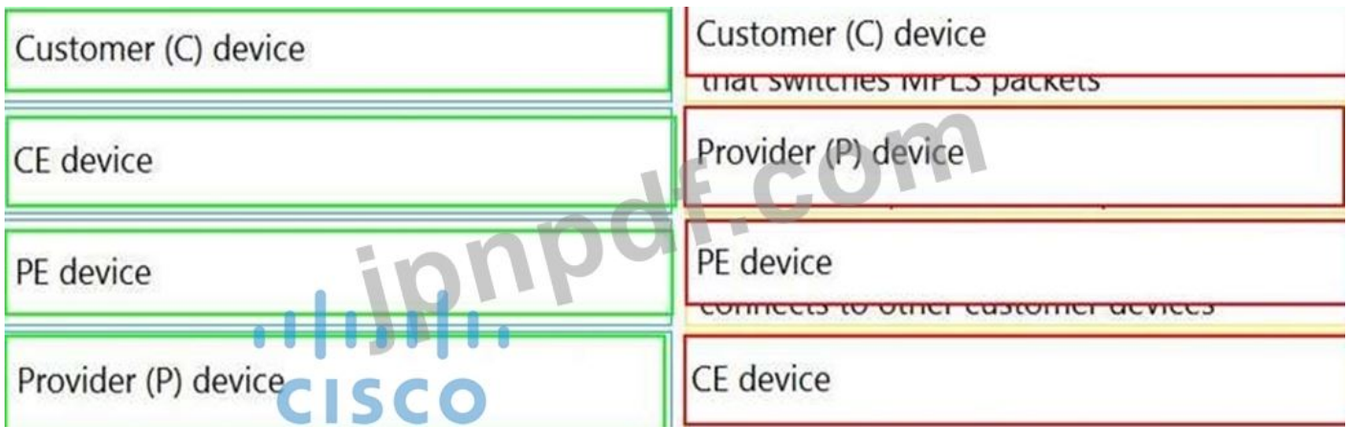
Syslog は UDP ポート 514 で実行され、NTP は UDP ポート 123 で実行されるため、それらを覚えていれば、一致する答えを簡単に見つけることができます。ただし、2001:d88:800:200c::c/126 の範囲は 2001:d88:800:200c:0:0:0:c から 2001:d88:800:200c:0 までであるため、この質問にはタイプミスがある可能性があります。:0:0:f (合計 4 つのホスト)。ホスト 2001:0D88:0800:200c::1f はカバーされません。2001:D88:800:200c::e/126 も同様で、範囲は次のとおりです。
2001:d88:800:200c:0:0:0:c から 2001:d88:800:200c:0:0:0:f はホスト 2001:0D88:0800:200c::1c をカバーしません

。

最新問題: **111**
MPLS VPN デバイス タイプを左側から右側の定義にドラッグ アンド ドロップします。



Answer:



最新問題: **112**
展示を参照してください。

ルーターへの認証試行の失敗を解決するのはどのアクションですか?

A. 回線 vty 0 4 で aaa authorization login コマンドを設定します。

B. ライン コンソール 0 で aaa authorization login コマンドを設定します。

C. aaa 認可コンソールのグローバル コマンドを設定します。

D. ライン vty 0 4 で aaa 認可コンソール コマンドを設定します。

Answer: C (メーッセージを残す**)**

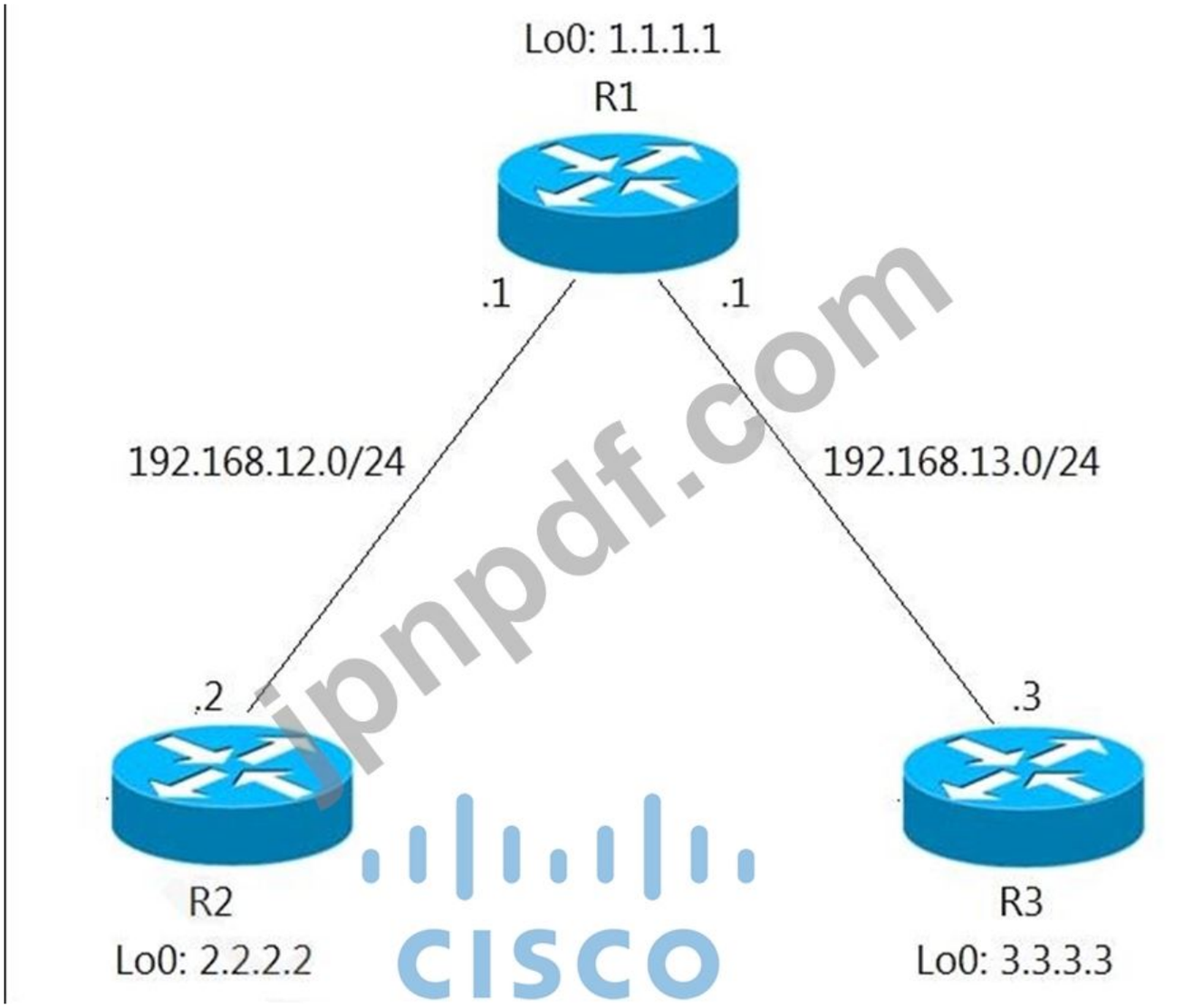
説明

デバッグ出力では、認可 (認証ではなく) が失敗したことがわかります。そのため、認可を修正する必要があります。認証を有効にするには、グローバル コマンドを使用する必要があります。

まずは ‘aaa認証コンソール」。

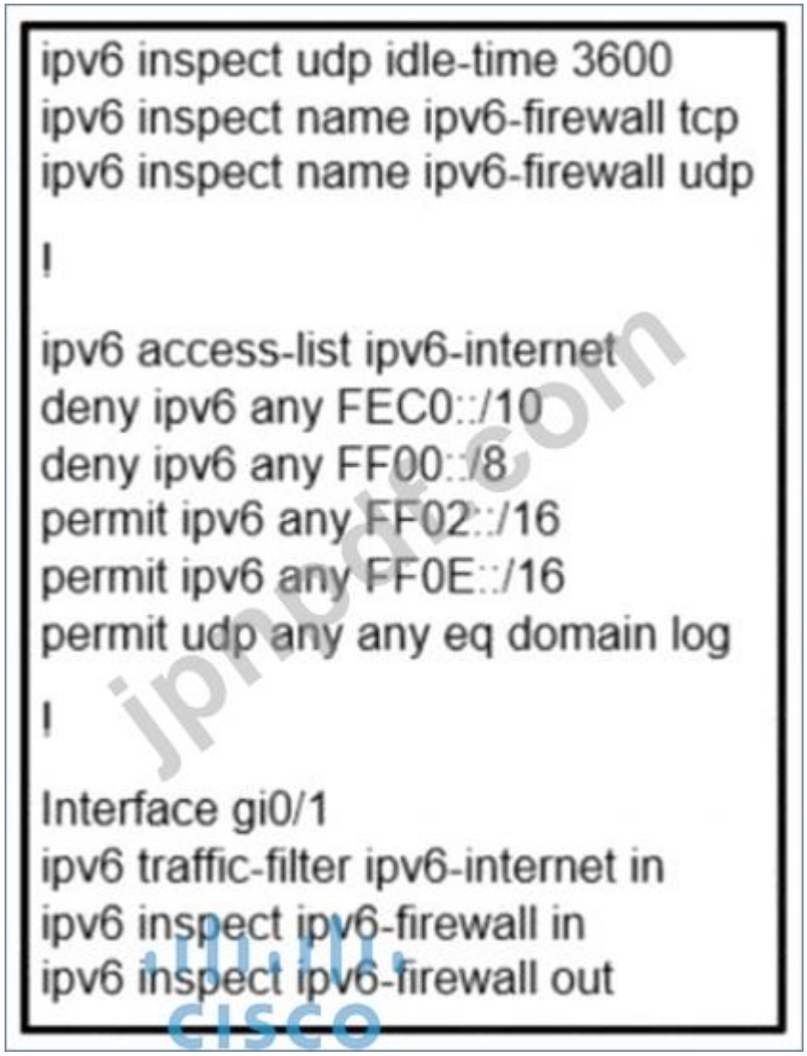
最新問題**: 113**

展示を参照してください。



エンジニアは R1 を EIGRP スタブ ルータとして設定しました。設定後、ルータ R3 は R2 ループバック アドレスに到達できませんでした。
R2 ループバックを R3 ルーティング テーブルにアドバタイズするアクションはどれですか?
A. R2 ループバック アドレスのスタティック ルートを R1 に追加し、それを再配布して R3 にアドバタイズします。
B. 必要なプレフィックスと一致するリーク マップを R1 で使用し、配布リスト コマンドを使用して R3 に適用します。
C. 必要なプレフィックスと一致する R3 上のリーク マップを使用し、EIGRP スタブ機能でそれを適用します。
D. R2 ループバック アドレスのスタティック null ルートを R1 に追加し、それを再配布して R3 にアドバタイズします。
Answer: A (メーッセージを残す**)**

最新問題**: 114**
展示を参照してください。



ネットワーク管理者は、受信アクセス リストを介して IPv6 トラフィックが許可されるように名前解決を設定しました。問題を解決するためにアクセス リストを適用しても、名前解決はまだ機能しません。ネットワーク管理者は名前解決の問題を解決するためにどのような措置を講じますか?

A. アクセス リストに任意の eq ドメイン 53 の任意のログを許可します。

B. グローバル設定の ipv6 検査名 ipv6-firewall udp 53 を検査します。

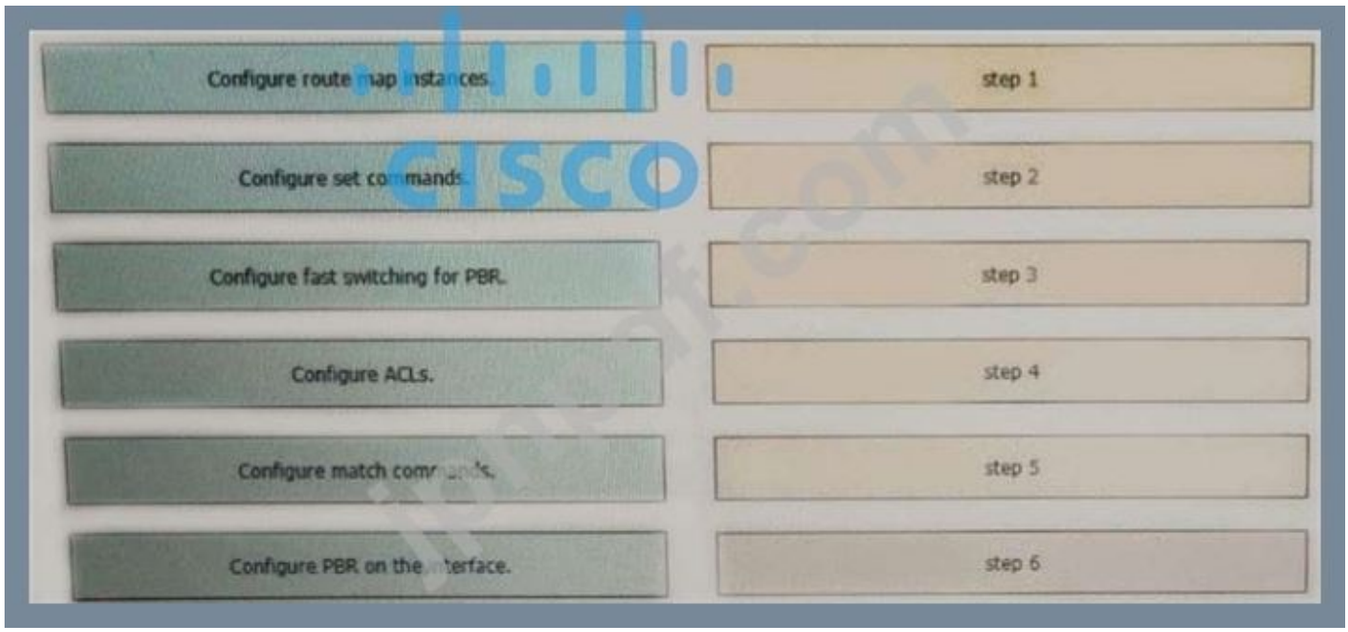
C. インターフェイス gi0/1 から ipv6 Inspection ipv6-firewall を削除します

D. アクセス リストに、permit udp any eq ドメイン any ログを追加します。

Answer: C (メーッセージを残す**)**

最新問題**: 115**

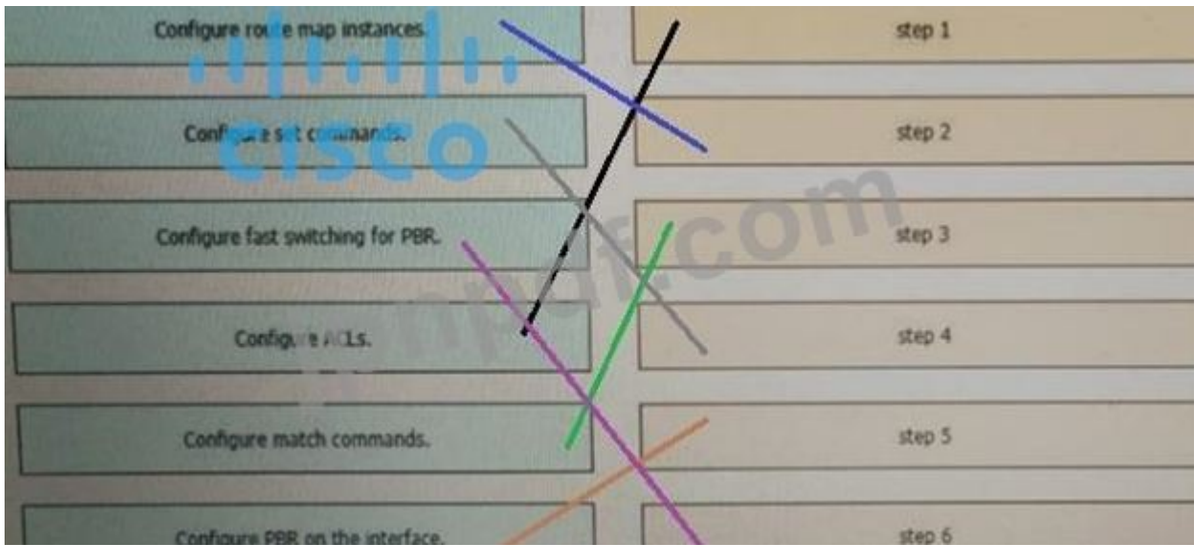
左側のアクションを右側の正しい順序にドラッグ アンド ドロップして、通常のルーティング パスに基づいたパケット転送を回避するポリシーを構成します。


Configure route map instances.
Configure set commands.
Configure fast switching for PBR.
Configure ACLs.
Configure match commands.
Configure PBR on the interface.
step 1
step 2
step 3
step 4
step 5
step 6

Answer:


Configure route map instances.
Configure set commands.
Configure fast switching for PBR.
Configure ACLs.
Configure match commands.
Configure PBR on the interface.
Configure ACLs.
Configure route map instances.
Configure match commands.
Configure set commands.
Configure PBR on the interface.
Configure fast switching for PBR.

説明

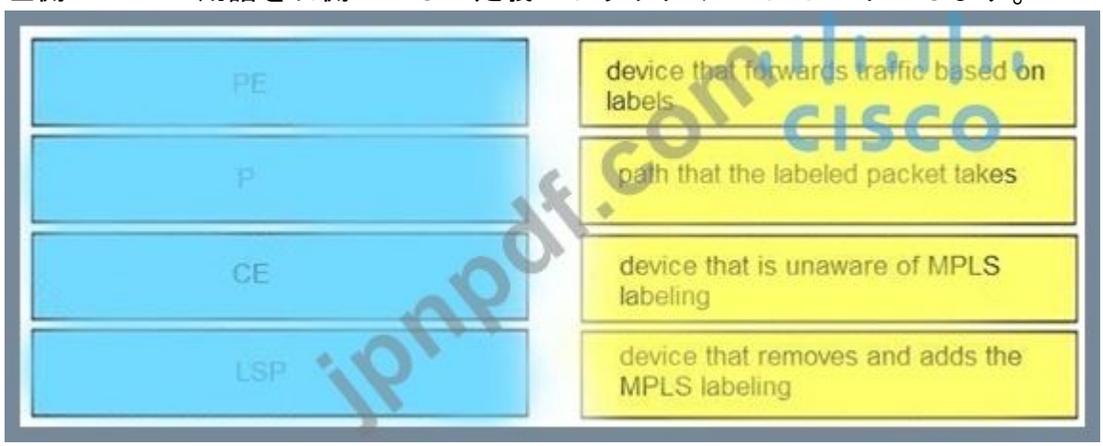

Configure route map instances.
Configure set commands.
Configure fast switching for PBR.
Configure ACLs.
Configure match commands.
Configure PBR on the interface.
step 1
step 2
step 3
step 4
step 5
step 6

https://community.cisco.com/t5/networking-documents/how-to-configure-pbr/ta-p/3122774

最新問題: **116**
展示を参照してください。

エンジニアは CoPP を実装しましたが、OSPF トラフィックが CoPP を通過するのを確認できませんでした。どの構成で問題が解決しますか?
A. ip access-list 拡張 OSPF 許可 ospf any any
B. ポリシーマップ COPP クラス OSFP ポリス 8000 適合アクション送信超過アクション送信違反アクション ドロップ
C. コントロール プレーン サービス ポリシー入力 COPP
D. クラスマップ一致すべて OSFP 一致アクセスグループ名 OSPF
Answer: B (メーッセージを残す**)**

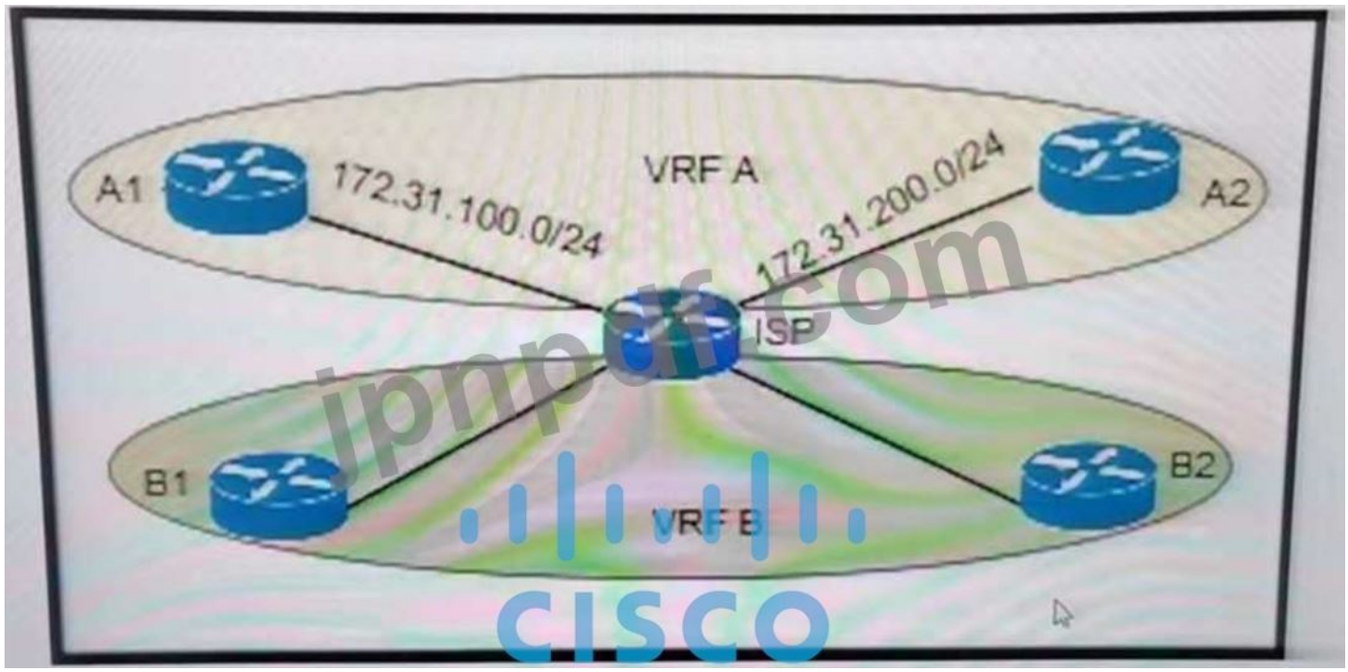
最新問題: **117**
左側の MPLS 用語を右側の正しい定義にドラッグ アンド ドロップします。



Answer:

最新問題: **118**

展示を参照してください。ISP ルータは、VRF-Lite 機能を使用して顧客 A と顧客 B 用に完全に設定されています。顧客 A がルーター A1 と A2 の間で通信するために必要な最小構成は何ですか?



A. A1
インターフェースfa0/0
説明 宛先 -> ISP
ip 追加 172.31.100.1 255.255.255.0
いいえ、閉じません
！
ルーターOSPF100
ネット 172.31.100.1 0.0.0.255 エリア 0
A2
インターフェースfa0/0
説明 宛先 -> ISP
ip 追加 172.31.200.1 255.255.255.0

いいえ、閉じません
！
ルーターOSPF100
ネット 172.31.200.1 0.0.0.255 エリア 0
B. A1
インターフェースfa0/0
説明 宛先 -> ISP
IP VRF フォワーディング A
ip 追加 172.31.100.1 255.255.255.0
いいえ、閉じません
！
ルーターOSPF100
ネット 172.31.100.1 0.0.0.255 エリア 0
A2
インターフェースfa0/0
説明 宛先 -> ISP
IP VRF フォワーディング A
ip 追加 172.31.200.1 255.255.255.0
いいえ、閉じません
！
ルーターOSPF100
ネット 172.31.200.1 0.0.0.255 エリア 0
C. A1
インターフェースfa0/0
説明 宛先 -> ISP
ip 追加 172.31.200.1 255.255.255.0
いいえ、閉じません
！
ルーターOSPF100
ネット 172.31.200.1 0.0.0.255 エリア 0
A2
インターフェースfa0/0
説明 宛先 -> ISP
ip 追加 172.31.100.1 255.255.255.0
いいえ、閉じません
！
ルーターOSPF100
ネット 172.31.100.1 0.0.0.255 エリア 0
D. A1
インターフェースfa0/0

説明 宛先 -> ISP
IP VRF フォワーディング A
ip 追加 172.31.100.1 255.255.255.0
いいえ、閉じません
！
ルーター ospf 100 vrf A
ネット 172.31.200.1 0.0.0.255 エリア 0
A2
インターフェースfa0/0
説明 宛先 -> ISP
IP VRF フォワーディング A
ip 追加 172.31.100.1 255.255.255.0
いいえ、閉じません
！
ルーター ospf 100 vrf A
ネット 172.31.200.1 0.0.0.255 エリア 0
Answer: C (メーッセージを残す**)**
A1 ルータと A2 ルータは、自分たちが VRF A に属していることを認識しません。
ISP の 2 つのインターフェイス (A1 と A2 に接続されている) は次のように構成されている必要があります (1 つのインターフェイスの構成のみを示しています)。
ISPルーター:
インターフェース g0/0
説明 ISP->To_CustomerA
IP VRF フォワーディング A
IPアドレス 172.31.100.2 255.255.255.0
ルーター ospf 100 vrf A
ネットワーク 172.31.200.2 0.0.0.255 エリア 0

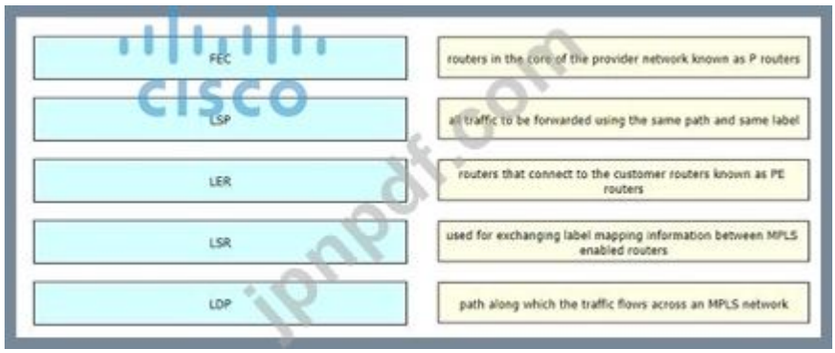
最新問題**: 119**
展示を参照してください。

エンジニアは 192.168.32.100 を 10.1.1.1 経由で転送しようとしましたが、10.1.1.2 経由で転送されました。10.1.1.1 経由でパケットを転送するアクションは何ですか?
A. 管理距離が短い 192.168.32.0 ルートを受信するように EIGRP を設定します。

B. /24 以上のプレフィックスを持つ 192.168.32.0 ルートを受信するように EIGRP を設定します。
C. /19 より長いプレフィックスを持つ 192.168.32.0 ルートを受信するように EIGRP を設定します。
D. より低いメトリックの 192.168.32.0 ルートを受信するように EIGRP を設定します。
Answer: B (メーッセージを残す**)**

最新問題**: 120**
CE ルーティングからの受信パケットに VPN ラベルを付けるルータはどれですか?
A. P ルーター
B. PE ルーター
C. コアルーター
D. CE ルーター
Answer: B (メーッセージを残す**)**

最新問題**: 121**
左側の説明を右側の対応する MPLS コンポーネントにドラッグ アンド ドロップします。

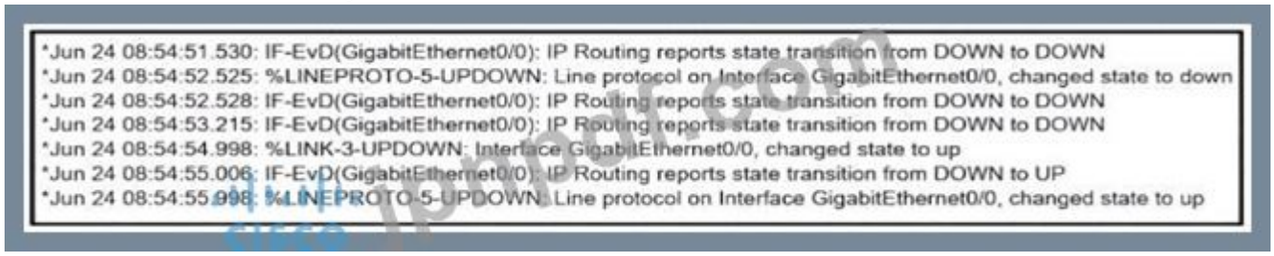


Answer:

最新問題: **122**
ネットワーク管理者は、Cisco Catalyst 6509 スイッチでコンパクト フラッシュ メモリのアップグレードを実行しました。
主要なインターフェイスの帯域幅を監視するように構成された SNMP を除いて、すべてが正常に機能していますが、インターフェイス インデックスは変更されています。どのグローバル構成が問題を解決しますか?
A. SNMP ifindex 永続
B. snmp サーバー ifindex 永続
C. SNMP サーバー ifindex 永続
D. SNMP ifindex 永続
Answer: A (メーッセージを残す**)**

最新問題: **123**
エンジニアは、TFTP を使用して、あるルータから別のルータに IOS ファイルをコピーしようとしています。ファイルのコピーを許可するには、どの 2 つのアクションが必要ですか? (2つお選びください。)
A. TFTP は最近の IOS バージョンではサポートされていないため、別の方法を使用する必要があります。
B. tftp-server flash:<filename> コマンドを使用して、ソース ルータ上の TFTP サーバを有効にします。
C. username tftp passwd tftp コマンドを使用して、ソース ルータでユーザを設定します。
D. tftp-serverauthenticationlocal コマンドを使用して、送信元ルータで TFTP 認証を設定します。
E. copy tftp: flash: コマンドを使用して、ファイルを宛先ルーターにコピーします。
Answer: B,D (メーッセージを残す**)**

最新問題: **124**
展示を参照してください。



R1 は GigabitEthernet0/0 経由で R2 に接続されていますが、R2 は R1 に ping できません。どのようなアクションをとれば問題が解決しますか?
A. ルーターに設定されているルート ダンプニングを修正します。
B. SFP モジュールはサポートされていないため、交換します。
C. インターフェイスで構成された IP イベント ダンプニングを修正します。

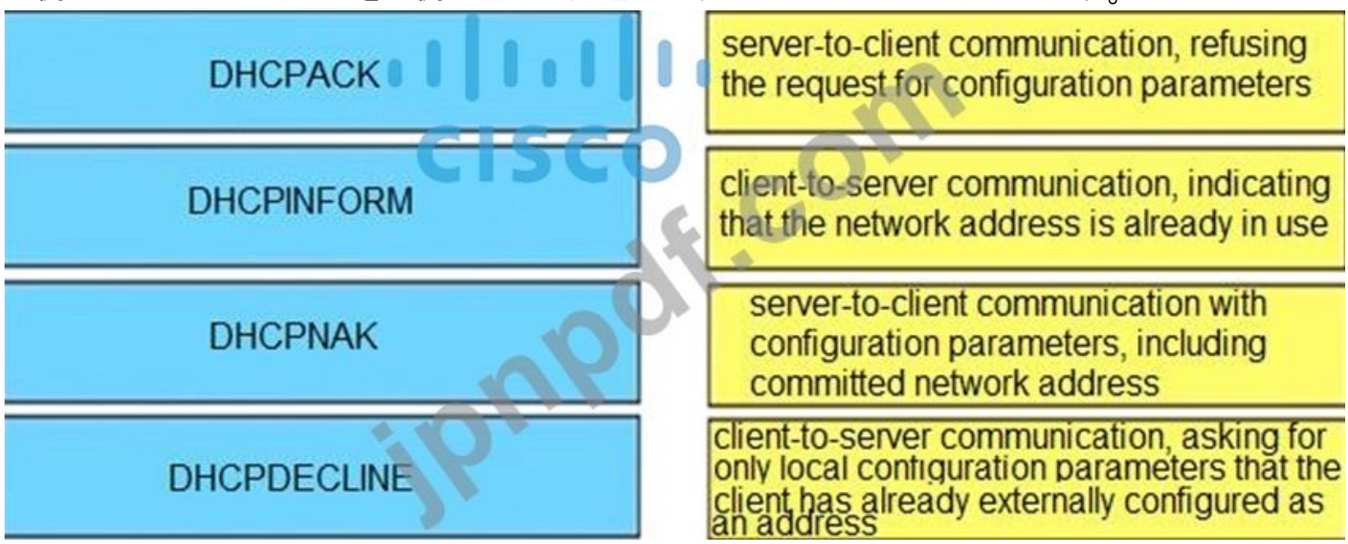
D. 失敗した IP SLA プローブを修正します。

Answer: (解答を表示する**)**

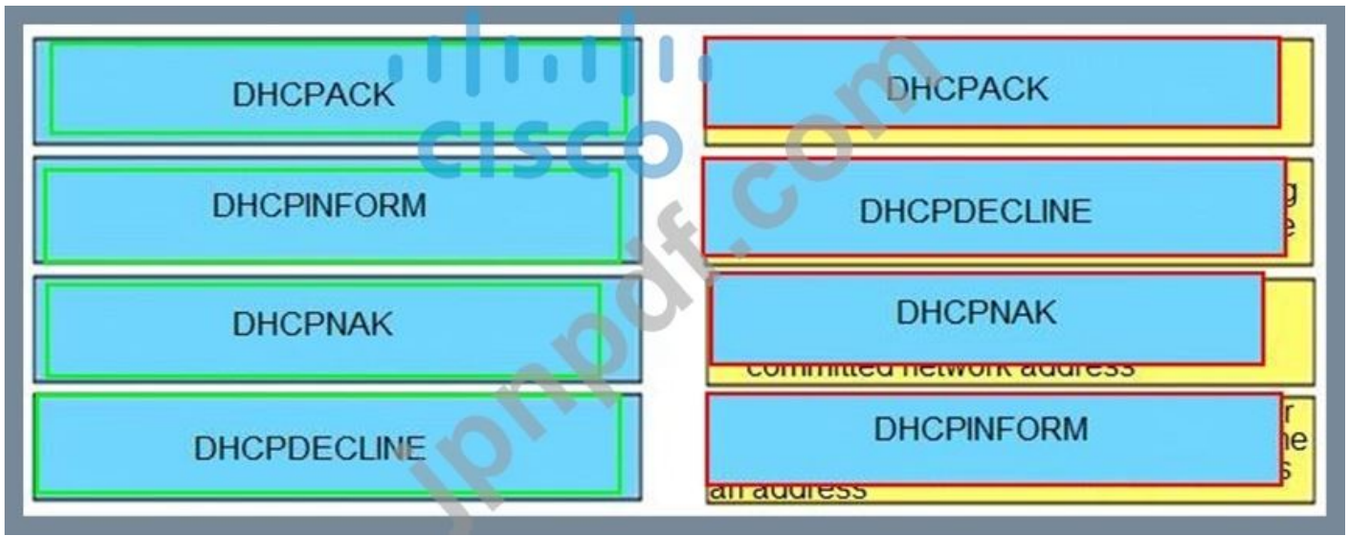
The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping.

最新問題**: 125**

左側の DHCP メッセージを右側の正しい用途にドラッグ アンド ドロップします。



Answer:



参照：

DHCPINFORM: クライアントが他の手段でネットワーク アドレスを取得している場合、または手動で構成された IP アドレスを持っている場合、クライアント ワークステーションは DHCPINFORM 要求メッセージを使用して、ドメイン名やドメイン ネーム サーバー (DNS) などの他のローカル構成パラメータを取得することがあります。。DHCPINFORM メッセージを受信した DHCP サーバーは、新しい IP アドレスを割り当てることなく、クライアントに適切なローカル構成パラメータを使用して DHCPACK メッセージを構築します。この DHCPACK はクライアントにユニキャストで送信されます。

DHCPNAK: 選択したサーバーが DHCPREQUEST メッセージを満たすことができない場合、DHCP サーバーは DHCPNAK メッセージで応答します。クライアントが DHCPNAK メッセージを受信した場合、ま

たは DHCPREQUEST メッセージに対する応答を受信しなかった場合、クライアントは要求状態になって構成プロセスを再開します。クライアントは、初期化状態を再開する前に、60 秒以内に DHCPREQUEST を少なくとも 4 回再送信します。
DHCPACK: DHCP サーバーは DHCPREQUEST を受信した後、DHCPACK メッセージで要求を確認し、初期化プロセスを完了します。
DHCPDECLINE: クライアントは DHCPACK を受信し、オプションでパラメータの最終チェックを実行します。クライアントは、DHCPACK で提供された IP アドレスに対するアドレス解決プロトコル (ARP) 要求を送信することによって、この手順を実行します。クライアントが ARP 要求への応答を受信することによってアドレスがすでに使用されていることを検出した場合、クライアントは DHCPDECLINE メッセージをサーバーに送信し、要求状態になって構成プロセスを再開します。
https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html

最新問題: **126**
エンジニアは、ホップ 10.1.1.1 のルーター上にデフォルトの静的ルートを作成します。エンジニアが検査したところ、ルータに Red と Blue の 2 つの VRF があることがわかりました。ネクスト ホップは両方の VRF で有効であり、割り当てられた各 VRF に存在します。どの構成で接続が実現しますか?

A.
```
ip route vrf BLUE 0.0.0.0 255.255.255.255 10.1.1.1
ip route vrf RED 0.0.0.0 255.255.255.255 10.1.1.1
```

B.
```
ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

C.
```
ip route vrf Red 0.0.0.0 0.0.0.0 10.1.1.1
ip route vrf Blue 0.0.0.0 0.0.0.0 10.1.1.1
```

D.
```
ip route vrf Red 0.0.0.0 255.255.255.255 10.1.1.1
ip route vrf Blue 0.0.0.0 255.255.255.255 10.1.1.1
```

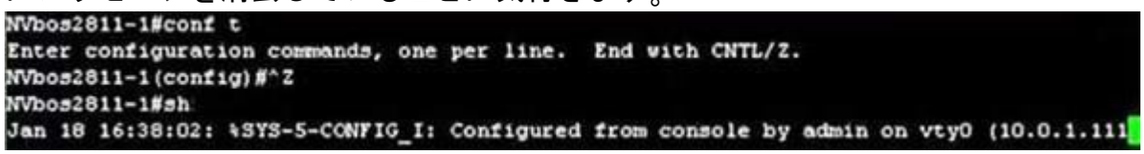
Answer: (解答を表示する**)**

最新問題: **127**
展示を参照してください。R1 と R2 は EIGRP 隣接関係を確立できません。EIGRP 隣接関係を確立するアクションはどれですか?
A. いずれかのルーターの現在の自律システム番号を削除し、別の値に変更します。
B. R2 設定と一致するように、passive-interface コマンドを R1 設定に追加します。
C. R1 設定と一致するように、no auto-summary コマンドを R2 設定に追加します。
D. R1 設定と一致するように、R2 設定からpassive-interface コマンドを削除します。
Answer: C (メーッセージを残す**)**

最新問題: **128**
ネットワーク エンジニアは、NTP サーバーと同期しているコア スイッチ上のフラッピング (アップ/ダウン) インターフェイスの問題を調査しています。ログ出力にはフラップの時間は表示されません。
デバイスの時計に従ってフラップの時間をスイッチ上で許可するコマンドはどれですか?
A. 時計カレンダー有効
B. サービスのタイムスタンプ ログの稼働時間
C. サービス timtstamps ログ datetime localtime show-timezone

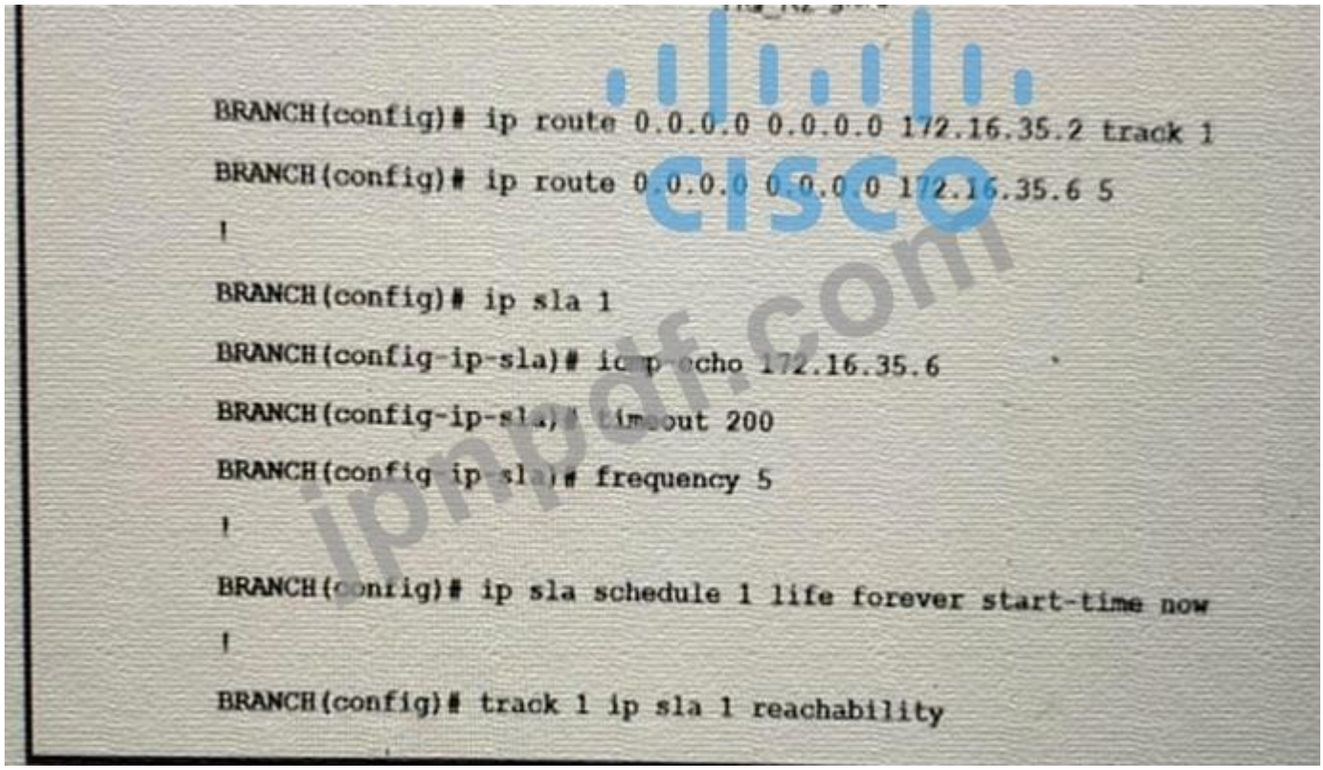
D. クロック サマータイム MST 繰り返し 3 月 2 日 2:00 11 月 1 日 2:00
Answer: C (メーッセージを残す**)**

最新問題**: 129**
エンジニアはルータのコンソール セッションでトラブルシューティングを行っており、複数のデバッグ コマンドを有効にしています。コンソール画面にはスクロールするデバッグ メッセージが表示され、どのコマンドも正しく入力されたかどうかを確認できず、出力も表示されません。エンジニアがデバッグ メッセージの分析を続行しながら、入力されたコンソール コマンドを確認できるようにするアクションはどれですか?
A. ロギング同期コマンドを構成します。
B. nologging コンソール デバッグ コマンドをグローバルに設定します。
C. ロギング同期レベル all コマンドを設定します。
D. no mon コマンドをグローバルに設定します。
Answer: A (メーッセージを残す**)**
説明
「ロギング同期」コマンドが入力コマンドにどのような影響を与えるかを見てみましょう。
このコマンドを使用しないと、メッセージがポップアップ表示され、そのメッセージが長すぎると何を入力したか分からなくなる可能性があります。コマンドを消去 (バックスペース) しようとすると、代わりにメッセージを消去していることに気付きます。



このコマンドを有効にすると、メッセージがポップアップ表示されると、新しい行にコマンドを入力することになります。

最新問題**: 130**
別紙を参照してください。



ブランチ ネットワークからのトラフィックは、パスが使用できない場合を除き、本社 R1 を経由してルーティングされる必要があります。エンジニアは、HQ_R1 ルーターに向かう BRANCH ルーターのインターフェイスをシャットダウンして、この機能をテストします。
192.168.20.0/24 はブランチ ルーターから到達できなくなりました。どの構成セットが問題を解決しますか?

A. HQ_R1(config)# ip sla レスポンダー
HQ_R1(config)# ip sla レスポンダー icmp-echo 172.16.35.2
B. BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.1
C. HQ_R2(config)# ip sla レスポンダー
HQ_R2(config)# ip sla レスポンダー icmp-echo 172.16.35.5
D. BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.2

Answer: D (メーッセージを残す)

説明
上記の設定では、エンジニアはメイン パス (172.16.35.2) を追跡する代わりに 172.16.35.6 (バックアップ パス) を追跡していたため、間違いを犯しました。したがって、彼がメイン パスをシャットダウンしたとき、トラック 1 はまだ稼動していたので、トラフィックは引き続きメイン パスを通過し、失敗しました。
この問題を解決するには、メイン パスのトラッキング インターフェイスを修正するだけです。

最新問題: **131**
展示を参照してください。

ネイバー関係が確立されていません 隣接関係が確立される 2 つの設定はどれですか? (2つお選びください)

A. LA
インターフェイス E 0/0
ip ospf 認証キー Cisco123

B. ニューヨーク
ルーターOSPF1
エリア 0 認証メッセージ ダイジェスト

C. ニューヨーク
インターフェイス E 0/0
no ip ospf メッセージ ダイジェスト キー 1 md5 Cisco123
ip ospf 認証キー Cisco123

D. LA
インターフェイス E 0/0
ip ospf メッセージ ダイジェスト キー 1 md5 Cisco123

E. LA
ルーターOSPF1
エリア 0 認証メッセージ ダイジェスト

Answer: (解答を表示する**)**

最新問題: **132**
展示を参照してください。

```
Router#show ip bgp vpnv4 rd 1100:1001 10.30.116.0/23
BGP routing table entry for 1100:1001:10.30.116.0/23, version 26765275
Paths: (9 available, best #6, no table)
 Advertised to update-groups:
   1    2      3
 (65001 64955 65003) 65089, (Received from a RR-dient)
       172.16.254.226 (metric 20645) from 172.16.224.236 (172.16.224.236)
       Origin IGP. metric 0, localpref 100, valid, confed-internal
       Extended Community: RT:1100:1001
       mpls labels in/out nolabel/362
 (65008 64955 65003) 65089
       172.16.254.226 (metric 20645) from 10.131.123.71 (10.131.123.71)
       Origin IGP, metric 0, localpref 100, valid, confed-external
       Extended Community: RT:1100:1001
       mpls labels in/out nolabel/362
 (65001 64955 65003) 65089
       172.16.254.226 (metric 20645) from 172.16.216.253 (172.16.216.253)
       Origin IGP, metric 0, localpref 100, valid, confed-external
       Extended Community: RT:1100:1001
       mpls labels in/out nolabel/362
 (65001 64955 65003) 65089
       172.16.254.226 (metric 20645) from 172.16.216.252 (172.16.216.252)
       Origin IGP, metric 0, localpref 100, valid, confed-external
       Extended Community: RT:1100:1001
       mpls labels in/out nolabel/362
 (64955 65003) 65089
       172.16.254.226   (metric 20645) from 10.77.255.57 (10.77.255.57)
       Origin IGP, metric 0, localpref 100, valid, confed-external
       Extended Community RT:1100:1001
       mpls labels in/out nolabel/362
 (64955 65003) 65089
       172.16.254.226 (metric 20645) from 10.57.255.11 (10.57.255.11)
       Origin IGP, metric 0, localpref 100, valid, confed-external, best
       Extended Community RT:1100:1001
       mpls labels in/out nolabel/362

 (64955 65003) 65089
  172.16.254.226 (metric 20645) from 172.16.224.253 (172.16.224.253)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community RT:1100:1001
  mpls labels in/out nolabel/362
 (65003) 65089
  172.16.254.226 (metric 20645) from 172.16.254.234 (172.16.254.234)
```

```
Origin IGP, metric 0, localpref 100, valid, confed-external
    Extended Community RT:1100:1001
    mpls labels in/out nolabel/362
65089, (Received from a RR-client)
 172.16.228.226 (metric 20645) from 172.16.228.226 (172.16.228.226)
 Origin IGP, metric 0, localpref 100, valid, confed-external
    Extended Community RT:1100:1001
    mpls labels in/out nolabel/278
```

エンジニアは BGP を設定し、現在の最適パスではなく 10.77.255.57 からのパスを最適パスとして選択したいと考えています。どのアクションで問題が解決しますか?

A. 現在の最適なパスの先頭に AS_PATH を追加するように構成します。

B. 最適なパスとして選択するようにより高い MED を構成します

C. 必要な最適パスの先頭に AS_PATH を設定します。

D. 最適なパスとして選択するように下位の LOCAL_PREF を構成します

Answer: (解答を表示する**)**

説明

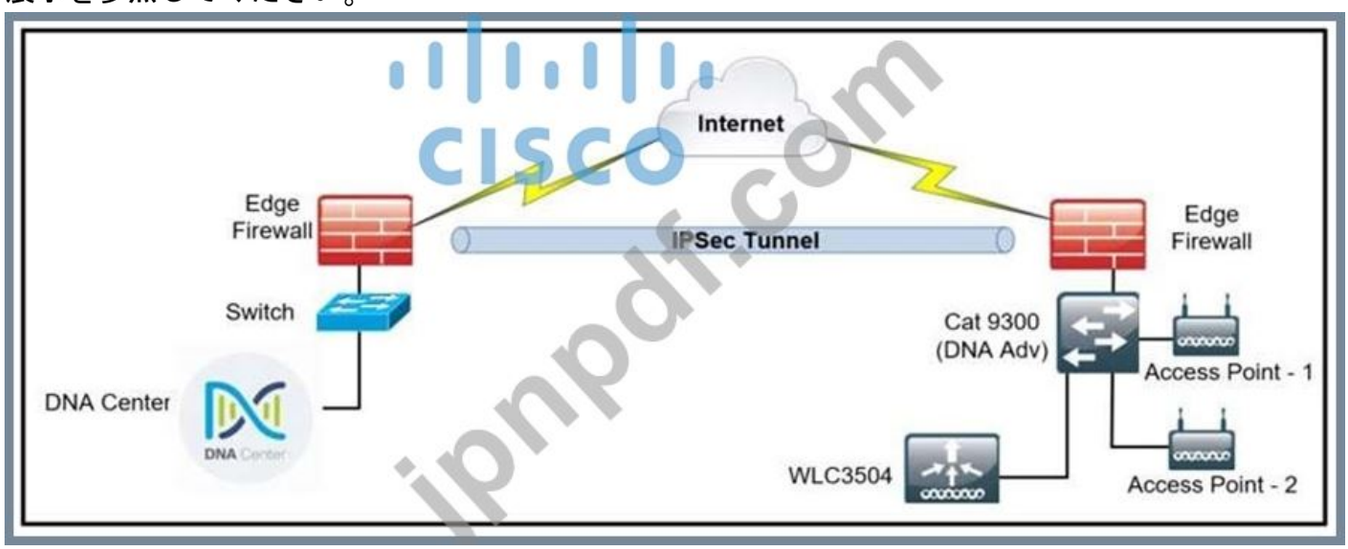
出力から、現在の最適なパスは 10.57.255.11 (「..valid、confed-external、best」を含む) からであり、このパスは 2 AS 離れている (64955 65003) ことがわかります。AS が 1 つしか離れていないパスがいくつかありますが (たとえば、172.16.254.234 からのパス)、それらは最適なパスとして選択されなかったため、最適なパスの決定に AS_PATH は使用されませんでした -> 回答 A と回答 C は正しくありません。

出力内のすべてのパスのメトリックは 0 であり、これがこの属性の最低 (最適) 値です。より高い MED を設定すると、他のパスよりも優先度が低くなります -> 回答 B は不正解です。

答え D だけが残っていますが、LOCAL_PREF 属性を優先するにはより高い値を設定する必要があるため、ここでの 「LOCAL_PREF が低い」ということはより高い値を意味すると考えられます。しかし、これが最良の答えです。

最新問題**: 133**

展示を参照してください。



ネットワーク管理者は、Cisco DNA Center で Cisco Catalyst 9300 と Cisco WLC 3504 を検出しています。Catalyst 9300 は正常に追加されましたが、管理者が Cisco DNA Center に追加しようとすると、WLC に "エラー 連絡不能」が表示されます。Cisco DNA Center で WLC を正常に検出するアクションはどれですか?

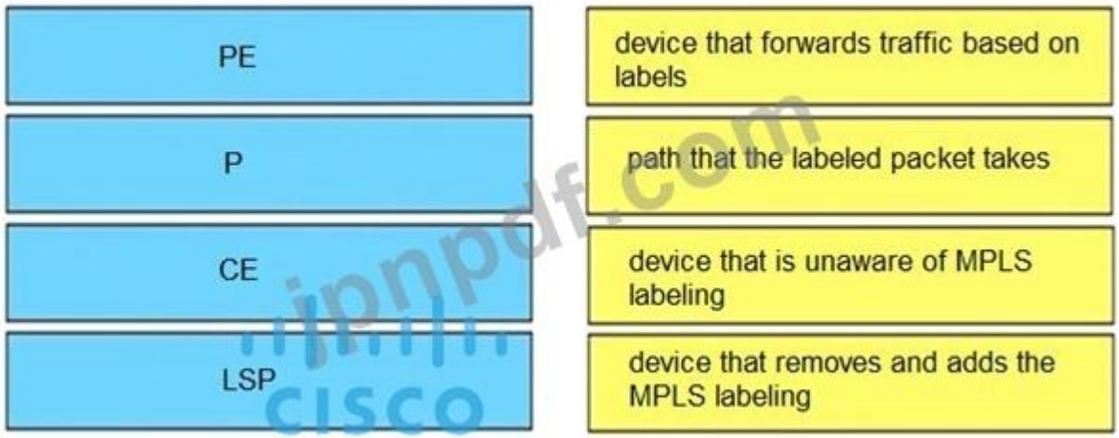
A. USB 上の Cisco DNA Center から .cert ファイルをコピーし、WLC 3504 にアップロードします。
B. USB 上の Cisco DNA Center から .pern ファイルをコピーし、WLC 3504 にアップロードします。
C. Catalyst 9300 接続デバイスの階層の下に WLC 3504 を追加します。
D. Cisco DNA Center から WLC 3504 を削除し、Cisco DNA Center に再度追加します。
Answer: (解答を表示する**)**

最新問題: **134**
展示を参照してください。

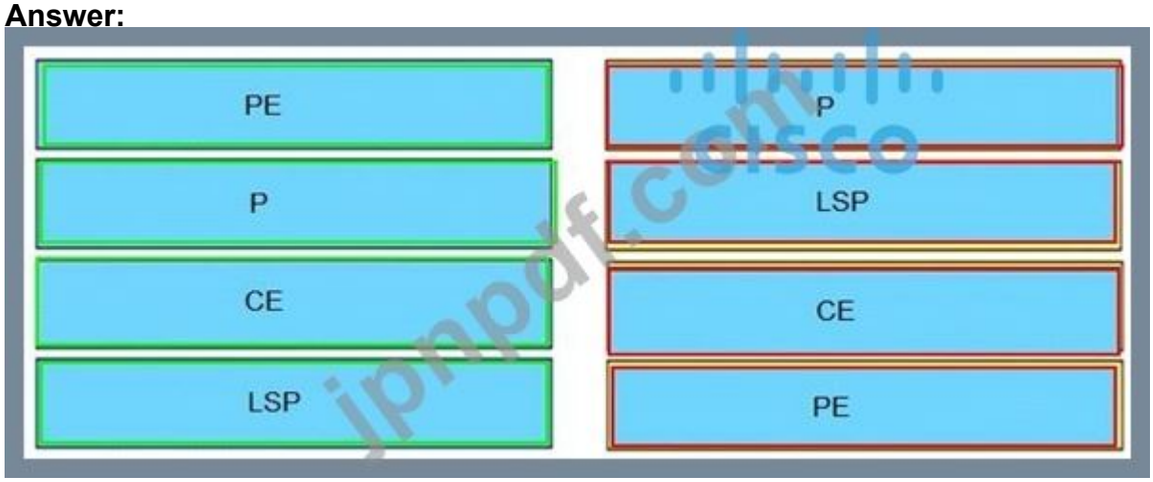
エンジニアは、ルーター設定に表示されるべきではない、暗号化されたユーザー パスワードを追加しようとしています。
問題を解決する 2 つの構成コマンドはどれですか? (2つお選びください)

A. サービスのパスワード暗号化
B. サービスパスワード暗号化なし
C. ユーザ名 管理者秘密 Cisco@maedeh motamedi
D. ユーザ名 管理者パスワード Cisco@maedeh motamedi
E. ユーザ名 管理者パスワード 5 Cisco@maedeh motamedi
F. パスワード暗号化 aes
Answer: A,C (メーッセージを残す**)**

最新問題: **135**
左側の MPLS 用語を右側の正しい定義にドラッグ アンド ドロップします。



Answer:



最新問題**: 136**

VPN ルーティング情報は MPLS ネットワーク内でどのように配布されますか?

A. 顧客データ パケットの最上位は、正しい CE デバイスに送信します。

B. VPN IPsec ピアを使用して確立されます。

C. VPN ターゲット コミュニティを使用して制御されます。

D. RD を使用して制御されます。

Answer: C (メーッセージを残す**)**

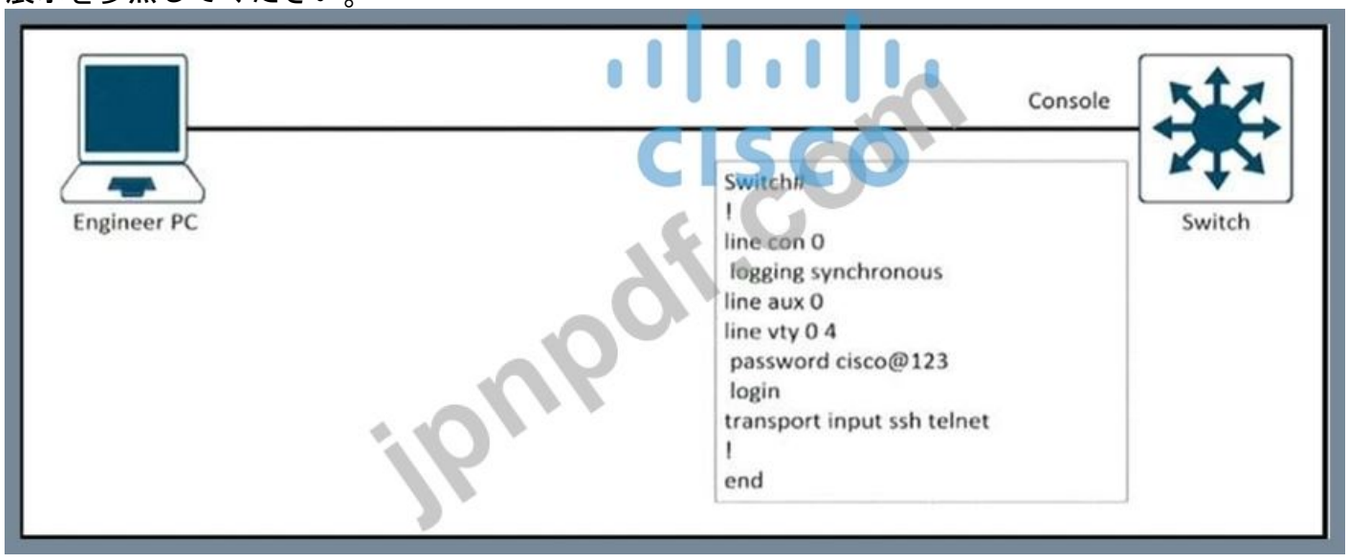
説明

仮想プライベート ネットワーク (VPN) ルーティング情報の配布は、ボーダー ゲートウェイ プロトコル (BGP) 拡張コミュニティによって実装される VPN ルート ターゲット コミュニティを使用して制御されます。

参照：

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/mp

最新問題: **137**
展示を参照してください。



エンジニアは、最近の企業セキュリティ ポリシーに基づいて、すべての企業リモート Cisco デバイスのコンソール ポートへのアクセスをブロックする必要がありますが、セキュリティ チームはコンソール ポート経由で接続できます。コンソール ポートのどの設定で問題が解決しますか?

A. トランスポート入力 Telnet
B. ログイン名とパスワード
C. 実行なし
D. 実行 0.0

Answer: C (メーッセージを残す**)**

説明

「no exec」は回線へのアクセスを無効にします。これは、発信セッションのみを許可する (着信セッションを無効にする) 場合に使用されるため、このコマンドはすべてのコンソール ポート アクセスをブロックします。

「exec 0 0」コマンドはありません。「execプロンプト」コマンドはIOSバージョンでのみ見つかります。15.4(2)T4。

最も類似したコマンドは「exec-timeout 0 0」コマンドで、Telnet/SSH セッションのタイムアウトを防ぐために使用されます。

最新問題: **138**

展示を参照してください。組織は管理プレーン保護を実装しました。GigabitEthernet0/3 に追加できる 2 つの管理プロトコルはどれですか? (2つお選びください。)

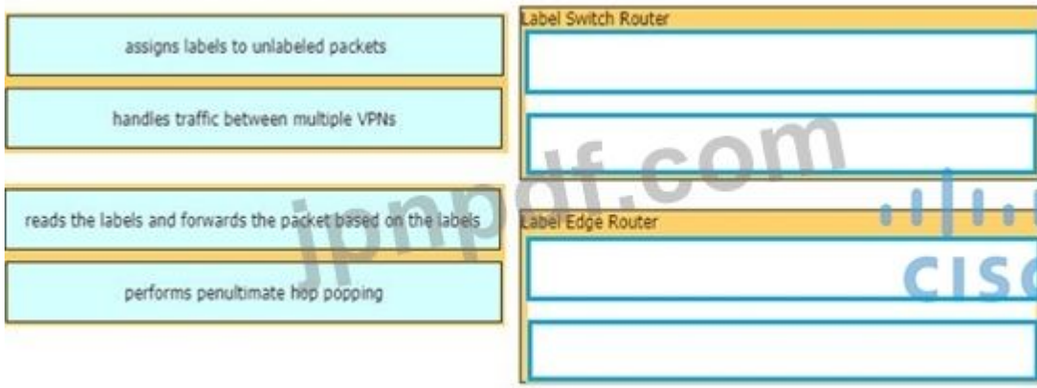
```
RouterA:
interface GigabitEthernet0/2
ip address 10.10.20.2 255.255.255.0
!
interface GigabitEthernet0/3
ip address 10.10.30.2 255.255.255.0
!

RouterA#show management-interface
Management interface GigabitEthernet0/2
          Protocol              Packets processed
          http                  0
          https                 10

Management interface GigabitEthernet0/3
          Protocol              Packets processed
          http                  0
          ssh                   10
          snmp                  1200

RouterB#ssh -l cisco 10.10.20.2
% Destination unreachable; gateway or host down
```

A. SCP
B. TFTP
C. CDP
D. Telnet
E. SMTP

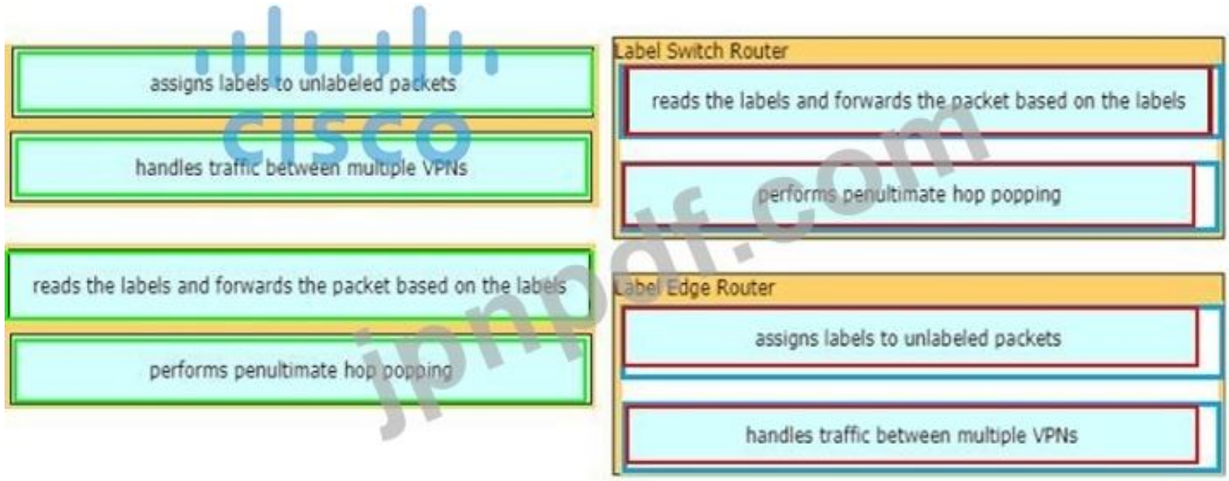
Answer: B,D (メーッセージを残す)
説明/参照:
https://www.cisco.com/c/en/us/td/docs/ios/security/configuration/guide/sec_mgmt_plane_prot.html

最新問題: **139**
DHCPv6 ガードの目的は何ですか?
A. DHCPv6 サーバーと DHCPv6 クライアント (またはリレー エージェント) の間でメッセージを送信します。
B. DHCPv5 サーバーのクライアントが影響を受けることを示します。
C. リレー エージェントから DHCPv6 サーバーへの DHCPv6 メッセージをブロックします。
D. (ルージュ) DHCPv6 サーバーからの DHCPv6 リプレイとアドバタイズメントを許可します。
Answer: (解答を表示する)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6fxe-16-book/ip6-dhcpv6-guard.html

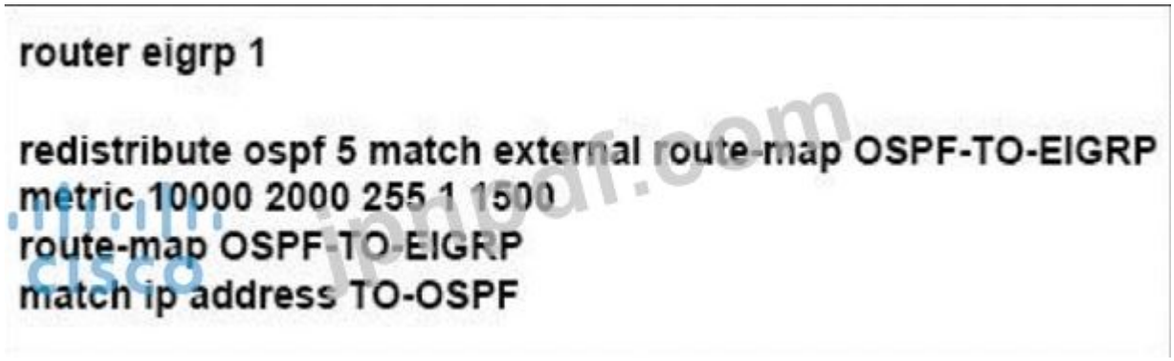
最新問題: **140**
左側の操作を、右側の操作が実行される場所にドラッグ アンド ドロップします。



Answer:



最新問題: **141**
展示を参照してください。



OSPF プロセス 5 からのどのルートが EIGRP に再配布されますか?

A. アクセス リスト TO-OSPF に一致する E1 および E2 サブネット

B. アクセス リスト TO-OSPF に一致する E2 サブネットのみ

C. プレフィックス リスト TO-OSPF に一致する E1 および E2 サブネット

D. プレフィックス listTO-OS1 に一致する E1 サブネットのみ

Answer: (解答を表示する**)**

最新問題**: 142**

ネットワーク エンジニアは、NTP サーバーと同期しているコア スイッチ上のフラッピング (アップ/ダウン) インターフェイスの問題を調査しています。現在、ログ出力にはフラップの時間は表示されません。スイッチのロギングで、デバイスの時計に応じたフラップの時間を表示できるコマンドはどれですか?

A. サービスのタイムスタンプ ログの稼働時間

B. クロック サマータイム MST 繰り返し 3 月 2 日 2:00 11 月 1 日 2:00

C. サービス タイムスタンプ ログ datetime localtime show-timezone

D. 時計カレンダー有効

Answer: (解答を表示する**)**

セクション: インフラストラクチャ サービス

最新問題**: 143**

展示を参照してください。

リモート NetFlow サーバーが NetFlow データの受信に失敗するのはなぜですか?

A. フロー エクスポーターは構成されていますが、使用されていません。

B. フロー モニターが間違った方向に適用されています。

C. フロー エクスポーターの宛先に到達できません。

D. フロー モニタが間違ったインターフェイスに適用されています。

Answer: A (メーッセージを残す**)**

最新問題**: 144**

IP/VPN ハブ アンド スポーク展開シナリオで AS_PATH 防止メカニズムを回避するには、ネットワーク エンジニアは何を構成する必要がありますか?

A. すべての Pe で allowed in および as-override を使用します。

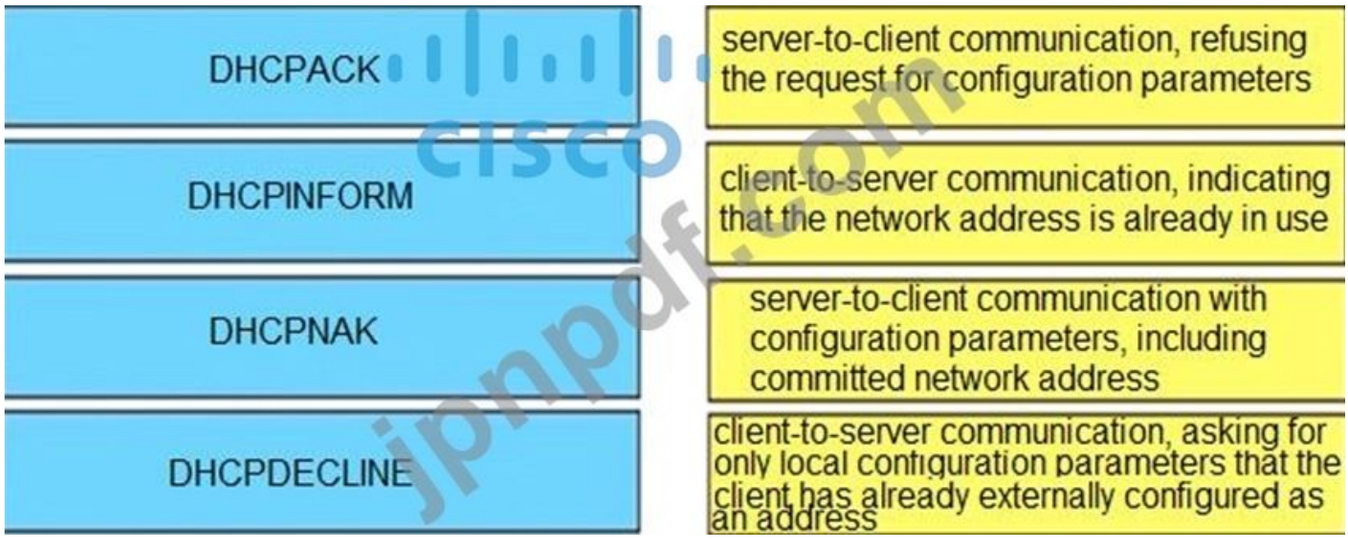
B. PE_Hub で as-override を使用します。
C. PE_Hub でAllowas-を使用する
D. PE ハブで、allowas in および as-override を使用します。
Answer: B (メッセージを残す**)**

最新問題**: 145**
展示を参照してください。

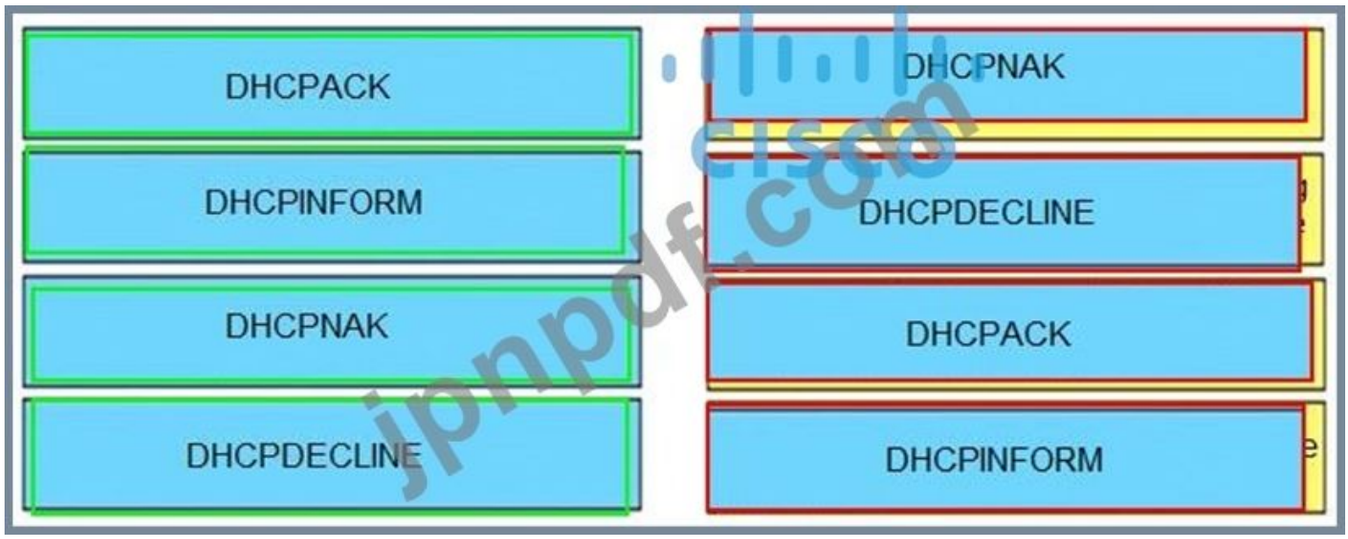
```
R1#show running-config | section dhcp
ip dhcp excluded-address 192.168.1.1 192.168.1.49
ip dhcp pool DHCP
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   dns-server 8.8.8.8
   lease 0 12
```

DHCP サーバーから IP アドレスを取得できないとユーザーから報告されています。DHCP サーバーは次のように構成されています。合計約 300 人の非同時ユーザーがこの DHCP サーバーを使用していますが、1 日あたり 2 時間を超えてアクティブになっているユーザーは一人もいません。現在のリソース内で問題を解決するアクションはどれですか?
A. DHCP プール内のネットワーク 192.168.1.0 255.255.254.0 コマンドにサブネット マスクを変更します。
B. network 192.168.2.0 255.255.255.0 コマンドを DHCP プールに追加します
C. DHCP リース時間をより小さい値に構成します
D. DHCP リース時間をより大きな値に設定します。
Answer: (解答を表示する**)**

最新問題**: 146**
左側の DHCP メッセージを右側の正しい用途にドラッグ アンド ドロップします。



Answer:



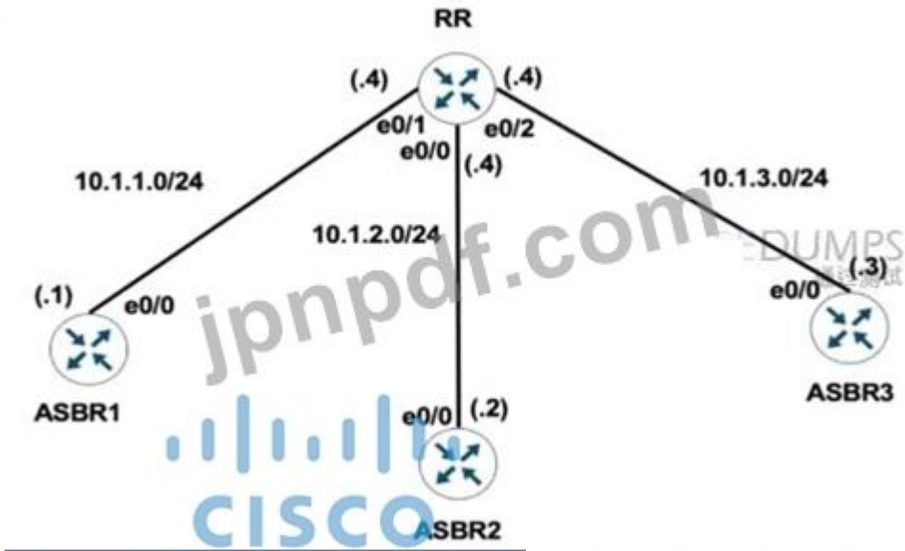
最新問題: **147**
展示を参照してください。

エンジニアは、R1 のコンソールに接続されたシリアル インターフェイスから別のルータの m バンドにアクセスしようとすると、このエラー メッセージを受け取ります。この問題を解決するには、R1 でどの構成が必要ですか?

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: D (メーッセージを残す**)**
https://community.cisco.com/t5/other-network-architecture/out-of-band-router-access/td-p/333295
「transport Output none」コマンドは、R1 から行われるプロトコル接続を禁止します。
したがって、192.168.12.2 への SSH 接続は拒否されました。この問題を解決するには、R1 の 「ライン コンソール 0」で 「トランスポート出力 ssh」を設定します。
注: パラメータ 「」は、リモート マシンにログインするためのユーザー名を指定します。

最新問題**: 148**
ネットワーク エンジニアは、NTP サーバーと同期しているコア スイッチ上のフラッピング (アップ/ダウン) インターフェイスの問題を調査しています。現在、ログ出力にはフラップの時間は表示されません。スイッチのロギングで、デバイスの時計に応じたフラップの時間を表示できるコマンドはどれですか?
A. 時計カレンダー有効
B. クロック サマータイム MST 繰り返し 3 月 2 日 2:00 11 月 1 日 2:00
C. サービス タイムスタンプ ログ datetime localtime show-timezone
D. サービスのタイムスタンプ ログの稼働時間
Answer: C (メーッセージを残す**)**

最新問題**: 149**
展示を参照してください。




```
RR Configuration:

router bgp 100
 neighbor IBGP peer-group
 neighbor IBGP route-reflector-client
 neighbor 10.1.1.1 remote-as 100
 neighbor 10.1.2.2 remote-as 100
 neighbor 10.1.3.3 remote-as 100
```

ネットワーク管理者は、すべてのデバイス間の接続を確立するようにネットワークを構成しましたが、ASBR に相互のルートがないことに気付きました。この問題を解決できる構成セットはどれですか?

```
router bgp 100
 neighbor 10.1.1.1 next-hop-self
 neighbor 10.1.2.2 next-hop-self
 neighbor 10.1.3.3 next-hop-self

router bgp 100
 neighbor IBGP update-source Loopback0

router bgp 100
 neighbor IBGP next-hop-self

router bgp 100
 neighbor 10.1.1.1 peer-group IBGP
 neighbor 10.1.2.2 peer-group IBGP
 neighbor 10.1.3.3 peer-group IBGP
```

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: B (メーッセージを残す**)**

最新問題**: 150**
ネットワーク管理者は、ポリシングされる OSPF トラフィックを 1 Mbps に制限するように、コントロール プレーン ポリシング用のルータを設定しました。この制限を超えるトラフィックも、この時点でトラ

フィック分析のために許可する必要があります。ルーターの構成は次のとおりです。
アクセス リスト 100 許可 ospf any any
！
クラスマップ CM-OSPF
アクセスグループ 100 に一致
！
ポリシーマップ PM-COPP
クラスCM-OSPF
警察 1000000 適合アクション送信
！
コントロールプレーン
サービス ポリシー出力 PM-COPP
コントロール プレーン ポリシングは、OSPF トラフィックの監視とポリシングに失敗しました。この問題はどの構成で解決されますか?

```
access-list 100 permit tcp any any eq 179
access-list 100 permit ospf any any
access-list 101 permit tcp any any range 22 23
!
!
class-map CM-MGMT
 no match access-group 100
 match access-group 101
!
control-plane
 no service-policy output PM-COPP
 service-policy input PM-COPP
```

```
No access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit tcp any any range eq 22
access-list 100 permit tcp any any range eq 23
access-list 100 permit ospf any any

control-plane
 no service-policy output PM-COPP
 service-policy input PM-COPP
```

```
no access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit ospf any any
access-list 101 permit tcp any any range 22 23
!
!
class-map CM-MGMT
 no match access-group 100
```

A. オプション D
B. オプション C
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**: 151**

エンジニアは、EIGRP ルートを要約し、特にループバックをアドバタイズするように Leak-map コマンドを設定しました
0、IP 10.1.1.1.255.255.255.252、サマリー ルート。設定を完了した後、顧客から、特定のループバック アドレスを持つ要約ルートを受信できないという苦情が寄せられました。どの 2 つの構成が問題を解決しますか? (2つお選びください。)

A. アクセス リスト 1 の許可 10.1.1.0.0.0.0.3 を設定します。
B. アクセス リスト 1 の許可 10.1.1.1.0.0.0.252 を設定します。
C. アクセス リスト 1 を設定し、ルート マップ Leak-Route で照合します。
D. ルート マップ リーク ルート許可 10 を設定し、アクセス リスト 1 と一致します。
E. ルートマップのリークルート許可 20 を設定します。
Answer: A,D (メーッセージを残す**)**
説明
EIGRP サマリー ルートを設定すると、サマリーの範囲内にあるすべてのネットワークが抑制され、インターフェイス上でアドバタイズされなくなります。サマリールートのみが広告されます。ただし、サマリー ルートとともに抑制されているネットワークをアドバタイズしたい場合は、リーク マップ機能を使用できます。以下のコマンドは、この質問の構成を修正します。
R1(config)#access-list 1 許可 10.1.1.0 0.0.0.3
R1(config)#route-map Leak-Route許可 10 // このコマンドは「oute_map Leak-Routedeny 10」コマンドも削除します。
R1(config-route-map)#match IP アドレス 1

最新問題: **152**

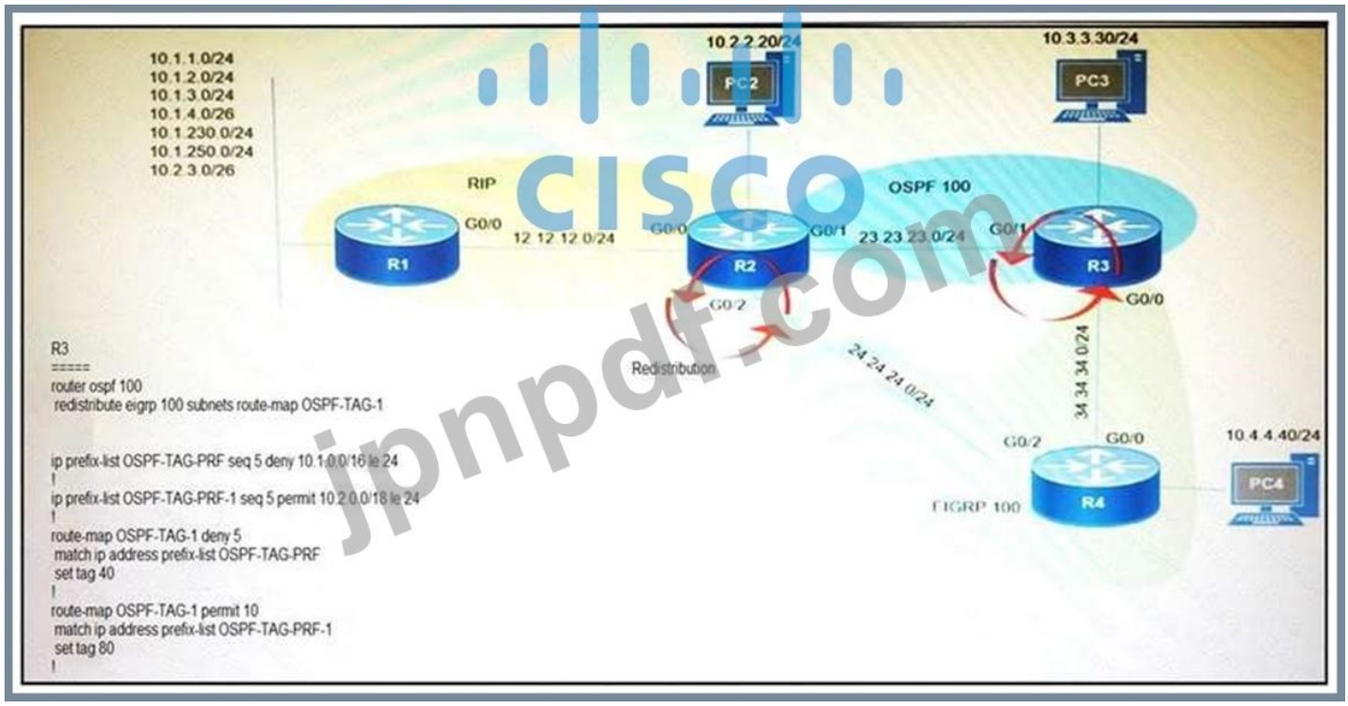
Customer (C) device	device in the core of the provider network that switches MPLS packets
CE device	device that attaches and detaches the VPN labels to the packets in the provider network
PE device	device in the enterprise network that connects to other customer devices
Provider (P) device	device at the edge of the enterprise network that connects to the SP network

Answer:

Customer (C) device	Provider (P) device
CE device	PE device
PE device	Customer (C) device
Provider (P) device	CE device

最新問題: **153**

展示を参照してください。



EIGRP から OSPF ルーティング プロトコルに再配布されるサブネットはどれですか?

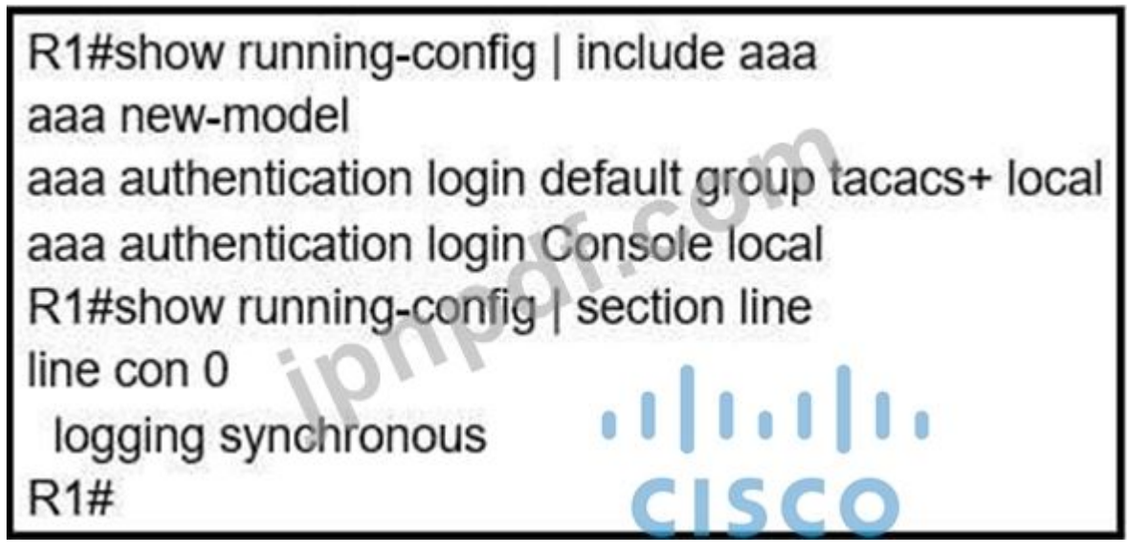
A. 10.1.2.0/24

B. 10.1.4.0/26

C. 10.2.2.0/24

D. 10.2.3.0/26
Answer: D (メーッセージを残す**)**

最新問題**: 154**
展示を参照してください。エンジニアはコンソール回線でローカル認証を設定しようとしていますが、デバイスは TACACS+ を使用して認証しようとしています。どのアクションによって目的の構成が生成されますか?



A. aaaauthenticationlogindefaultnone コマンドをグローバル設定に追加します。
B. aaa 認証ログイン コンソール ローカル コマンドの大文字の 「C」を小文字の 「c」に置き換えます。
C. aaaauthenticationlogindefaultgrouptacacs+local-case コマンドをグローバル コンフィギュレーションに追加します。
D. 回線設定にログイン認証コンソールコマンドを追加します。
Answer: D (メーッセージを残す**)**
セクション: インフラストラクチャのセキュリティ

最新問題**: 155**
ハッカーが偽のルーターを導入するのを防ぐために、MPLS クラウド全体で MD-5 認証を使用して保護する必要があるプロトコルはどれですか?
A. MP-BGP
B. LSP
C. 自民党
D. 出欠確認
Answer: A (メーッセージを残す**)**

最新問題**: 156**
展示を参照してください。

ACL は、ルータの受信ギガビット 0/1 インターフェイスに配置されます。ホスト
フローが許可されている場合でも、192.168.10.10 はホスト 192.168.100.10 に SSH 接続できません。このルーターへのフルアクセスを開かずに問題を解決するアクションはどれですか?

A. フローが機能するかどうかを確認するために、permit ip any any 行を ACL の先頭に一時的に移動します。

B. インターフェイスから ACL を一時的に削除して、フローが機能するかどうかを確認します。

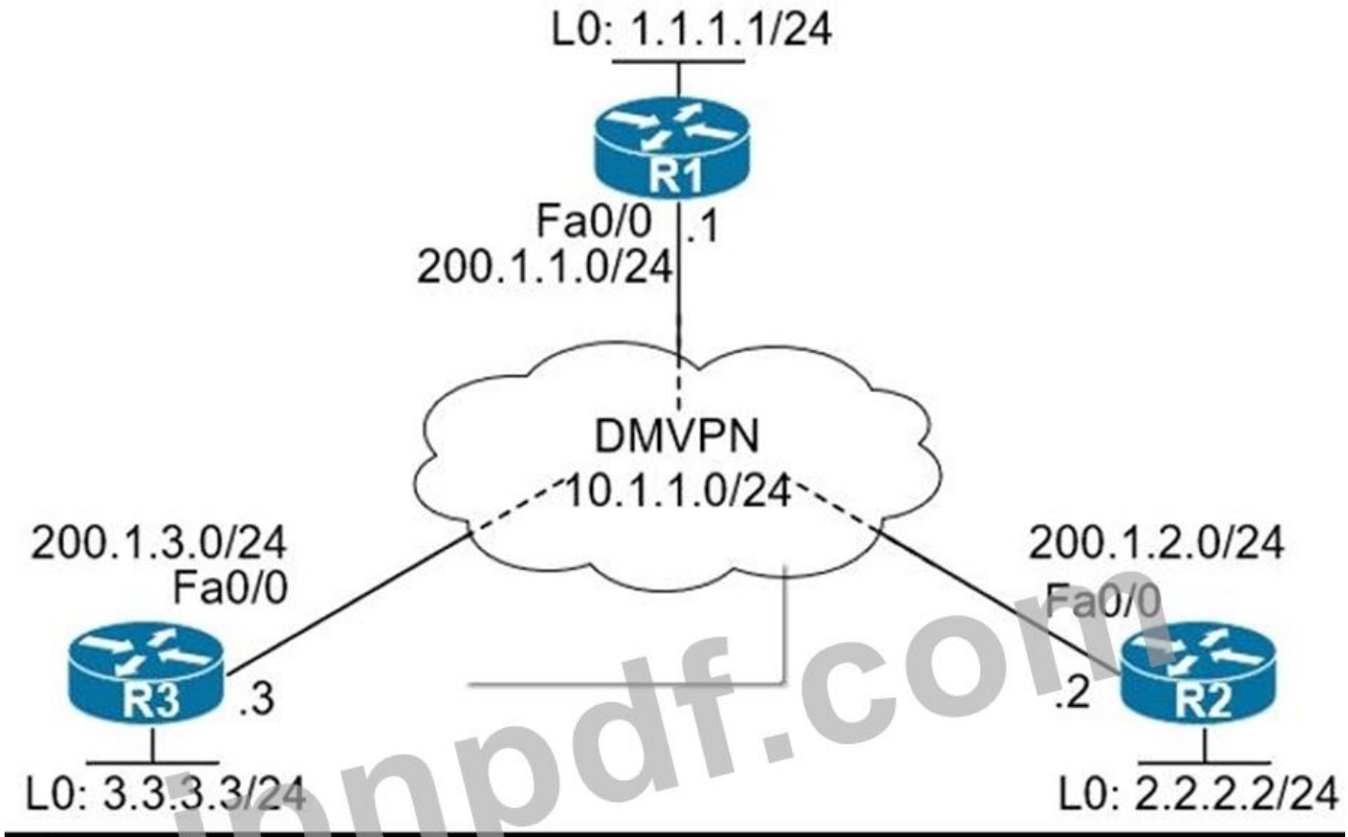
C. SSH エントリを ACL の先頭に移動します

D. show access-list FILTER コマンドを実行して、SSH エントリに関連するヒット統計があるかどうかを表示します。

Answer: C (メーッセージを残す**)**

最新問題**: 157**

展示品をご参照ください。




```
R2:
======
R2(config)# crypto isakmp policy 10
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# encryption 3des
R2(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R2(cfg-crypto-trans)# mode transport
R2(config)# crypto ipsec profile TST
R2(ipsec-profile)# set transform-set TSET
R2(config)# interface tunnel 123
R2(config-if)# tunnel protection ipsec profile TST
```

DMVPN が設定されている場合、トンネル ソースとしてループバックを使用したスポークツースポーク通信を許可する設定はどれですか?

A. ハブ上で暗号 isakmp キーのシスコ アドレス 0.0.0.0 を設定します。

B. ハブ上で暗号 isakmp キー Cisco アドレス 200.1.0.0 255.255.0.0 を設定します。

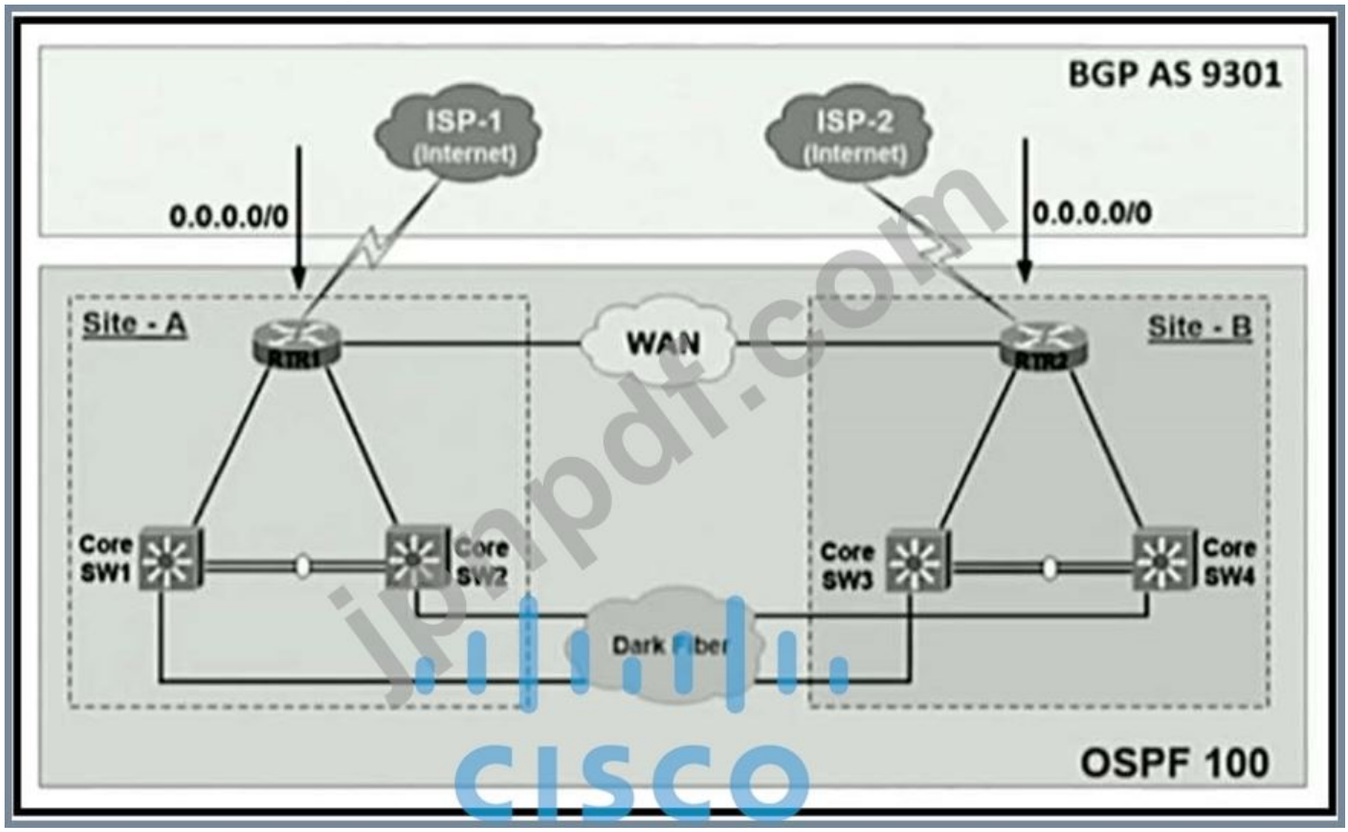
C. スポーク上で暗号 isakmp キーのシスコ アドレス 200.1.0.0 255.255.0.0 を設定します。

D. スポーク上で暗号 isakmp キーのシスコ アドレス 0.0.0.0 を設定します。

Answer: D (メーッセージを残す)

https://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd802b8f3c.html

最新問題: **158**
展示を参照してください。



リンクと BGP 接続が稼働している場合、インターネット トラフィックは常にサイト A ISP-1 を優先する必要があります。それ以外の場合、すべてのインターネット トラフィックは ISP-2 に送信される必要があります。再配布は BGP ルーティング プロトコルと OSPF ルーティング プロトコルの間で構成されており、期待どおりに機能しません。どのようなアクションをとれば問題が解決しますか?

A. サイト A RTR1 でメトリック タイプ 2 を設定し、サイト B RTR2 でメトリック タイプ 1 を設定します。

B. サイト A RTR1 で OSPF コスト 100 を設定し、サイト B RTR2 で OSPF コスト 200 を設定します。

C. サイト A RTR1 で OSPF コスト 200 を設定し、サイト B RTR2 で OSPF コスト 100 を設定します。

D. サイト A RTR1 でメトリック タイプ 1 を設定し、サイト B RTR2 でメトリック タイプ 2 を設定します。

Answer: D (メーッセージを残す)

OSPF タイプ 1 ルートは、同じ宛先に対してタイプ 2 ルートよりも常に優先されるため、サイト A RTR1 でメトリック タイプ 1 を設定して、サイト B RTR2 よりも優先されるようにすることができます。

注記：

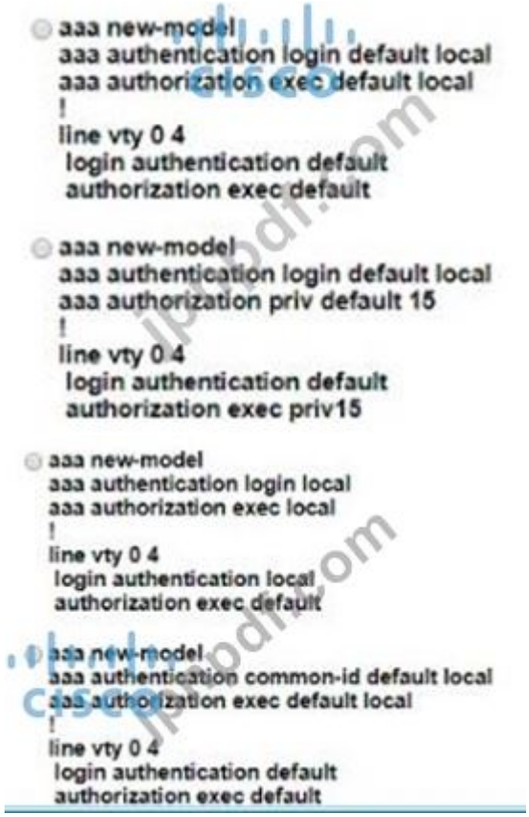
ルートは OSPF でタイプ 1 (E1) ルートまたはタイプ 2 (E2) ルートとして再配布されます。タイプ 2 がデフォルトです。

- タイプ 1 ルートのメトリックは、内部 OSPF コストと外部再配布コストの合計です。
- タイプ 2 ルートのメトリックは、再配布コストのみとなります。
- ルートがタイプ 2 として OSPF に再配布される場合、OSPF ドメイン内のすべてのルーターは外部ネットワークに到達するために同じコストがかかります。
- ルートがタイプ 1 として OSPF に再配布される場合、外部ネットワークに到達するコストはルーター

ごとに異なる可能性があります。

最新問題: **159**
展示を参照してください。

展示を参照してください。認証が期待どおりに機能せず、ユーザーはユーザー実行モードに落ちます。どの構成で問題が解決しますか?

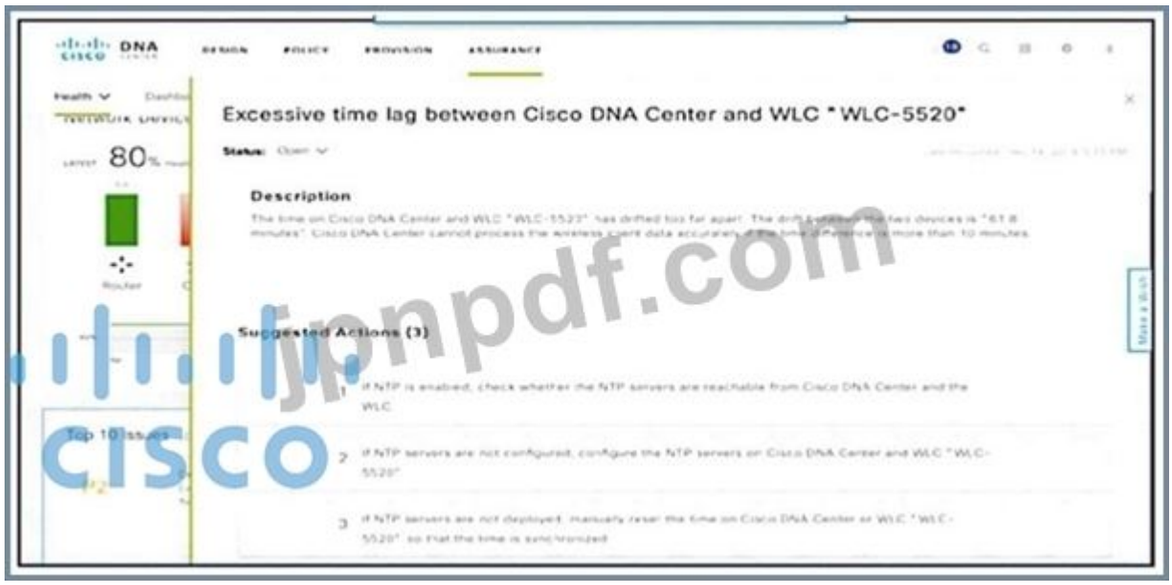


A. オプション A
B. オプション C
C. オプション B
D. オプション D
Answer: B (メーッセージを残す**)**

最新問題: **160**
ポート上の 802.1x 認証を無効にし、認証なしのトラフィックを許可するコマンドは何ですか?
A. dot1x ポート制御の無効化
B. dot1x ポート制御強制未承認
C. dot1x ポート制御自動
D. dot1x ポート制御強制承認

Answer: D (メーッセージを残す)
コマンド dot1x port-controlforce-authorized は、ポート上で 802.1x を無効にし、認証なしのトラフィックを許可するために使用されます。Dot1x ポートは、許可または未許可の 2 つの状態のいずれかになります。許可されたポートでは、ユーザー トラフィックがポートを通過することが許可されます。通常、この状態は認証が成功した後に発生します。未承認のポートでは、ポートを通過する承認トラフィックのみが許可されます。通常、ポートは無許可状態で開始されます。これにより、ユーザはポートと AAA 認証トラフィックを交換できるようになります。ユーザーが正常に認証されると、ポートは許可された状態に変更され、ユーザーはポートを通常どおり使用できるようになります。
802.1x の通常の使用では、ポートは dot1x port-control auto ステートメントで構成されます。これにより、認証が成功するまでポートは無許可状態になります。認証が成功すると、ポートは許可された状態に変更されます。
802.1x が最初に設定されるとき、ポートのデフォルトのポート制御は強制的に承認されます。これにより、認証が成功しなくても、ポートは強制的に許可された状態になります。この設定により、認証の必要性が無効になり、すべてのトラフィックが許可されます。
Force-unauthorized キーワードは、認証トラフィックに関係なく、ポートを未承認ポートとして設定します。
このキーワードを使用して設定されたポートでは、ユーザー トラフィックは許可されず、認証トラフィックも許可されません。
コマンド dot1x port-control disable は、構文が間違っているため、有効なコマンドではありません。
客観的：
インフラストラクチャのセキュリティ
副目的:
TACACS+ および RADIUS を備えた Cisco IOS AAA を使用したデバイス セキュリティについて説明する
参考文献:
Cisco > Catalyst 6500 シリーズ リリース 15.0SY ソフトウェア コンフィギュレーション ガイド > セキュリティ > IEEE 802.1X ポートベース認証 Cisco > Catalyst 4500 シリーズ スイッチ Cisco IOS コマンド リファレンス、12.2(52)SG > aaa アカウンティング dot1x インスタンスを介したデフォルトの開始/停止グループ半径 > dot1x port-control Cisco > Catalyst 4500 シリーズ スイッチ Cisco IOS コマンド リファレンス、12.2(52)SG > aaa アカウンティング dot1x インスタンスを介したデフォルトのスタート/ストップ グループ半径 > dot1x port-control

最新問題**: 161**
展示する：



NTP は、ネットワーク インフラストラクチャと Cisco DNA Center 全体にわたって設定されます。NTP の問題は、17:15 に Cisco DNA Center で報告されました。どのアクションで問題が解決しますか?

A. WLC と NTP サーバ間の到達可能性を確認して解決します。

B. NTP サーバーをリセットして、すべてのデバイスの同期の問題を解決します。

C. Cisco DNA Center と NTP サーバ間の到達可能性を確認して解決します。

D. WLC で NTP を確認して設定し、Cisco DNA Center と同期します

Answer: D (メーッセージを残す)

説明

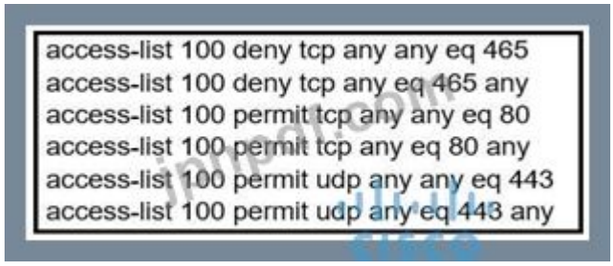
Cisco DNA Center とデバイス間の過度のタイムラグ :Cisco DNA Center とデバイスの IP アドレス間の時間差が大きく離れています。時間差が 3 分を超える場合、CiscoDNA Center はデバイス データを正確に処理できません。

参照：

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

最新問題: **162**

展示を参照してください。



トラブルシューティング中に、安全な Web ブラウザを使用してデバイスにアクセスできないことが判明しました。問題を解決するには何が必要ですか?

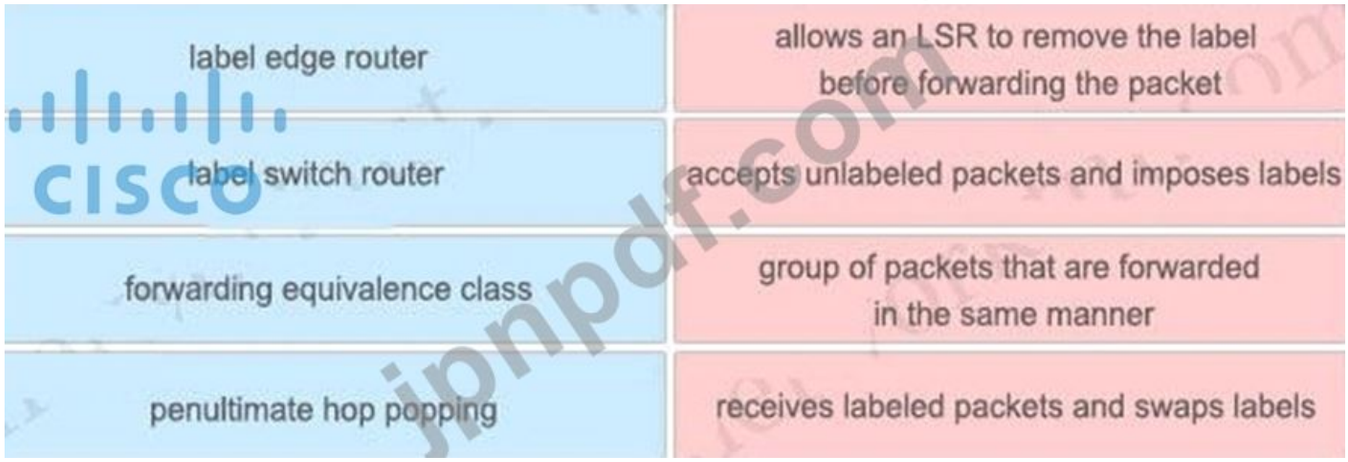
A. UDP ポート 465 を許可します

B. TCP ポート 443 を許可します

C. TCP ポート 22 を許可します

D. TCP ポート 465 を許可します
Answer: B (メッセージを残す**)**

最新問題**: 163**
左側の MPLS 概念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**: 164**
R2 にはローカルに発信されたプレフィックス 192.168.130.0/24 があり、次の構成があります。

```
ip prefix-list test seq 5 permit 192.168.130.0/24
!
route-map OUT permit 10
match ip address prefix-list test
set as-path prepend 65000
```

ルート マップ OUT コマンドが、neighbor 1.1.1.1 ルート マップ OUT out コマンドを使用して eBGP ネイバー R1 (1.1.1.1) に適用されると、結果はどうなりますか?
A. R1 は 192.168.130.0/24 以外のルートを受け入れません
B. R1 は 192.168.130.0/24 を 1 AS ホップではなく 2 AS ホップと認識します。
C. ネットワーク 192.168.130.0/24 は R1 テーブルでは許可されていません
D. R1 は 192.168.30.0/24 宛てのトラフィックを転送しません。
Answer: B (メッセージを残す**)**
最新問題**: 165**

顧客は、内部ネットワークを隠すためにループバックを使用して、2 つの顧客サイト間のプロバイダーネットワーク経由の GRE トンネルを要求しました。R1 とのトンネルを確立する R2 の設定はどれですか?

A. R2(config)# インターフェイス トンネル 1
R2(config-if)# IP アドレス 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1500
R2(config-if)# ip tcp 調整-mss 1360
R2(config-if)# トンネルソース 10.10.2.2
R2(config-if)# トンネル宛先 10.10.1.1

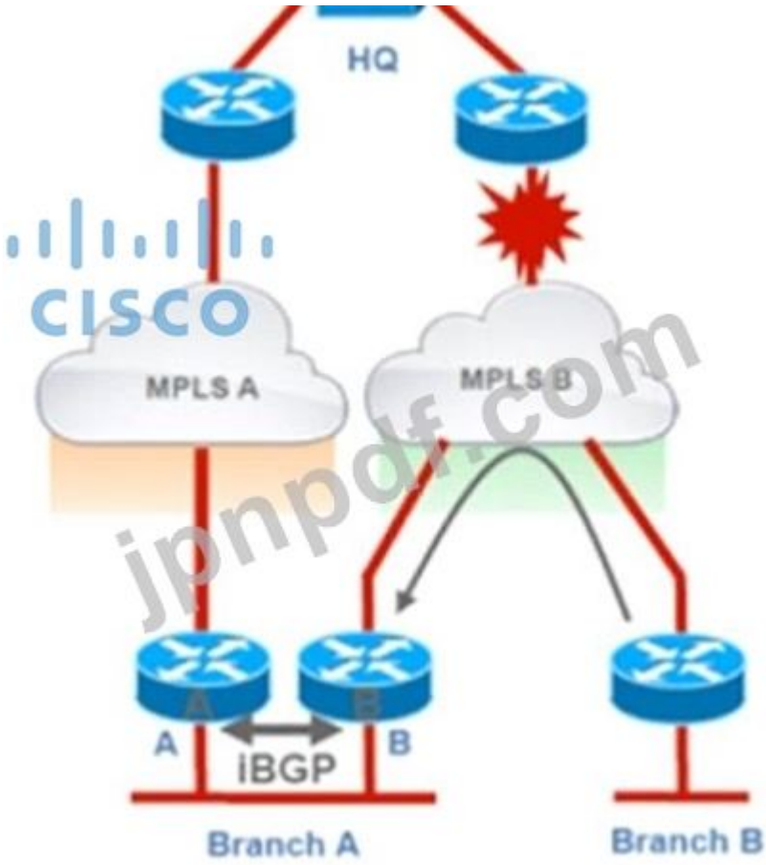
B. R2(config)# インターフェイス トンネル 1
R2(config-if)# IP アドレス 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp 調整-mss 1360
R2(config-if)# トンネル送信元 192.168.20.1
R2(config-if)# トンネル宛先 192.168.10.1

C. R2(config)# インターフェイス トンネル 1
R2(config-if)# IP アドレス 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp 調整-mss 1360
R2(config-if)# トンネルソース 10.10.2.2
R2(config-if)# トンネル宛先 10.10.1.1

D. R2(config)# インターフェイス トンネル 1
R2(config-if)# IP アドレス 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1500
R2(config-if)# ip tcp 調整-mss 1360
R2(config-if)# トンネル送信元 192.168.20.1
R2(config-if)# トンネル宛先 10.10.1.1

Answer: (解答を表示する**)**

最新問題**: 166**
展示を参照してください。



トラブルシューティングを行い、ブランチ B が本社に到達するために MPLS B ネットワークのみを使用するようにします。この要件を達成するアクションはどれですか?

A. ブランチ B で MPLS B ネットワークから受信したすべての HQ プレフィックスのローカル プリファレンスを、MPLS A ネットワークで使用されるローカル プリファレンスよりも高くします。

B. ブランチ A ルーターに AS パス フィルターを導入して、ローカル プレフィックスのみが BGP にアドバタイズされるようにします。

C. ブランチ A の MPLS B ネットワーク接続の先頭に AS パスを追加し、ブランチ A から MPLS B ネットワークに向かう HQ アドバタイズメントが 3 回先頭に追加されるようにします。

D. ブランチ B で MPLS B ネットワークから受信したすべての HQ プレフィックスの重みを、MPLS A ネットワークで使用される重みよりも高く変更します。

Answer: B (メーッセージを残す**)**

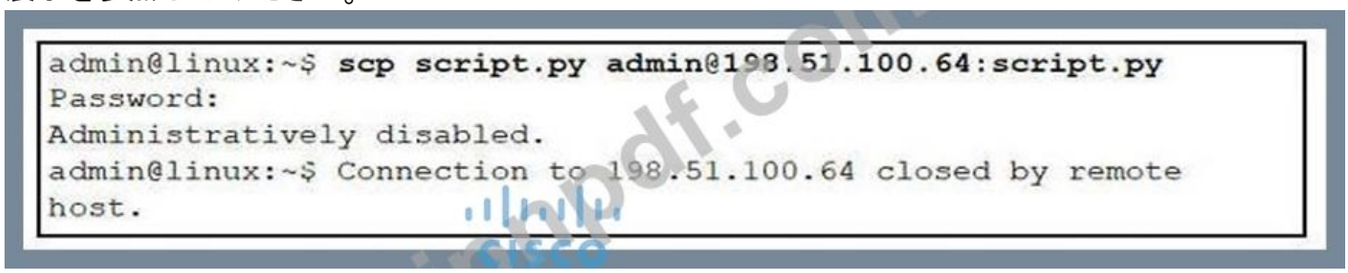
最新問題: **167**

左側のアドレスを右側の適切な IPv6 フィルターの目的にドラッグ アンド ドロップします。

Answer:

最新問題: **168**

展示を参照してください。



ネットワーク管理者は、ローカル Linux マシン上で Python スクリプトを開発し、それをルーターに転送しようとしています。ただし、転送は失敗します。この問題を解決するにはどのアクションを実行すればよいでしょうか?

A. SSH サービスは、crypto key generated rsa コマンドを使用して有効にする必要があります。

B. SCP サービスは、ip scpserverenable コマンドを使用して有効にする必要があります。

C. Python インタープリターは、最初に guestshell Enable コマンドを使用して有効にする必要があります。

D. Transport input ssh コマンドを使用して、VTY 回線で SSH アクセスを許可する必要があります。

Answer: B (メーッセージを残す**)**

管理的に無効になっています」というエラーは、次のコマンドを使用してルータ上で SCP を有効にする必要があることを意味します: Router(config)#ip scpserverenable

最新問題: **169**

MPLS レイヤ 3 VPN はどのように機能しますか?

A. 複数の顧客サイトがサービス プロバイダー ネットワークを通じて相互接続し、顧客エッジ デバイス間に安全なトンネルを作成します。

B. 一連のサイトは、顧客サイトで集約のためにマルチプロトコル BGP を使用します。

C. セキュリティのために、一連のサイトがインターネット経由でプライベートに相互接続します。

D. カスタマー エッジからプロバイダー エッジへの接続を使用して、複数の顧客サイトがサービス プロバイダー ネットワークを通じて相互接続します。

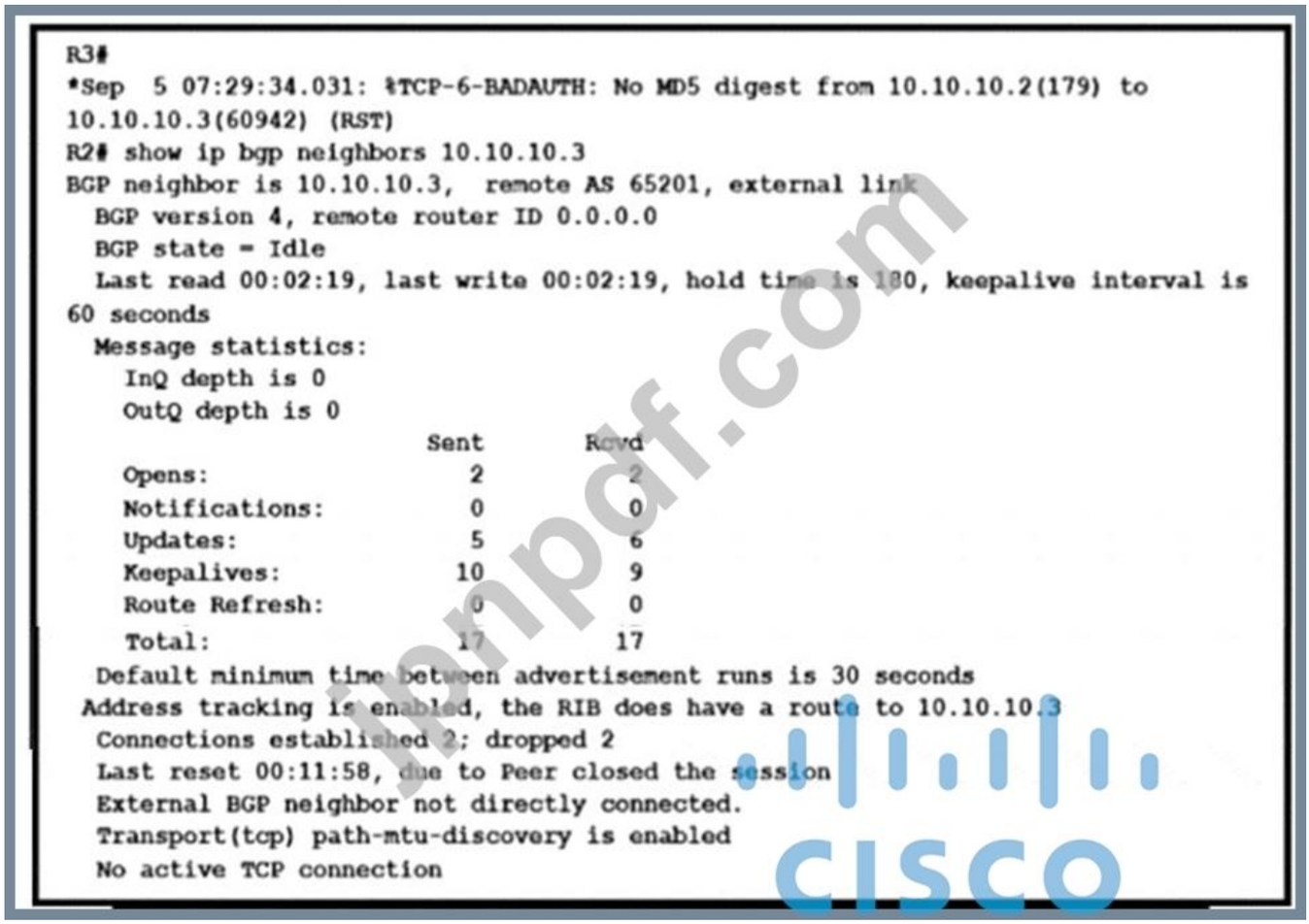
Answer: D (メーッセージを残す**)**

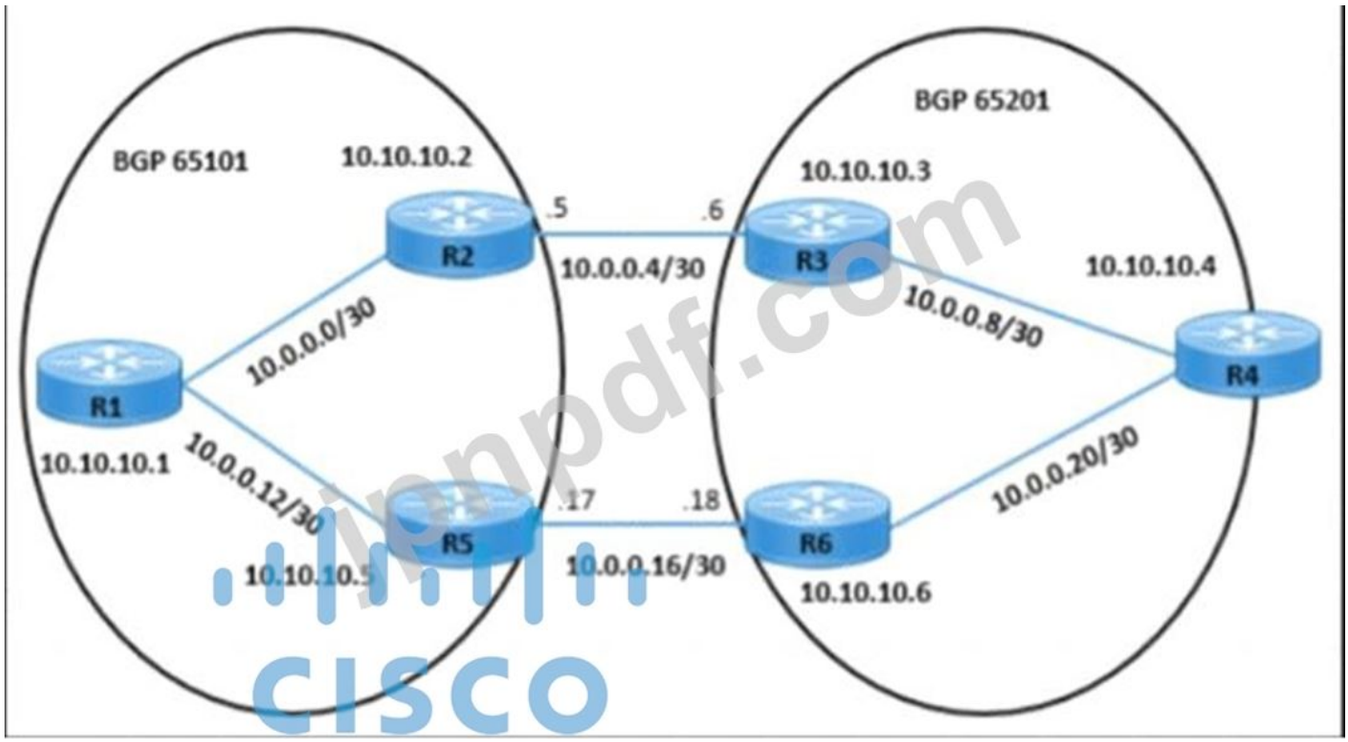
説明

マルチプロトコル ラベル スイッチング (MPLS) レイヤ 3 仮想プライベート ネットワーク (VPN) は、MPLS プロバイダー コア ネットワークによって相互接続された一連のサイトで構成されます。各顧客サイトでは、1 つ以上のカスタマー エッジ (CE) ルーターが 1 つ以上のプロバイダー エッジ (PE) ルーターに接続されています。

最新問題**: 170**

展示を参照してください。





ネットワーク運用チームは、R2 と R3 の間のトラフィック転送の問題を観察しています。
※R2からR3へのループバックIPアドレスのpingとtracerouteは成功します。
* AS 65101 および AS 65201 の iBGP ピアリングは稼働中です。
どの構成で問題が解決しますか?

A. R2 および R3 ルーターで eBGP マルチホップをセットアップします。
B. R2 で MD5 パスワード認証を構成します。
C. AS 65101 および AS 65201 で R2 および R3 ループバック IP をアドバタイズします。
D. R3 の MD5 パスワード認証を削除します。
Answer: A (メーッセージを残す**)**

最新問題**: 171**
エンジニアは PBR en R5 を設定し、10.10.10.0/24 宛てのトラフィックに一致するポリシーを作成して 10.1.1 1 に転送したいと考えています。このトラフィックの IP 優先順位も 5 に設定する必要があります。他のすべてのトラフィックは 10.10.10/24 に転送する必要があります。10.1.1.2 であり、その IP 優先順位は 0 に設定されています。要件を満たす構成はどれですか?


```
access-list 100 permit ip any 10.10.10.0 0.0.0.255
route-map CCNP permit 10
 match ip address 100
 set ip next-hop 10.1.1.1
 set ip precedence 5
!
route-map CCNP permit 20
 set ip next-hop 10.1.1.2
 set ip precedence 0
```

```
access-list 1 permit 10.10.10.0 0.0.0.255
access-list 2 permit any
route-map CCNP permit 10
 match ip address 1
 set ip next-hop 10.1.1.1
 set ip precedence 5
!
route-map CCNP permit 20
 match ip address 2
 set ip next-hop 10.1.1.2
 set ip precedence 0
!
route-map CCNP permit 30
```

A. オプション A

B. オプション C

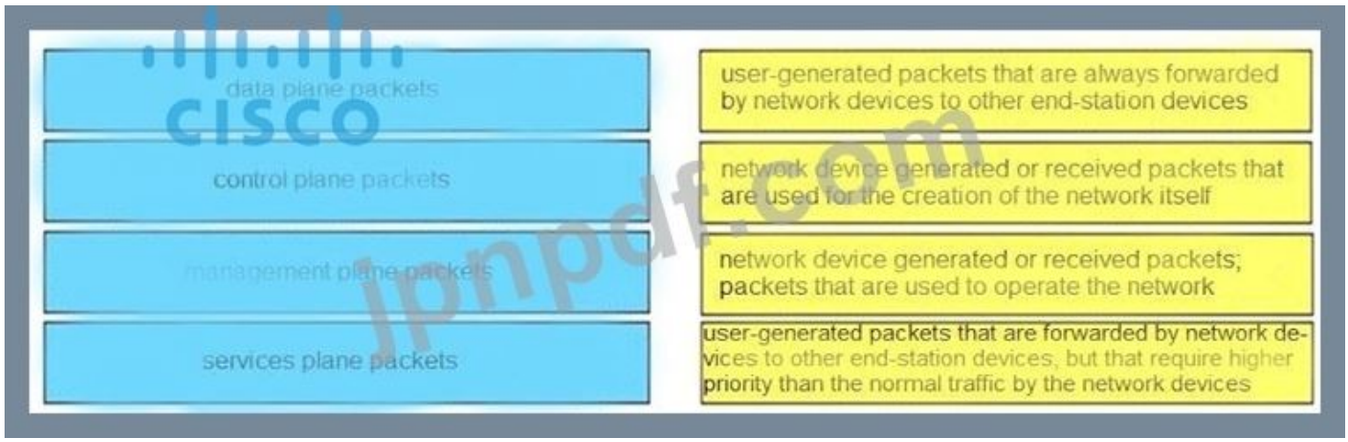
C. オプション B

D. オプション D

Answer: A (メーッセージを残す**)**

最新問題**: 172**

左側のパケット タイプ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:

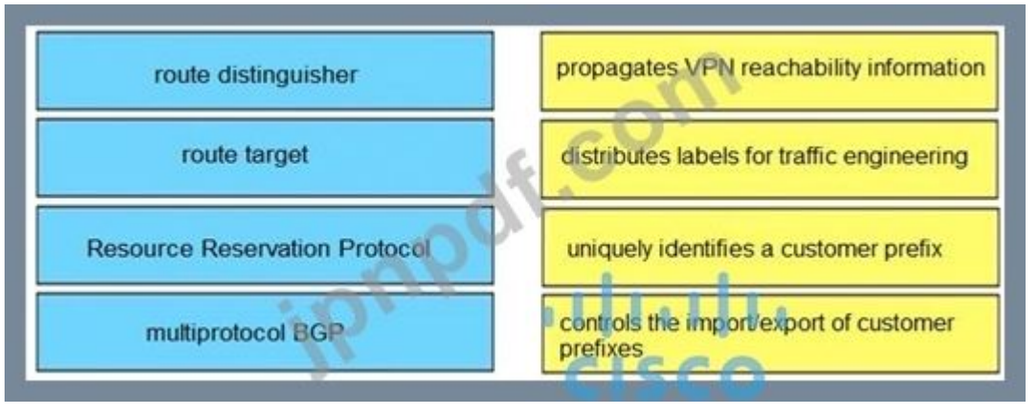
説明

個別のデータ チャネルと制御チャネルを定義する ISDN、フレーム リレー、ATM などの従来のネットワーク テクノロジとは異なり、IP はすべてのパケットを 1 つのパイプ内で伝送します。したがって、ルーターやスイッチなどの IP ネットワーク デバイスは、データ プレーン、コントロール プレーン、および管理プレーンのパケットを区別して、各パケットを適切に処理できる必要があります。IP トラフィック プレーンの観点からは、パケットは次の 4 つの異なる論理グループに分割できます。1. データ プレー

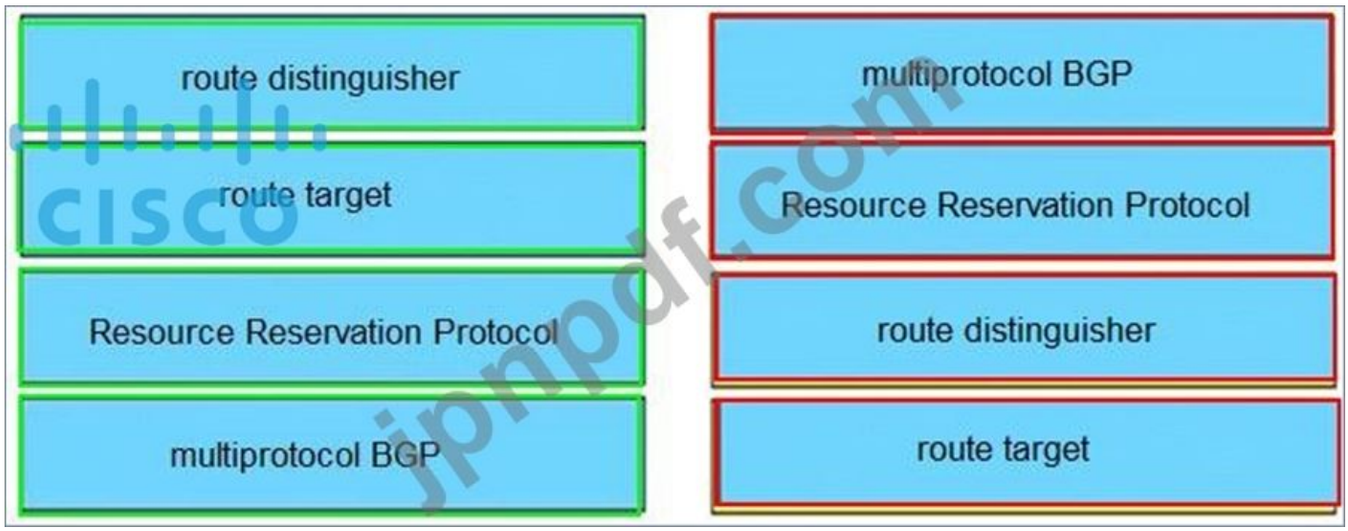
ン パケット - ネットワーク デバイスによって常に他のエンド ステーション デバイスに転送される、エンド ステーションのユーザー生成パケット。ネットワーク デバイスの観点から見ると、データ プレーン パケットには常に中継先 IP アドレスがあり、通常の宛先 IP アドレス ベースの転送プロセスで処理できます。コントロール プレーン パケット - ネットワーク自体の作成と運用に使用される、ネットワーク デバイスが生成または受信したパケット。ネットワーク デバイスの観点から見ると、コントロール プレーン パケットには常に受信宛先 IP アドレスがあり、ネットワーク デバイスのルート プロセッサの CPU によって処理されます。例には、ARP、BGP、OSPF などのプロトコルや、ネットワークを結び付けるその他のプロトコルが含まれます。管理プレーン パケット - ネットワークの管理に使用される、ネットワーク デバイスが生成または受信したパケット、または管理ステーションが生成または受信したパケット。ネットワーク デバイスの観点から見ると、管理プレーン パケットには常に受信宛先 IP アドレスがあり、ネットワーク デバイスのルート プロセッサの CPU によって処理されます。例には、Telnet、セキュア シェル (SSH)、TFTP、SNMP、FTP、NTP などのプロトコルや、デバイスやネットワークの管理に使用されるその他のプロトコルが含まれます。サービス プレーン パケット - データ プレーン パケットの特殊なケースであるサービス プレーン パケットも、ネットワーク デバイスによって他のエンド ステーション デバイスに転送されるユーザー生成パケットですが、ネットワーク デバイスによるハイタッチ処理が必要です（上記以外にも）。通常の宛先 IP アドレスベースの転送）を使用してパケットを転送します。ハイタッチ処理の例には、GRE カプセル化、QoS、MPLS VPN、SSL/IPsec 暗号化/復号化などの機能が含まれます。ネットワーク デバイスの観点から見ると、サービス プレーン パケットには通過先 IP アドレスが含まれる場合もあれば、送信先 IP アドレスが含まれる場合もあります。受信宛先 IP アドレス (VPN トンネル エンドポイントの場合など)。

最新問題: **173**

左側の MPLS VPN の概念を右側の適切な説明にドラッグ アンド ドロップします。

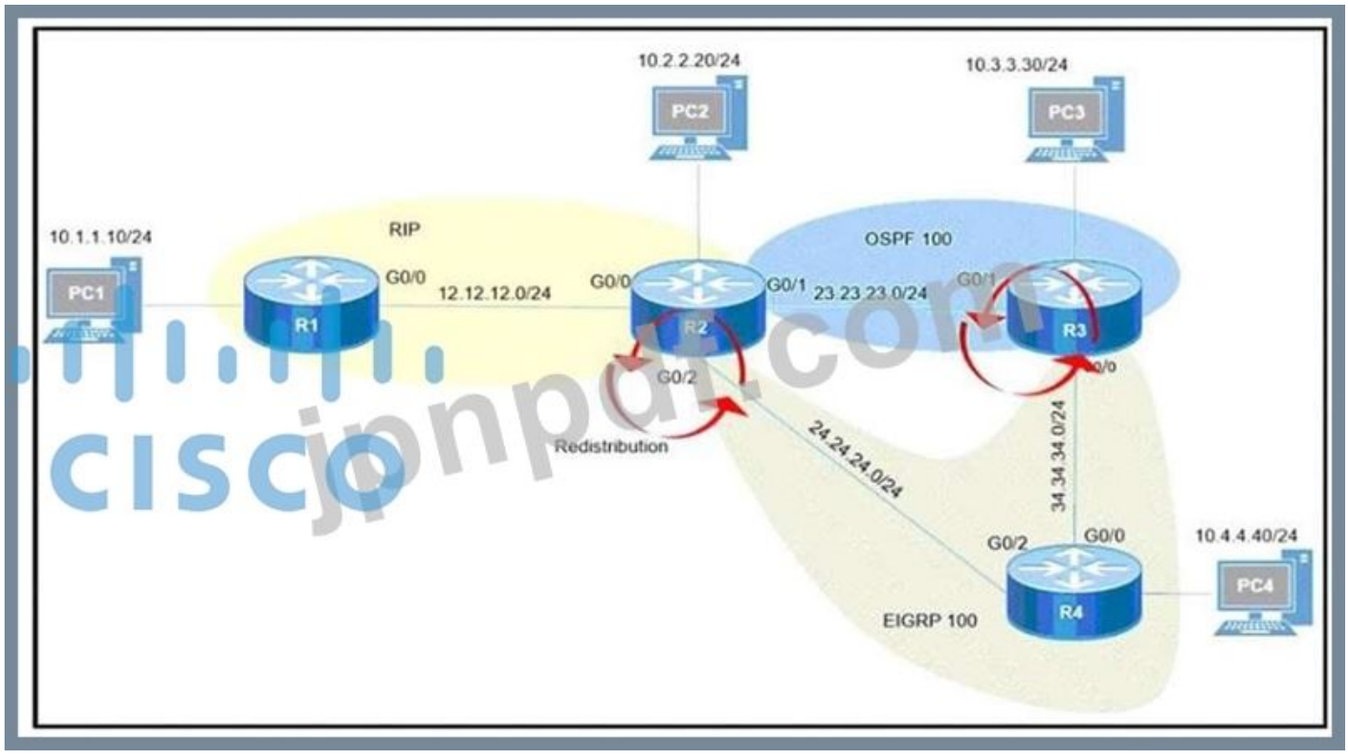


Answer:



参照：
https://www.rogerperkin.co.uk/featured/route-distinguisher-vs-route-target/

最新問題: **174**
展示を参照してください。



ルーティング プロトコル間で再配布が有効になった後。PC2、PC3、および PC4 は PC1 に到達できません。すべての PC にアクセスできるように問題を解決するために、エンジニアはどのようなアクションを実行できますか?

A. OSPF から EIGRP に再配布されるときにプレフィックス 10.1.1.0/24 をフィルタリングします。
B. R2 の RIP プロセスでアドミニストレーティブ ディスタンス 100 を設定します。
C. RIP から EIGRP に再配布されるときにプレフィックス 10.1.1.0/24 をフィルタリングします。
D. R2 上で直接接続されたインターフェイスを再配布します。
Answer: A (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。

```
CPE(config)# lin c 0
CPE(config-line)# no exec
CPE(config-line)# end
CPE#
*Jan 31 23:07:22.655: %SYS-5-CONFIG_I: Configured from console
by console
CPE# wr
Building configuration...
[OK]
CPE# exit

CPE con0 is now available

Press RETURN to get started.

! Console stopped responding at this moment !
```

管理者は、一定期間非アクティブな状態が続いた後の自動ログアウトを無効にしようとしています。ログアウト後、コンソールはすべてのキーワード入力に応答しなくなります。SSH を介したリモート アクセスは引き続き機能し、問題は解決しますか?

A. 行 con 0 で no exec-timeout コマンドを設定します。

B. con 0 行目に exec コマンドを設定します。

C. 行 con 0 でデフォルトの exec-timeout コマンドを構成します。

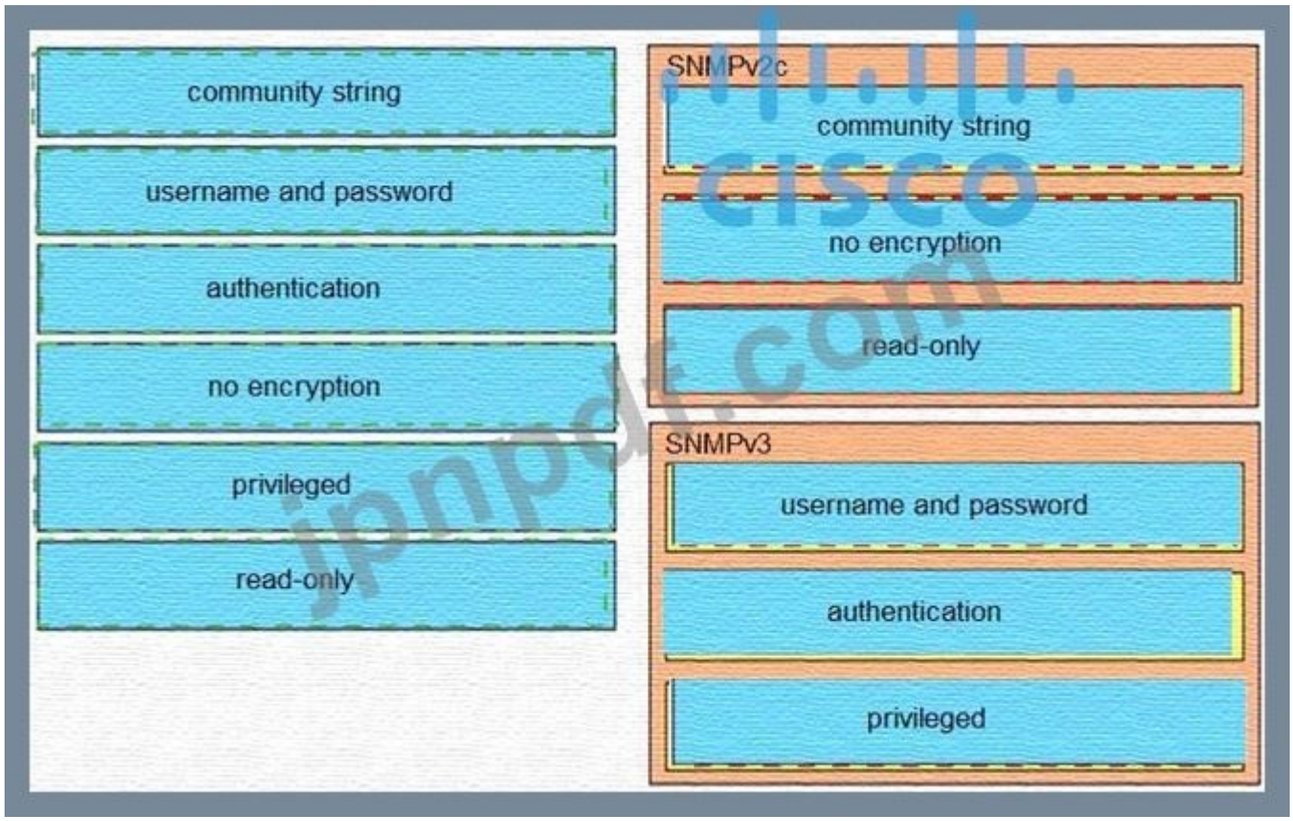
D. 行 con 0 で絶対タイムアウト コマンドを設定します。

Answer: A (メーッセージを残す**)**

最新問題: **176**

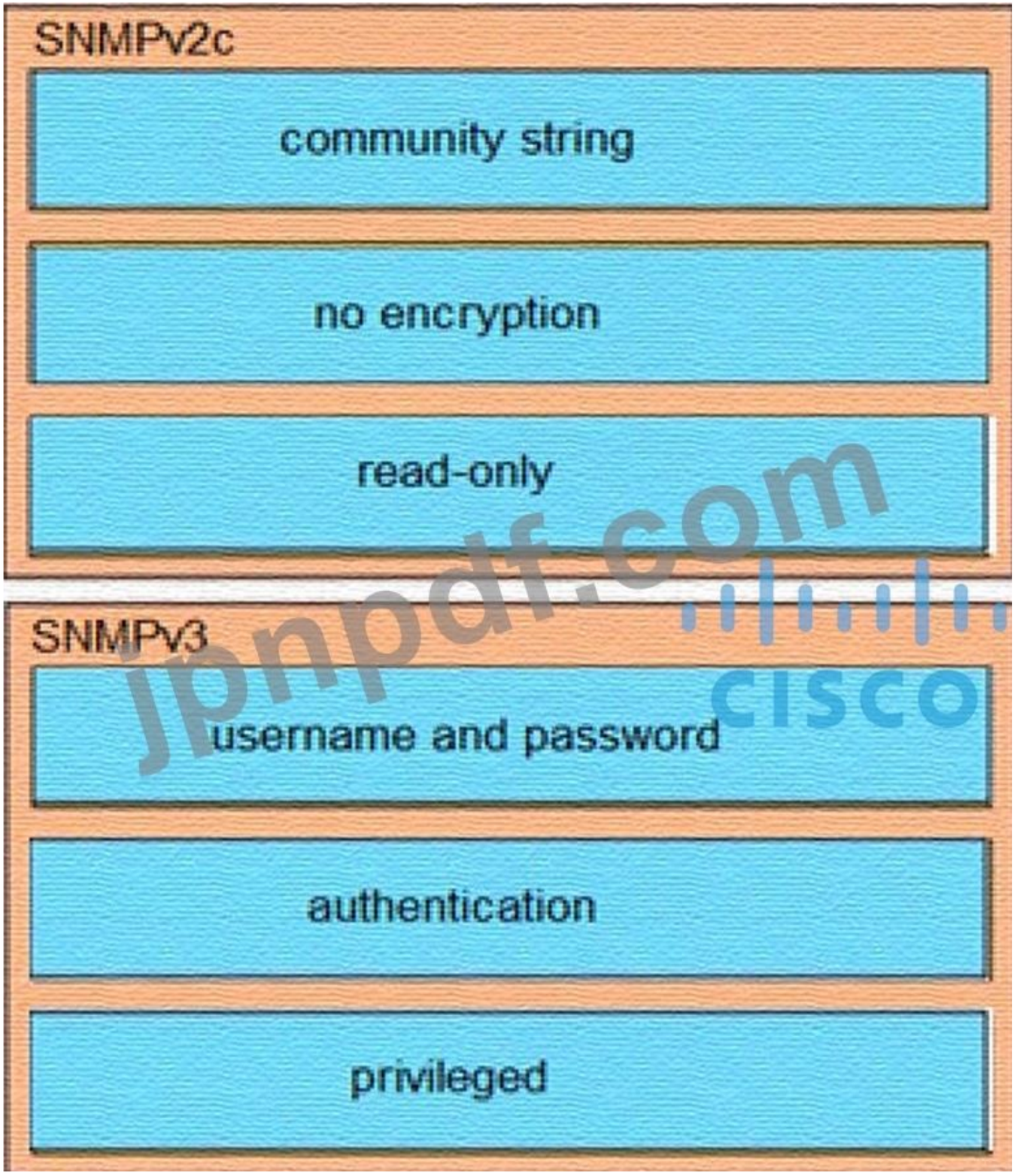
Cisco IOS デバイスの SNMP 属性を左側から右側の適切な SNMPv2c または SNMPV3 カテゴリにド

Answer:



説明

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



最新問題: **177**
展示を参照してください。

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
time-range Office-hour
periodic weekdays  08:00 to 17:00
!
access-list 101 permit tcp 10.0.0.0 0.0.0.0 172.16.1.0 0.0.0.255 eq ssh time-range Office-hour
```

IT スタッフ メンバーが通常の営業時間内にオフィスに出社しましたが、SSH 経由でデバイスにアクセスできません。この問題を解決するにはどのようなアクションを実行する必要がありますか?

A. 正しい IP アドレスを使用するようにアクセス リストを変更します。

B. 正しい時間範囲を設定します。

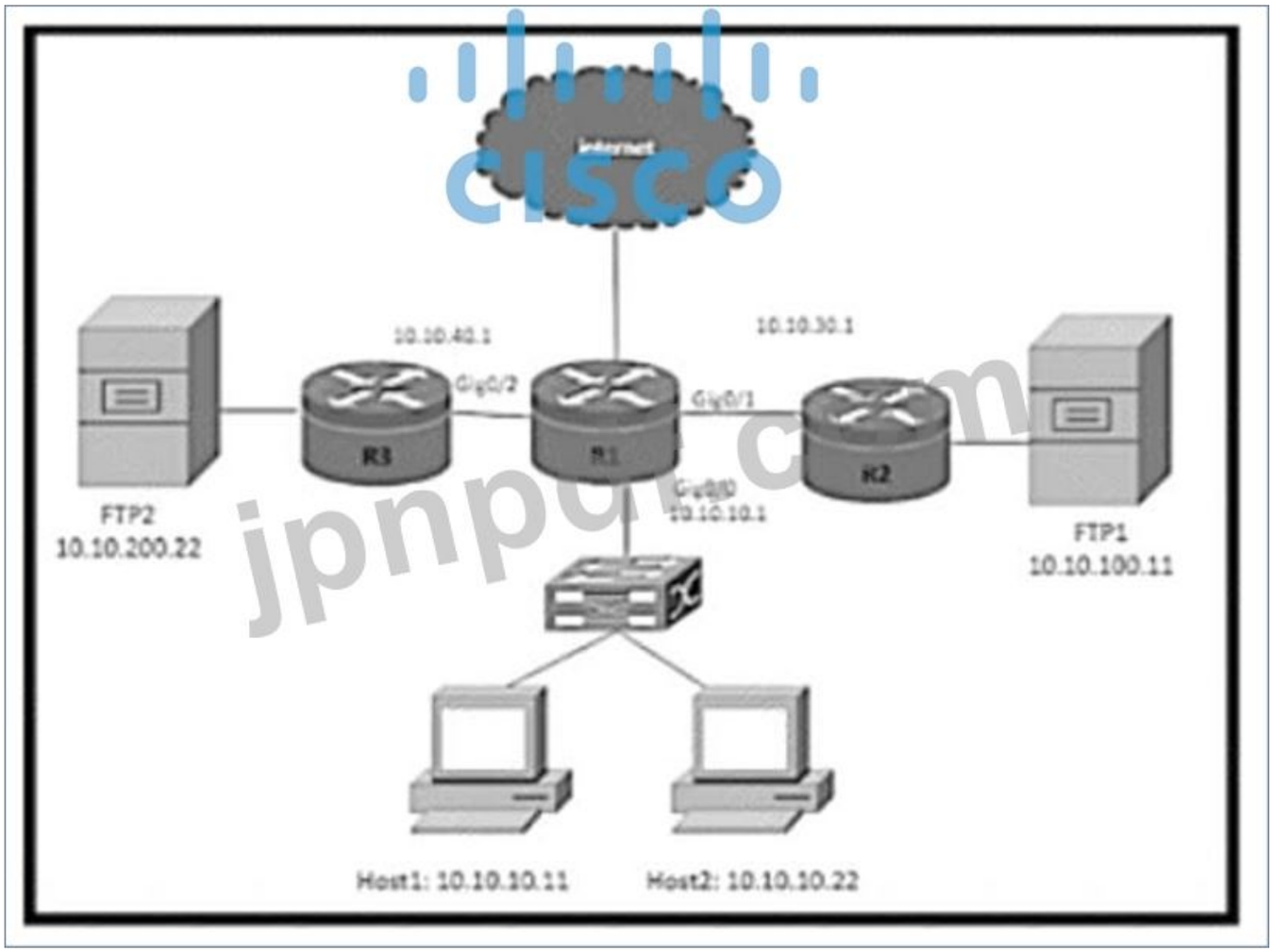
C. アクセス リストを変更してサブネット マスクを修正します。

D. アウトバウンド方向のアクセス リストを設定します。

Answer: A (メーッセージを残す**)**

ACL には tcp 101 10.1.1.1 0.0.0.0 を許可する必要があります

最新問題**: 178**



展示を参照してください。R1 ルーティング テーブルには、FTP1 および FTP2 ファイル サーバーのプレ

フィックスが付いています。ネットワーク エンジニアは、次の要件に従って R1 を構成する必要があります。

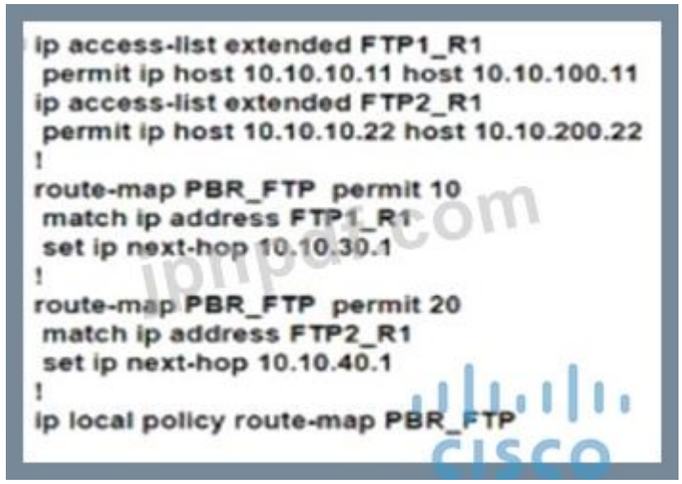
* Host1 は FTP1 ファイルサーバーを使用する必要があります。
* Host2 は FTP2 ファイルサーバーを使用する必要があります。

R1 の要件を満たす構成はどれですか?

A.

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP  permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
interface GigabitEthernet 0/0
 ip policy route-map PBR_FTP
```

B.



```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP  permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
ip local policy route-map PBR_FTP
```

C.

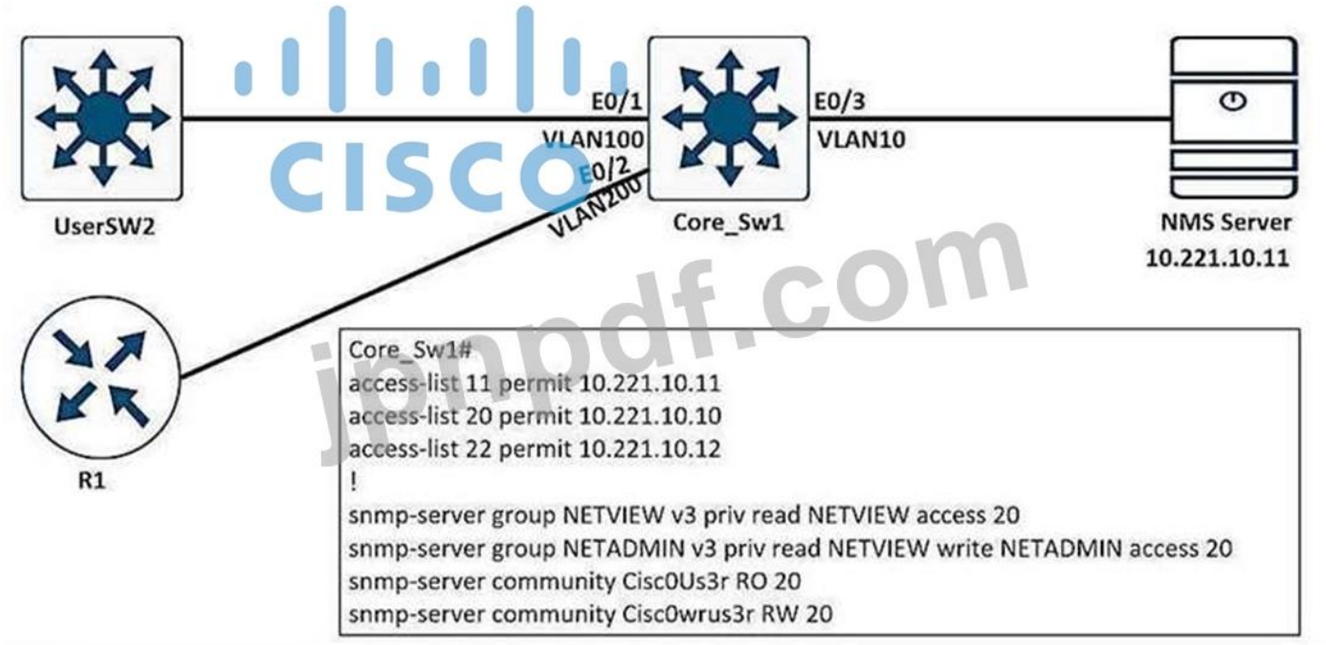
```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.40.1
route-map PBR_FTP  permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.30.1
!
ip local policy route-map PBR_FTP
```

```
access-list extended FTP1_R1
permit ip host 10.10.10.11 any
access-list extended FTP2_R1
permit ip host 10.10.10.22 any
route-map PBR_FTP  permit 10
match ip address FTP1_R1
set ip next-hop 10.10.30.1

route-map PBR_FTP  permit 20
match ip address FTP2_R1
set ip next-hop 10.10.40.1

interface GigabitEthernet 0/0
```

D. ip policy route-map PBR_FTP

Answer: A (メッセージを残す**)**

最新問題**: 179**



A. アクセスリスト 20 許可 10.221.10.12

B. アクセスリスト 20 許可 10.221.10.11

C. SNMP サーバー グループ NETADMIN v3 priv 読み取り NETVIEW 書き込み NETADMIN アクセス 22

D. SNMP サーバー グループ NETVIEW v2c priv 読み取り NETVIEW アクセス 20

Answer: (解答を表示する**)**

最新問題**: 180**

展示を参照してください。管理者は、conf Me パッケージを FTP サーバーにアップロードする必要があります。ただし、FTP サーバーは匿名サービスを拒否し、ユーザーに認証を要求しました。問題を解決する 2 つの方法は何ですか? (2つお選びください。)

A. FTP URL に FTP サーバーの資格情報を直接入力します。
ftp://ユーザー名:パスワードQ192.0.2.40/ 構文。

B. FTP サーバー上のユーザー名とパスワードに一致するユーザーを rooter 上に作成し、コピーを試行する前にログインします。

C. 代わりに copy flash:packages.conf scp: コマンドを使用し、プロンプトが表示されたら FTP サーバーの認証情報を入力します。

D. is ftp username および ip ftp passwd 設定コマンドを使用して、有効な FTP サーバー資格情報を指定します。

E. 代わりに copy flash-packages conf ftp: コマンドを使用し、プロンプトが表示されたら FTP サーバーの credent-ais を入力します。

Answer: A,D (メーッセージを残す**)**

最新問題**: 181**
展示を参照してください。

ユーザーはルーターに SSH 接続できません。この問題を解決するにはどのような措置を講じる必要がありますか?

A. トランスポート入力 SSH を構成する

B. トランスポート出力 SSH を構成する

C. ip ssh バージョン 2 を構成します

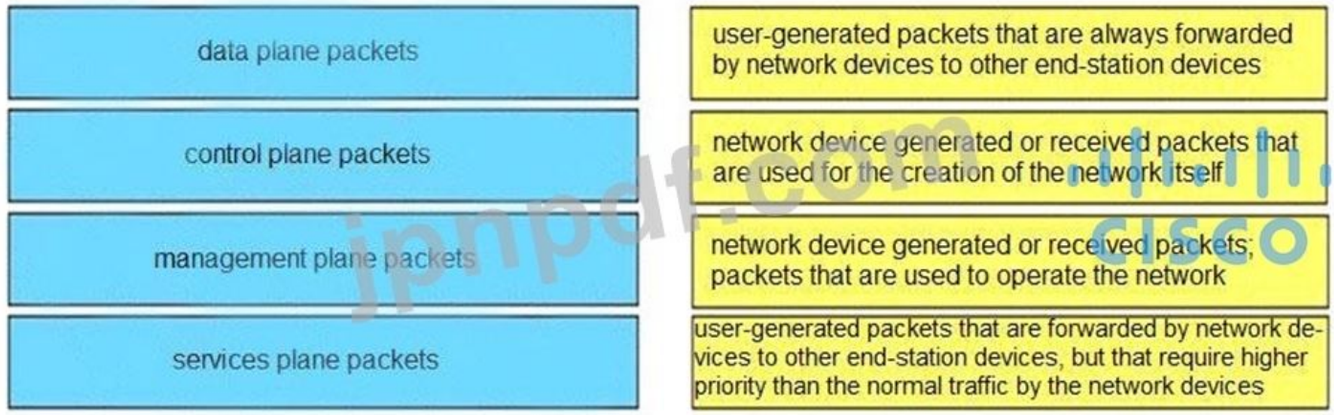
D. ip ssh ソース インターフェイス ループバック 0 を設定します。

Answer: A (メーッセージを残す**)**

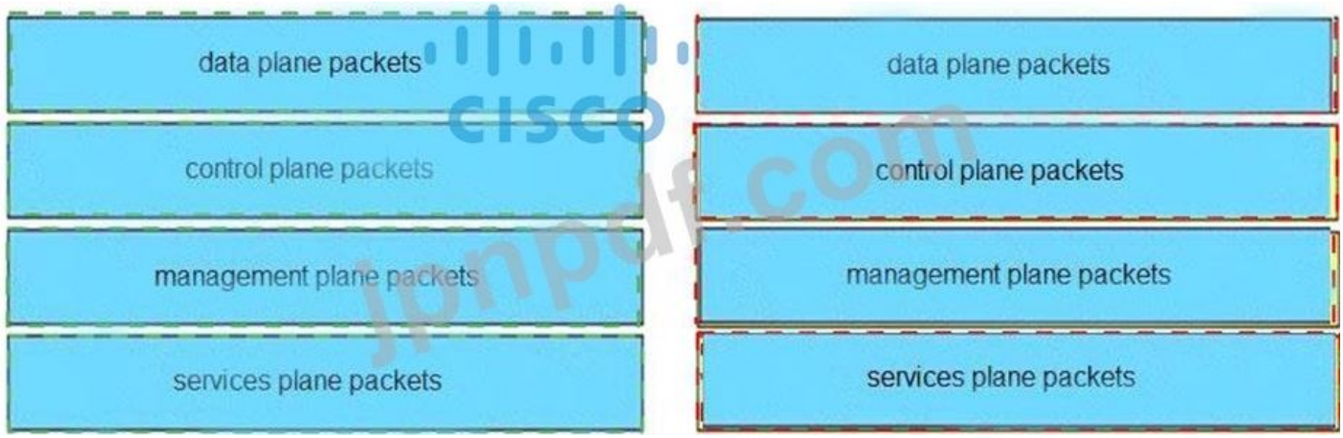
説明

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configurati 960-x_cg_chapter_01001.html

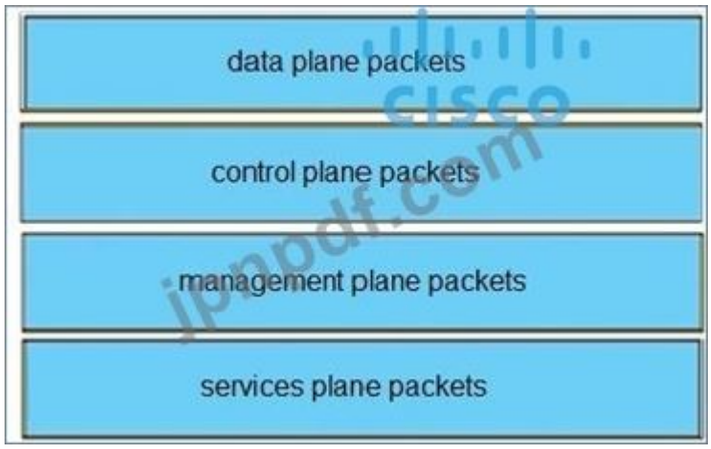
最新問題: 182
左側のパケット タイプを右側の正しい説明にドラッグ アンド ドロップします。



Answer:



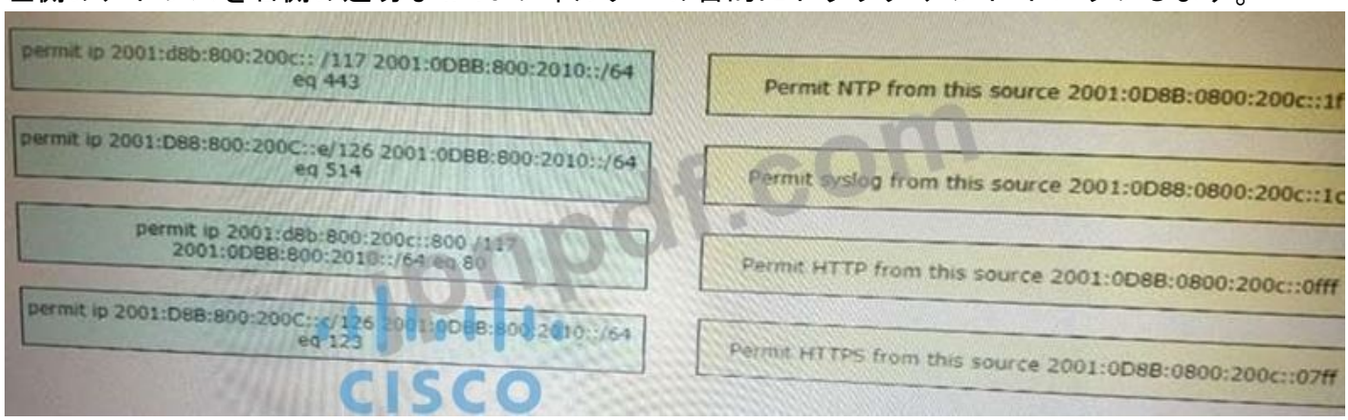
説明



個別のデータ チャネルと制御チャネルを定義する ISDN、フレーム リレー、ATM などの従来のネットワーク テクノロジとは異なり、IP はすべてのパケットを 1 つのパイプ内で伝送します。したがって、ルーターやスイッチなどの IP ネットワーク デバイスは、データ プレーン、コントロール プレーン、および管理プレーンのパケットを区別して、各パケットを適切に処理できる必要があります。IP トラフィック プレーンの観点からは、パケットは次の 4 つの異なる論理グループに分割できます。1. データ プレー

ン パケット - ネットワーク デバイスによって常に他のエンド ステーション デバイスに転送される、エンド ステーションのユーザー生成パケット。ネットワーク デバイスの観点から見ると、データ プレーン パケットには常に中継先 IP アドレスがあり、通常の宛先 IP アドレス ベースの転送プロセスで処理できます。コントロール プレーン パケット - ネットワーク自体の作成と運用に使用される、ネットワーク デバイスが生成または受信したパケット。ネットワーク デバイスの観点から見ると、コントロール プレーン パケットには常に受信宛先 IP アドレスがあり、ネットワーク デバイスのルート プロセッサの CPU によって処理されます。例には、ARP、BGP、OSPF などのプロトコルや、ネットワークを結び付けるその他のプロトコルが含まれます。管理プレーン パケット - ネットワークの管理に使用される、ネットワーク デバイスが生成または受信したパケット、または管理ステーションが生成または受信したパケット。ネットワーク デバイスの観点から見ると、管理プレーン パケットには常に受信宛先 IP アドレスがあり、ネットワーク デバイスのルート プロセッサの CPU によって処理されます。例には、Telnet、セキュア シェル (SSH)、TFTP、SNMP、FTP、NTP などのプロトコルや、デバイスやネットワークの管理に使用されるその他のプロトコルが含まれます。サービス プレーン パケット - データ プレーン パケットの特殊なケースであるサービス プレーン パケットも、ネットワーク デバイスによって他のエンド ステーション デバイスに転送されるユーザー生成パケットですが、ネットワーク デバイスによるハイタッチ処理が必要です（上記以外にも）。通常の宛先 IP アドレスベースの転送）を使用してパケットを転送します。ハイタッチ処理の例には、GRE カプセル化、QoS、MPLS VPN、SSL/IPsec 暗号化/復号化などの機能が含まれます。ネットワーク デバイスの観点から見ると、サービス プレーン パケットには通過先 IP アドレスが含まれる場合もあれば、送信先 IP アドレスが含まれる場合もあります。受信宛先 IP アドレス (VPN トンネル エンドポイントの場合など)。

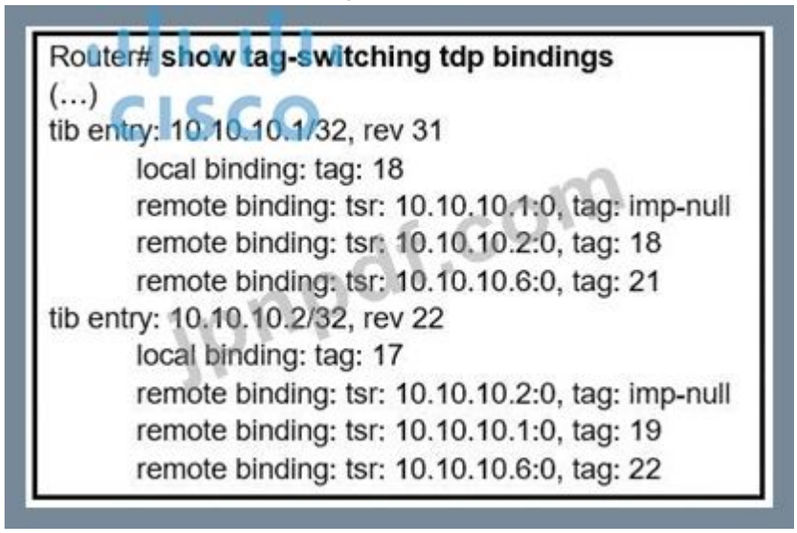
最新問題: **183**
左側のアドレスを右側の適切な IPv6 フィルターの目的にドラッグ アンド ドロップします。



Answer:

最新問題**: 184**

展示を参照してください。



MPLS VPN クラウドでは imp-null タグは何を表しますか?

A. ラベルをポップします

B. ラベルを面付けします

C. EXP ビットを含めます

D. EXP ビットを除外します

Answer: A (メーッセージを残す**)**

説明

imp-null (暗黙的ヌル) タグは、パケットを転送する前にタグ スタックからタグ エントリをポップするように上流ルータに指示します。

注: Pop は、最上位の MPLS ラベルを削除することを意味します

最新問題**: 185**

MPLS ルーター間でラベル バインディング交換が頻繁に行われる原因となるフラッピング リンクを克服するために使用される 2 つのソリューションはどれですか? (2つお選びください)

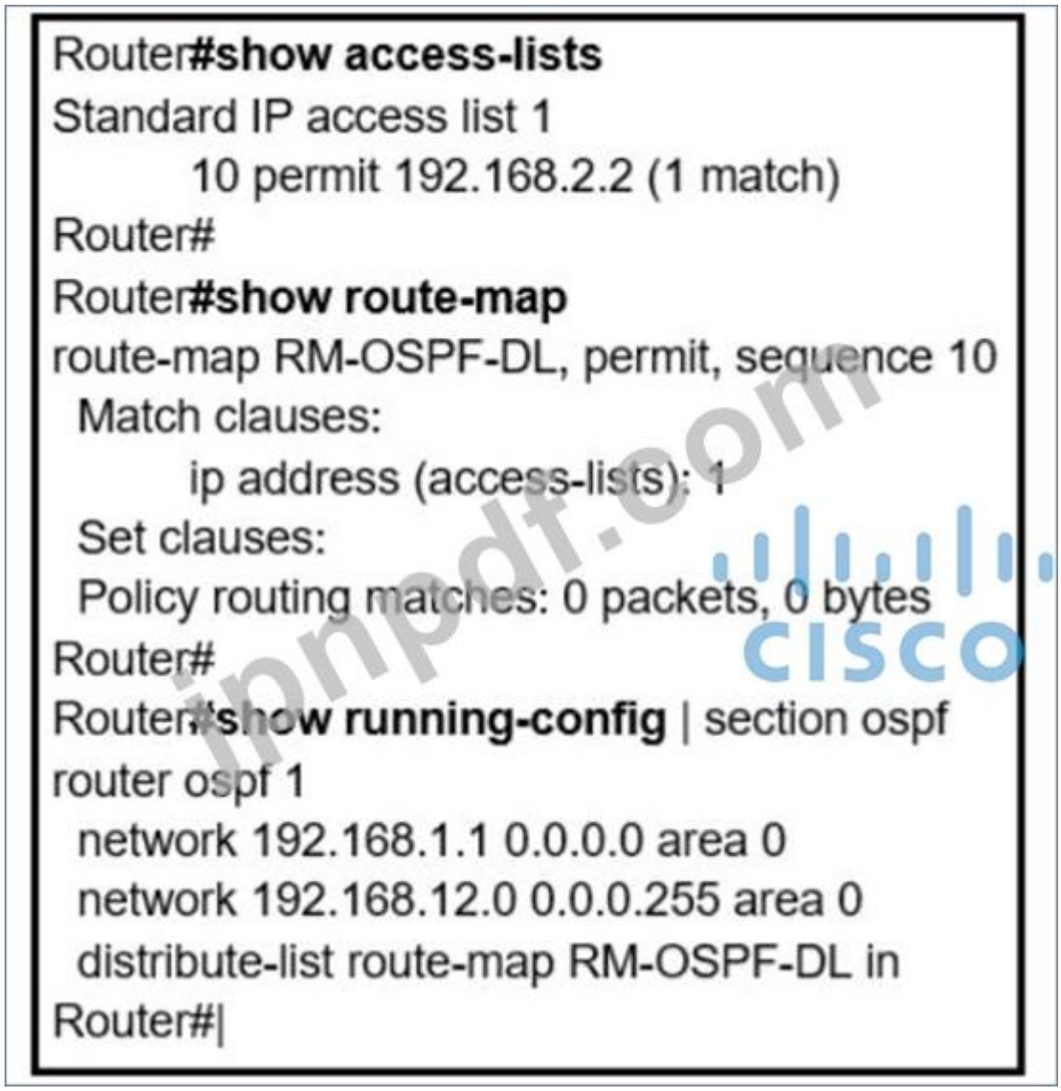
A. リンクにリンク ダンプニングを作成してセッションを保護します。

B. セッションを保護するために、リンク上の入力キューを増やします。

C. セッションを保護するためにターゲットを絞った hello を作成します。

D. セッションを保護するためにホールド タイマーを増やします。
E. セッションを保護するためにセッション遅延を増やします。
Answer: A,C (メーッセージを残す**)**
説明
LDP セッションを完全に再構築する必要を避けるために、LDP セッションを保護することができます。直接接続された 2 つの LSR 間のLDP セッションが保護されている場合、対象のLDP セッションが 2 つの LSR 間に構築されます。2 つの LSR 間で直接接続されたリンクがダウンした場合でも、2 つの LSR 間に代替パスが存在する限り、対象のLDP セッションは維持されます。
保護が機能するには、両方の LSR で保護を有効にする必要があります。これが不可能な場合は、一方の LSR でこれを有効にし、mpls ldp Discovery target-hello accept コマンドを設定することで、もう一方の LSR がターゲットのLDP Hello を受け入れることができます。

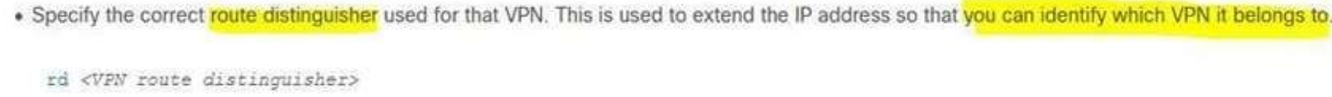
最新問題: **186**
展示を参照してください。



エンジニアは、示されている構成を使用して、ルーティング テーブルから 192.168.2.2 へのルートをブロックしようとしています。
このルートは、OSPF ルートとしてルーティング テーブルにまだ存在します。

どのアクションがルートをブロックしますか?
A. このステートメントをルート マップに追加します。route-map RM-OSPF-DLdeny 20
B. ルート マップでアクセス リストの代わりにプレフィックス リストを使用します。
C. ルート マップ コマンドのシーケンス 10 を許可から拒否に変更します。
D. 標準アクセス リストの代わりに拡張アクセス リストを使用します。
Answer: C (メーッセージを残す**)**

最新問題**: 187**
エンジニアがどの VPN に属しているかを識別できるように、IP アドレスを拡張するために MPLS VPN のどのコンポーネントが使用されますか?
A. VPNv4 アドレス ファミリ
B. RD
C. RT
D. 自民党
Answer: B (メーッセージを残す**)**



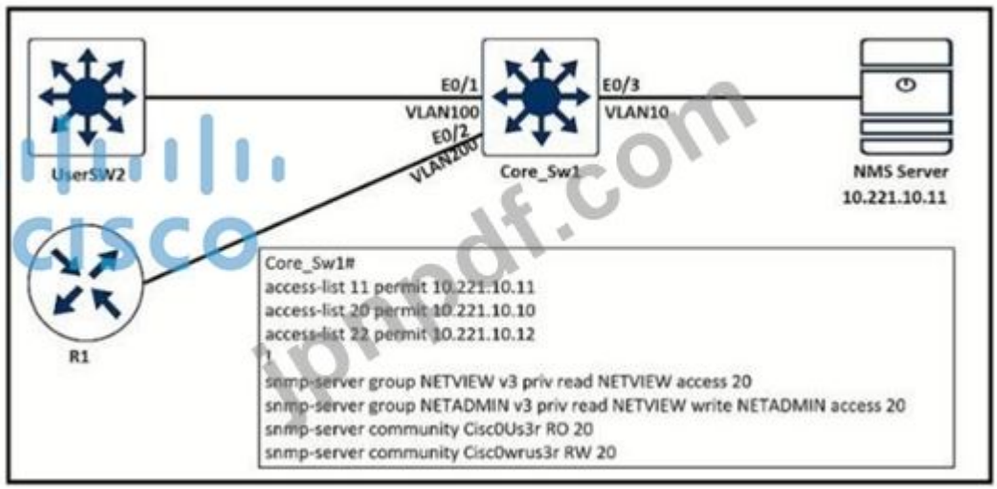
最新問題**: 188**
会社の所在地 407173257 での OSPF の再コンバージェンス時間を最適化するには、Hello タイマーとデッド タイマーを減らすよりも CPU の使用量が少ないどのメカニズムを選択する必要がありますか?
A. SSO
B. デッドピア検出キープアライブ
C. BFD
D. OSPF デマンド回路
Answer: C (メーッセージを残す**)**

最新問題**: 189**
展示を参照してください。この構成を適用するとどうなるでしょうか?

```
R1#show policy-map control-plane
 Control Plane
        Service-policy input: CoPP-BGP
         Class-map: BGP (match all)
          2716 packets, 172071 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: access-group name BGP
          drop

         Class-map: class-default (match-any)
          5212 packets, 655966 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: any
```

A. ルーターは他のデバイスと BGP 隣接関係を形成できます。
B. ルーターは他のデバイスと BGP ネイバーシップを形成できません。
C. ルータは、という名前のアクセス リストに一致するデバイスと BGP ネイバーシップを形成できません。
BGP」。
D. ルーターは、BGP」という名前のアクセス リストに一致する任意のデバイスと BGP ネイバーシップを形成できます。
Answer: A (メーッセージを残す**)**
セクション: レイヤ 3 テクノロジー

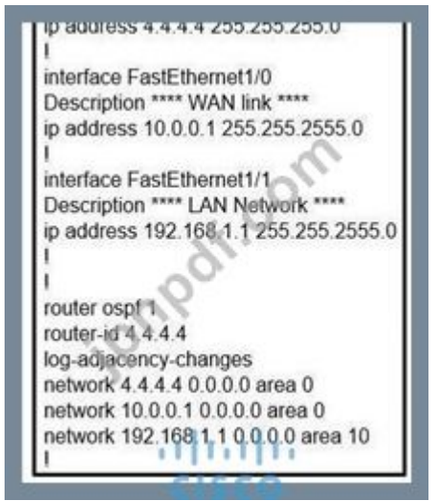
最新問題**: 190**
展示を参照してください。



エンジニアが Core_SW1 上で SNMP コミュニティを構成しましたが、SNMP サーバーは Core_SW1 から情報を取得できません。この問題はどの構成で解決されますか?
A. アクセスリスト 20 許可 10.221.10.12
B. SNMP サーバー グループ NETVIEW v2c priv 読み取り NETVIEW アクセス 20

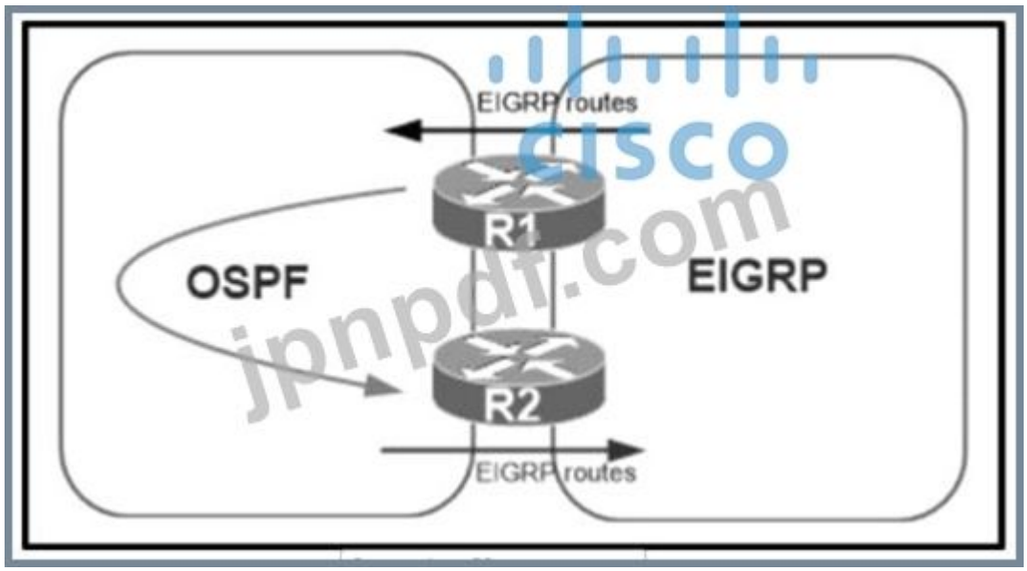
C. アクセスリスト 20 許可 10.221.10.11
D. SNMP サーバー グループ NETADMIN v3 priv 読み取り NETVIEW 書き込み NETADMIN アクセス 22
Answer: (解答を表示する**)**

最新問題**: 191**
展示を参照してください。



A)
```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf network broadcast
```
B)
```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf interface type network
```
C)
```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf network point-to-point
```
D)
```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf interface area 10
```
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**: 192**
展示を参照してください。



ネットワーク管理者が R1 ルーターと R2 ルーターで相互再配布を構成したため、ネットワークが不安定になりました。どのアクションで問題が解決しますか?

A. R1 上の OSPF に EIGRP を再配布するときに、ルート マップにタグを設定します。OSPF を EIGRP に再配布するときに許可するために、R2 上の同じタグと一致します。

B. EIGRP ネットワーク ルートのプレフィックス リストを R1 の OSPF ドメインに適用して、EIGRP ルーティング ドメインに伝播します。

C. R1 上の OSPF に EIGRP を再配布するときにルート マップにタグを設定し、OSPF を EIGRP に再配布するときに R2 上の同じタグと一致して拒否します。

D. EIGRP の要約ルートを OSPF にアドバタイズし、OSPF への再配布時に特定の EIGRP ルートを拒否します。

Answer: C (メーッセージを残す**)**

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html

最新問題**: 193**

展示を参照してください。

```
Router#show running-config | include ip route
ip route 192.168.2.2 255.255.255.255 209.165.200.225 130
Router#show ip route

<output omitted>

Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.1 is directly connected, Loopback0
      192.168.2.0/32 is subnetted, 1 subnets
O        192.168.2.2[110/11] via 192.168.12.2, 00:52:09, Ethernet0/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Ethernet0/0
L        192.168.12.1/32 is directly connected, Ethernet0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/24 is directly connected, Ethernet0/1
         209.165.200.226/32 is directly connected, Ethernet0/1
```

エンジニアはルーターに静的ルートを設定しますが、宛先へのルートを確認すると、別のネクストホップが選択されます。その理由は何でしょうか?

A. 静的ルートの構文が無効であるため、ルートは考慮されません。

スタティック ルートの AD は、OSPF ルーターの AD 110 よりも高い 130 に手動で設定されます。

B. スタティック ルートに設定された AD は、OSPF の AD よりも上位です。

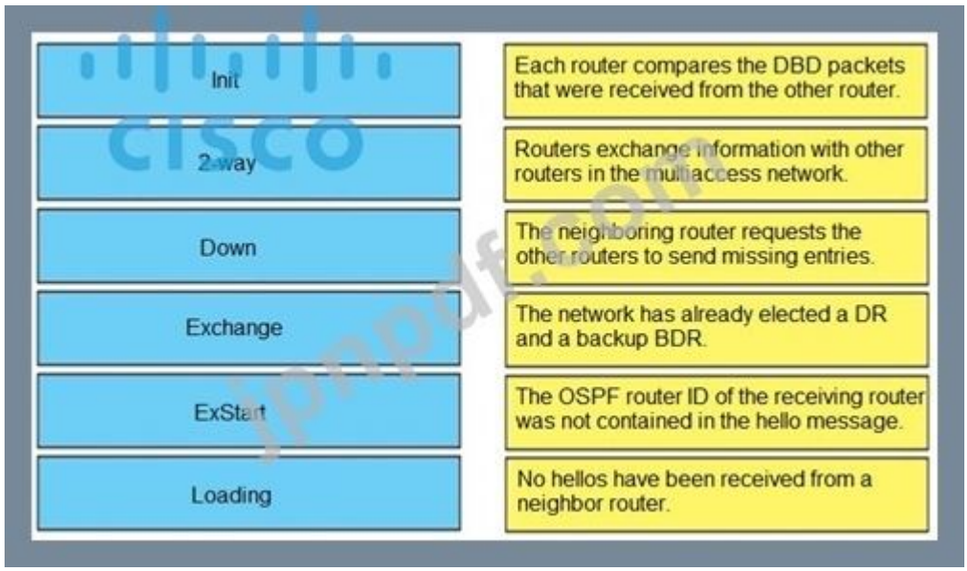
C. OSPF ルートのメトリックがスタティック ルートのメトリックよりも低いです。

D. 動的ルーティング プロトコルは常に静的ルートよりも優先されます。

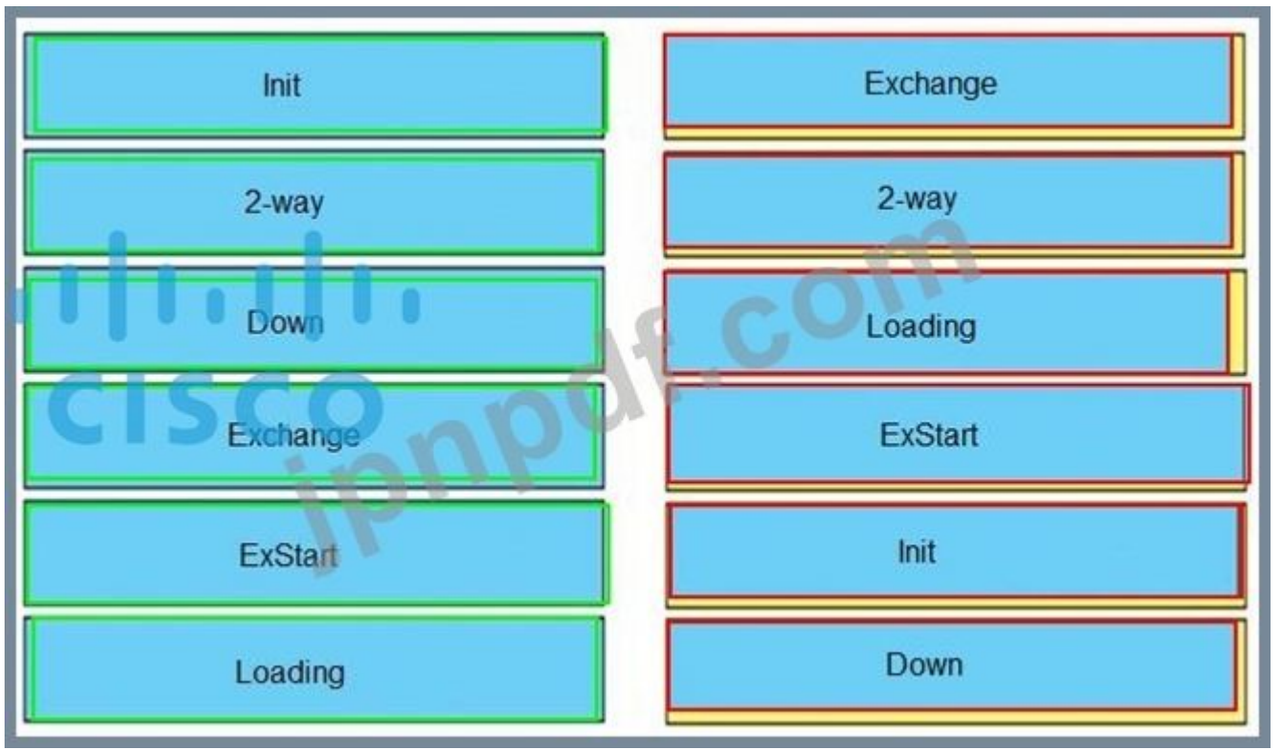
Answer: B (メーッセージを残す**)**

最新問題**: 194**

OSPF 隣接状態を左側から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: **195**

管理プレーン保護 (MPP) がサポートする 3 つのプロトコルまたはプロトコルの組み合わせはどれですか? (3つお選びください。)

A. SFTP

B. SSH

C. HTTP と HTTPS の両方

D. FTP

E. HTTP のみ

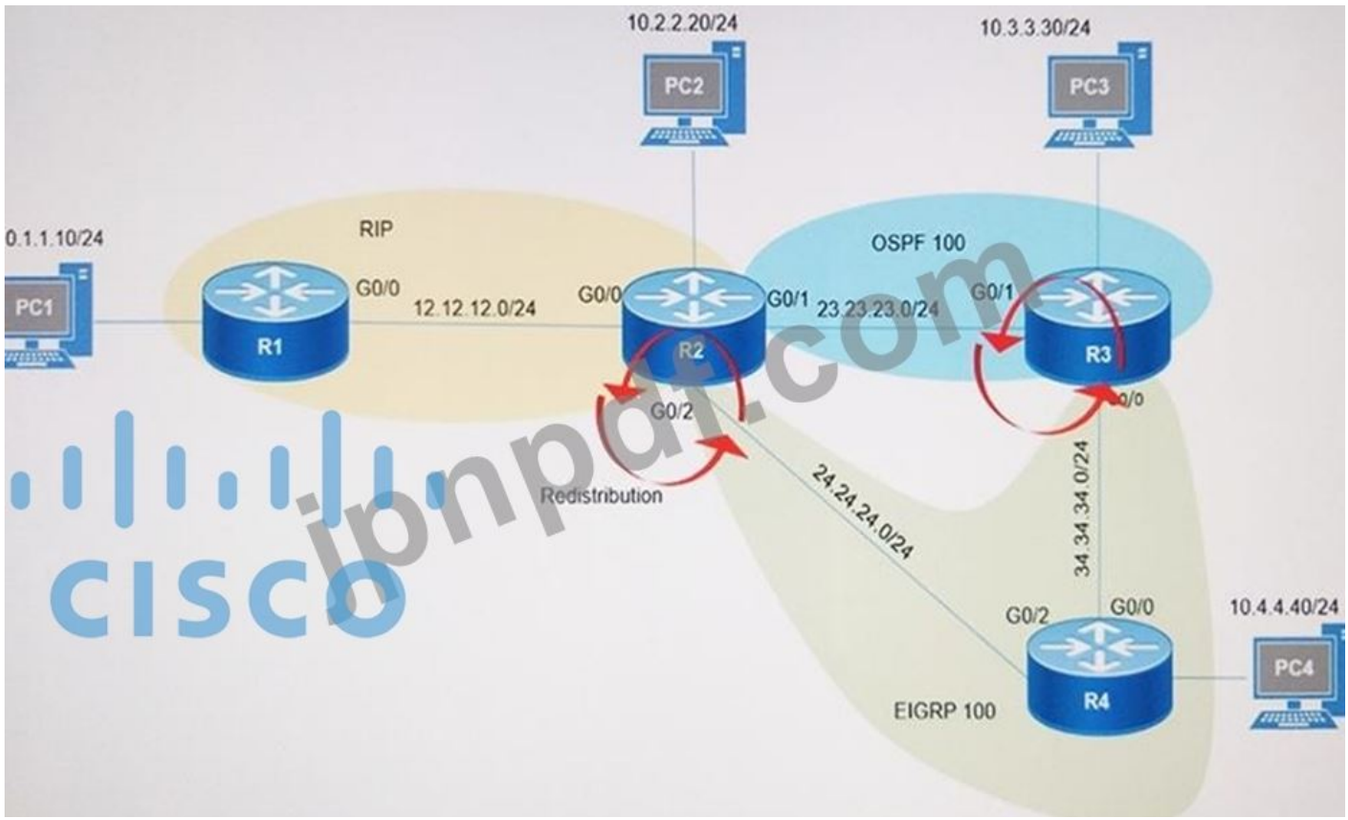
F. OSPF

Answer: B,C,D (メーッセージを残す)

現在、MPP は、TFTP、Telnet、Simple Network Management Protocol (SNMP)、Secure Shell (SSH)、HTTP などのプロトコルの受信管理要求のみを制御します。
MPP 機能がサポートする管理プロトコルは次のとおりです。これらの管理プロトコルは、MPP が有効になっている場合に影響を受ける唯一のプロトコルでもあります。
Extensible Exchange Protocol (BEEP) をブロックします
FTP
HTTP
HTTPS
SSH、v1 および v2
SNMP、すべてのバージョン
Telnet
TFTP
参照: https://www.cisco.com/c/en/us/td/docs/ios/security/configuration/guide/sec_mgmt_plane_prot.html

最新問題: **196**
障害が発生したプライマリ RP をセカンダリ RP が引き継ぐ場合、MPLS フォワーディング ステートを回復できるコントロール プレーン プロセスはどれですか?
A. LDP は SSO を使用してコントロール プレーン サービスの中断から回復します
B. LSP は NSF を使用して中断から回復します *i コントロール プレーン サービス
C. FEC はコントロール プレーン サービスを使用して、プライマリ プロセッサとセカンダリ プロセッサ間で情報を配布します。
D. MP-BGP は、MPLS 転送テーブルのラベル プレフィックス バインディングにコントロール プレーン サービスを使用します。
Answer: C (メーッセージを残す**)**

最新問題: **197**
展示を参照してください。



ルーティング プロトコル間で再配布が有効になった後。PC2、PC3、および PC4 は PC1 に到達できません。すべての PC にアクセスできるように問題を解決するために、エンジニアはどのようなアクションを実行できますか?

A. RIP から EIGRP に再配布されるときに、プレフィックス 10.1.1.0/24 をフィルタリングします。

B. OSPF から EIGRP に再配布されるときにプレフィックス 10.1.1.0/24 をフィルタリングします。

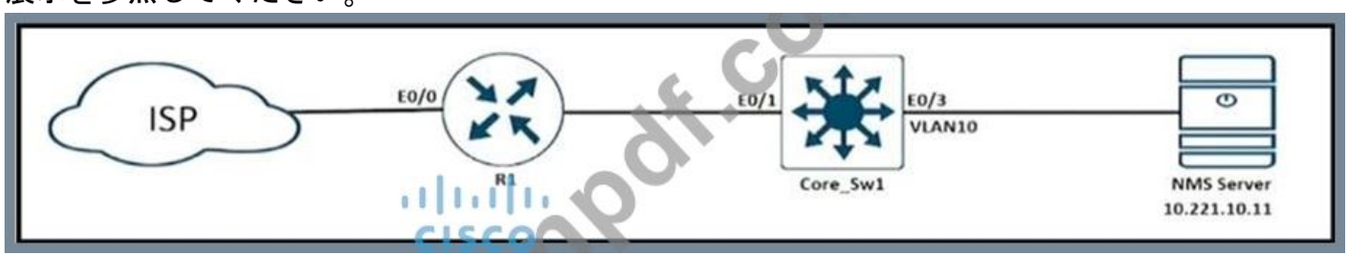
C. R2 上で直接接続されたインターフェイスを再配布します。

D. R2 の RIP プロセスでアドミニストレーティブ ディスタンス 100 を設定します。

Answer: B (メーッセージを残す**)**

最新問題: **198**

展示を参照してください。



ISP ルーターのメンテナンス中、インターフェイスのフラッピングにより、ネットワークで多くのアラートが生成されました。R1 のどの構成が問題を解決しますか?

A. SNMP トラップのリンクステータスがありません

B. SNMP トラップ IP ドロップ率の確認

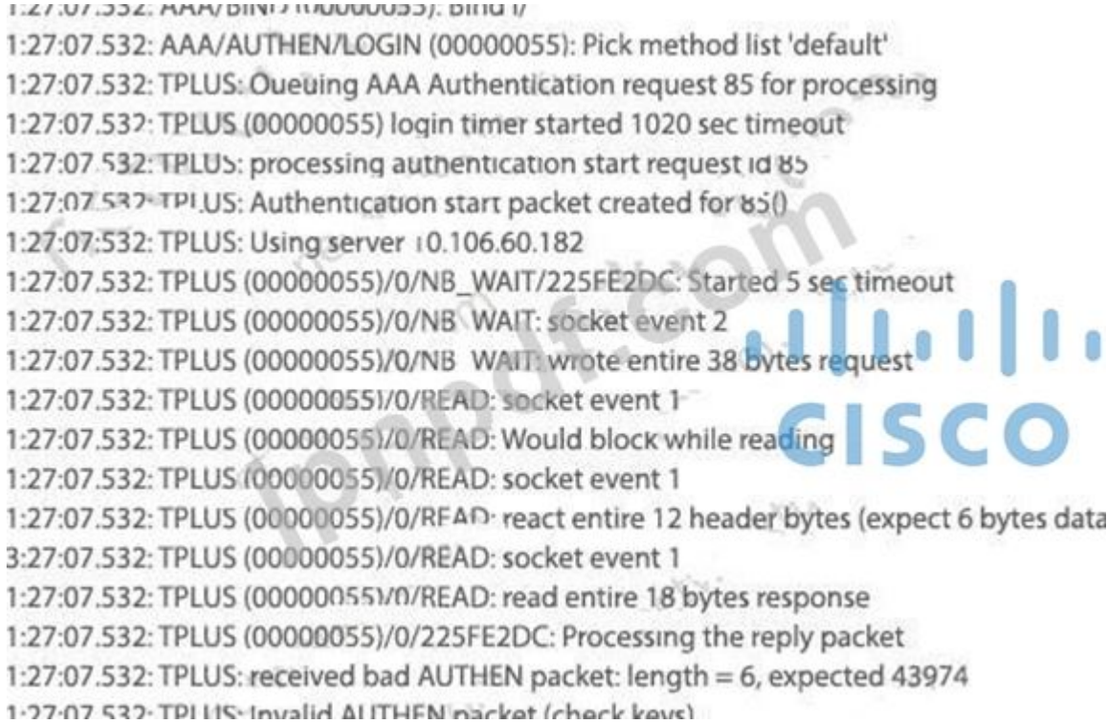
C. SNMP トラップのリンクステータスがダウンしています

D. ip verify ドロップレート通知ホールドダウン 60

Answer: (解答を表示する**)**

最新問題: **199**

展示する：



どのアクションが認証の問題を解決しますか?

A. TACACS+ サーバーでユーザー名を設定します。

B. TACACS+ サーバーで UDP ポート 1812 を許可するように設定します。

C. ルーターが到達できるように TCP ポート 49 を構成します。

D. TACACS+ サーバーとルーター間で同じパスワードを設定します。

Answer: (解答を表示する**)**

説明

出力の最後の行から、結果が 「無効な AUTHEN パケット」であることがわかります。したがって、ユーザー名またはパスワードに問題が発生しました。

最新問題: **200**

展示を参照してください。

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 2 name ISP2
```

管理者は、ISP1 に障害が発生したときに接続が ISP2 に切り替わらず、2 つの ISP 間でフラッピングしていることに気付きました。どのアクションで問題が解決しますか?

A. icmp-echo ステートメントに有効なsource-interface キーワードを含めます。

B. ISP1 ではなく ISP2 を介してデフォルト ルート上のトラック オブジェクト 1 を参照します。

C. ネクストホップと発信インターフェイスの両方を参照するように静的ルートを変更します。

D. ISP2 ルートのアドミニストレーティブ ディスタンスに一致するようにしきい値を変更します。

Answer: A (メーッセージを残す**)**

説明

https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-withdefault-routes-using-l.html

最新問題**: 201**

展示を参照してください。

```
Router#show access-lists
Standard IP access list 1
        10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, permit, sequence 10
  Match clauses:
        ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
  network 192.168.1.1 0.0.0.0 area 0
  network 192.168.12.0 0.0.0.255 area 0
  distribute-list route-map RM-OSPF-DL in
Router#|
```

エンジニアは、示されている構成を使用して、ルーティング テーブルから 192.168.2.2 へのルートをブロックしようとしています。ルートは OSPF ルートとしてルーティング テーブルにまだ存在します。ど

のアクションがルートをブロックしますか?

A. ルート マップでアクセス リストの代わりにプレフィックス リストを使用します。

B. 標準アクセス リストの代わりに拡張アクセス リストを使用します。

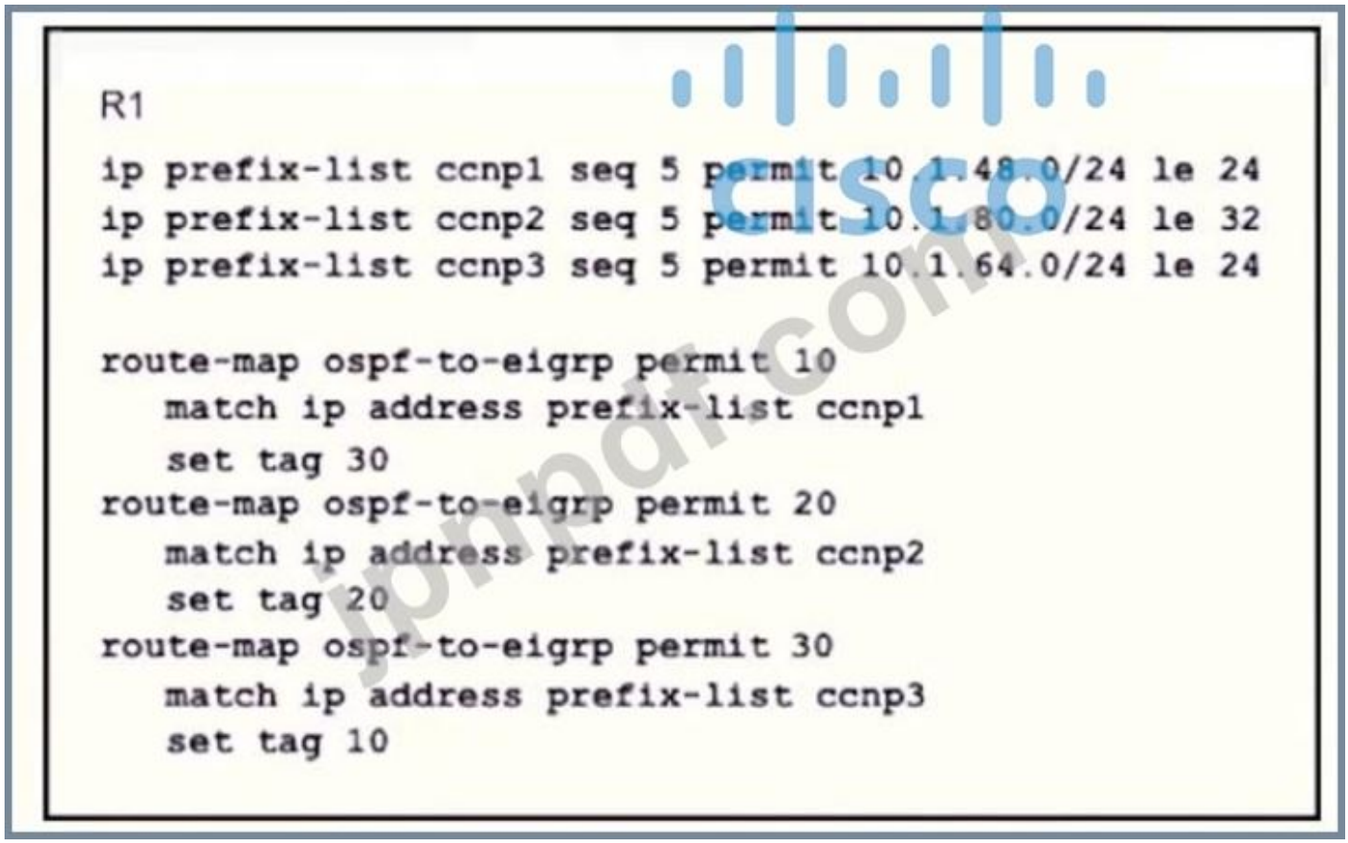
C. 次のステートメントをルート マップに追加します:route-map RM-OSPF-DLdeny 20。

D. ルート マップ コマンドのシーケンス 10 を許可から拒否に変更します。

Answer: D (メーッセージを残す**)**

最新問題**: 202**

展示を参照してください。



エンジニアはルート 10 1.80.65/32 に 30 のタグを設定しようとしましたが、失敗しました。問題はどのように修正されますか?

A. prefix-list ccnp3 を変更して 10.1.64.0/20 le 24 を追加します

B. プレフィックス リスト ccnp3 を変更して 10.1.64.0/20 ge 32 を追加します。

C. ルート マップ ospf-to-eigrp 許可 30 を変更し、プレフィックス リスト ccnp2 と一致します。

D. ルート マップ ospf-to-eigrp 許可 10 を変更し、プレフィックス リスト ccnp2 と一致します。

Answer: (解答を表示する**)**

最新問題**: 203**

展示を参照してください。

```
NY
router ospf 1
 network 192.168.12.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
!
interface E 0/0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 Cisco123
```

ネイバー関係が確立されていません 隣接関係が確立される 2 つの設定はどれですか? (2つお選びください)

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

最新問題: **204**

展示を参照してください。エンジニアは BGP を設定し、現在の最適パスではなく 10.77.255.57 からのパスを最適パスとして選択したいと考えています。どのアクションで問題が解決しますか?

A. 最適なパスとして選択されるように、より高い MED を構成します。

B. 現在の最適なパスの先頭に AS_PATH を追加するように構成します。

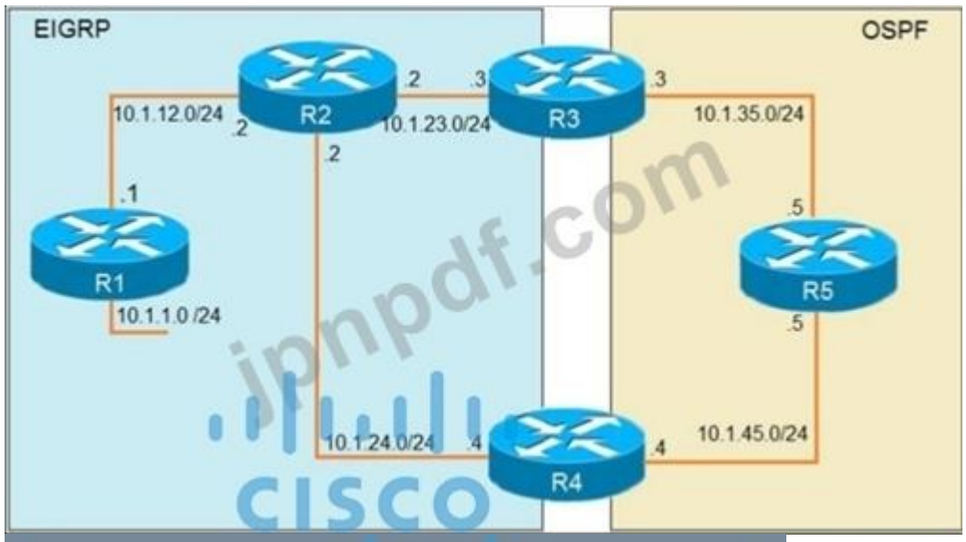
C. 必要な最適パスの先頭に AS_PATH を設定します。

D. 最適なパスとして選択されるように、下位の LOCAL_PREF を構成します。

Answer: B (メーッセージを残す**)**

最新問題**: 205**

展示を参照してください。




```
R1
router eigrp 1
 redistribute connected
 network 10.1.12.1 0.0.0.0

R3
router ospf 1
 redistribute eigrp 1 subnets
 network 10.1.35.3 0.0.0.0 area 0

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500
!
router ospf 1
 network 10.1.45.4 0.0.0.0 area 0

R5#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

 1 10.1.35.3 80 msec 44 msec 20 msec
 2 10.1.23.2 44 msec 104 msec 64 msec
 3 10.1.24.4 44 msec 64 msec 40 msec
 4 10.1.45.5 24 msec 40 msec 20 msec
 5 10.1.35.3 92 msec 144 msec 148 msec
 6 10.1.23.2 108 msec 76 msec 80 msec
        <output truncuated>
```

R5 からのトレースの出力には、ネットワーク内のループが示されています。
このループを防ぐ構成はどれですか?
A)

```
R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG deny 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
 match tag 1
```

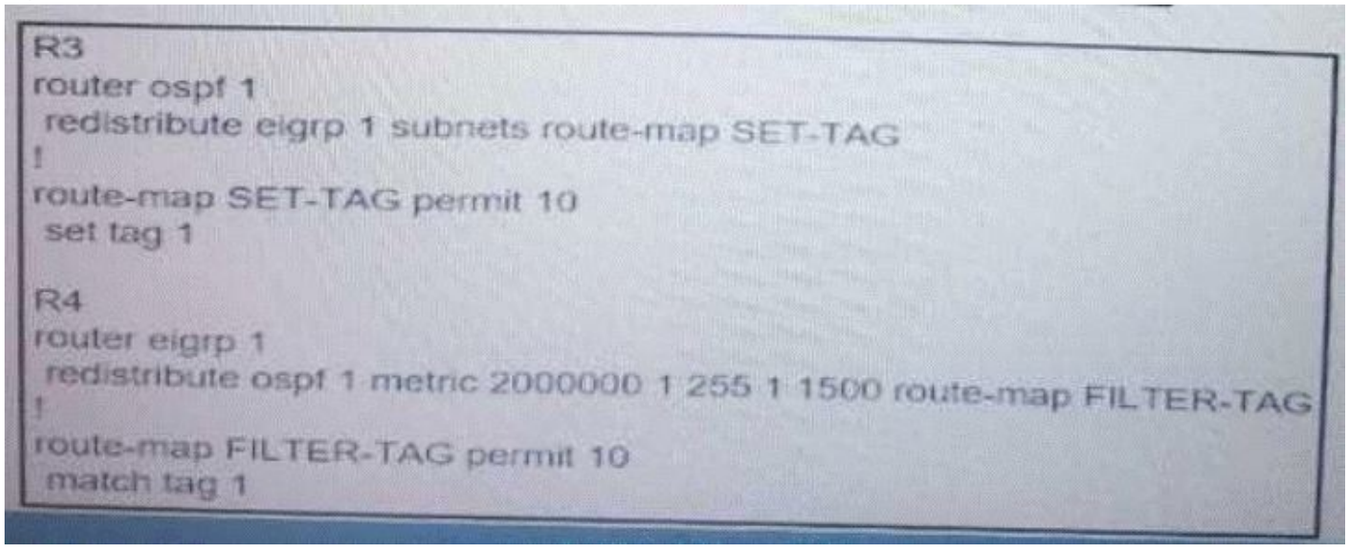
B)

```
R3
router eigrp 1
 redistribute OSPF 1 route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
 network 10.1.24.4 0.0.0.0
!
route-map FILTER-TAG deny 10
 match tag 1
!
route-map FILTER-TAG permit 20
```

C)

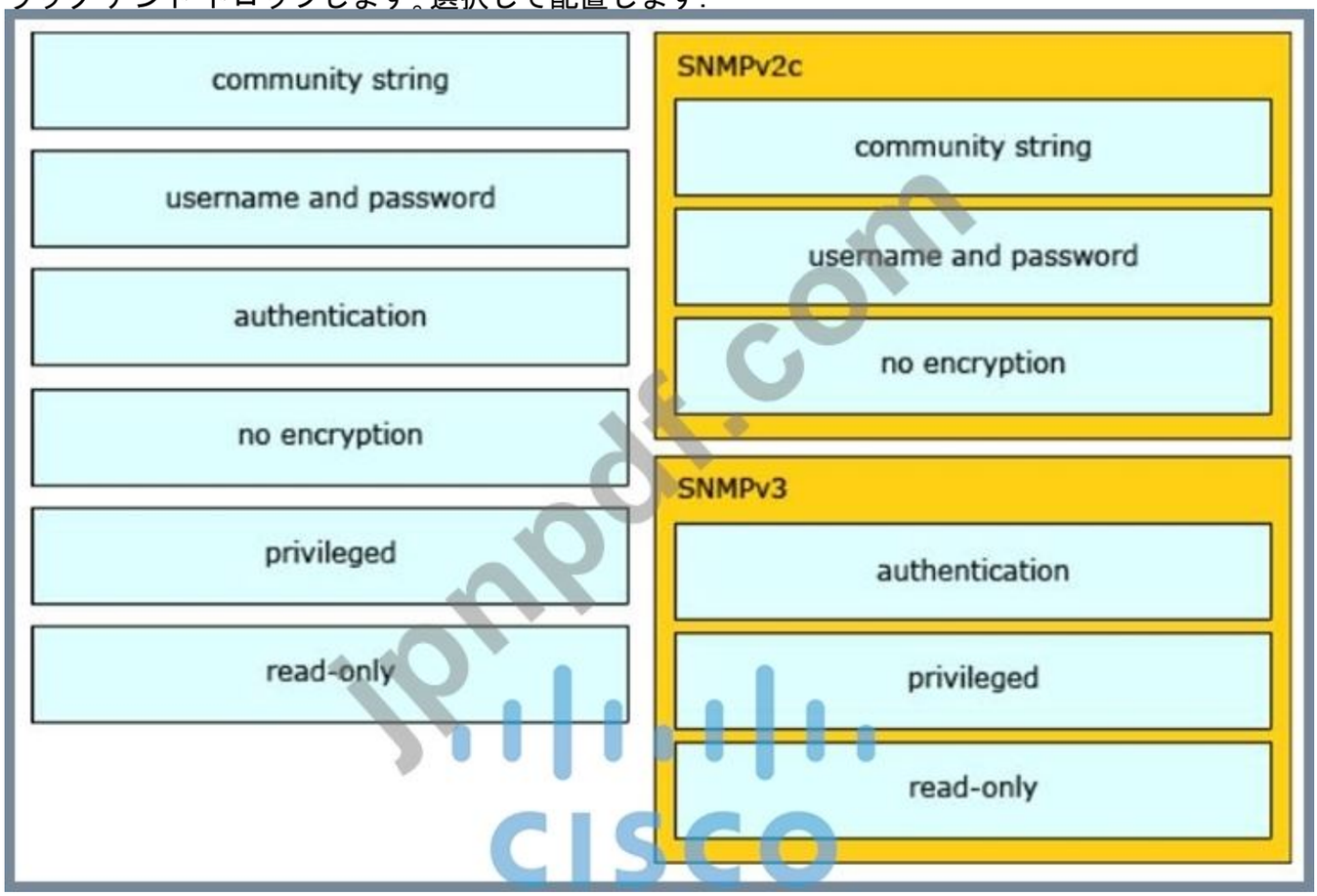
```
R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
 match tag 1
!
route-map FILTER-TAG permit 20
```

D)

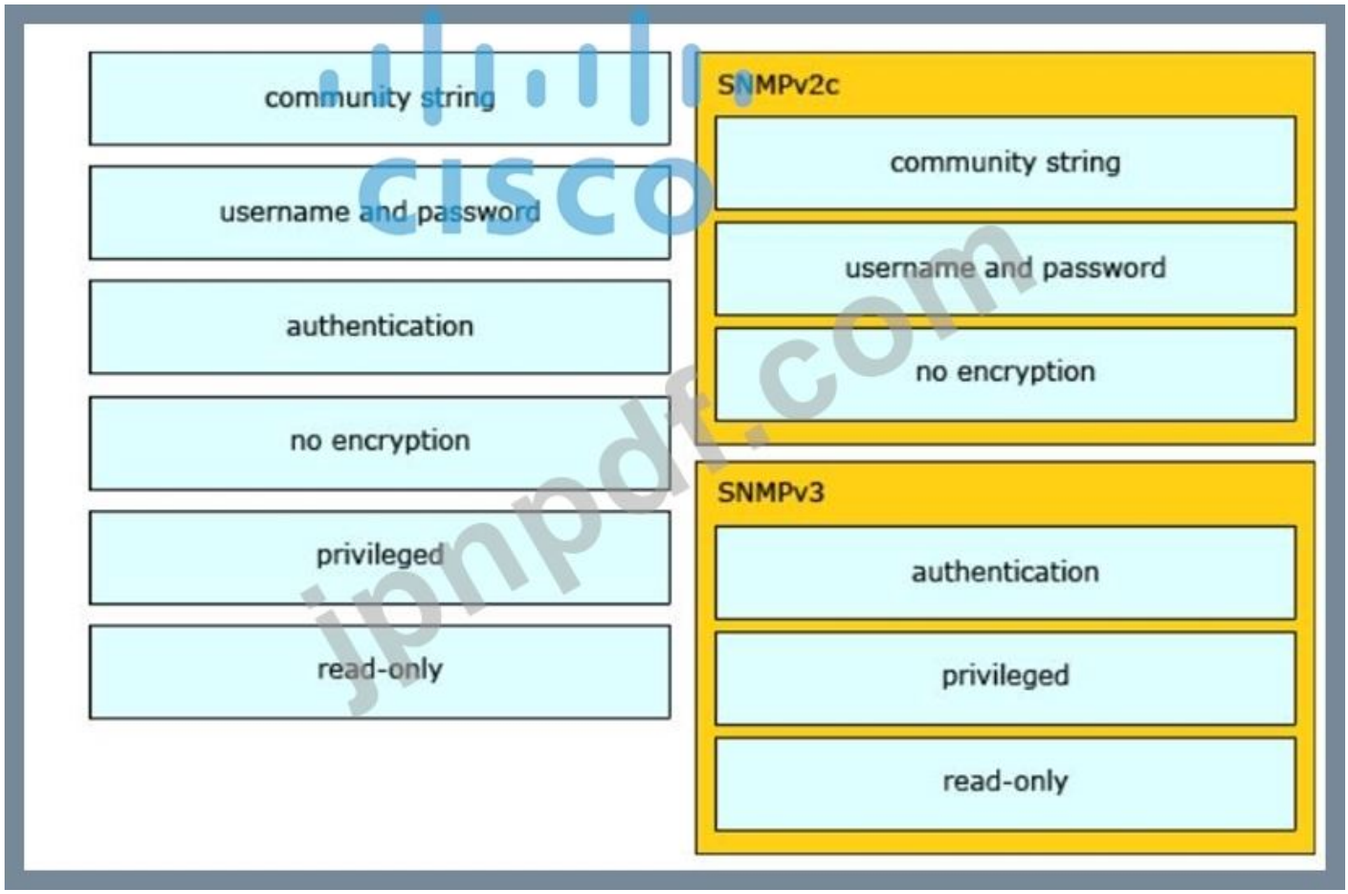


A. オプション C
B. オプション A
C. オプション D
D. オプション B
Answer: (解答を表示する**)**

最新問題**: 206**
Cisco IOS デバイスの SNMP 属性を左側から右側の適切な SNMPv2c または SNMPV3 カテゴリにドラッグ アンド ドロップします。選択して配置します:



Answer:



最新問題: **207**

展示を参照してください。

IT スタッフ メンバーが通常の営業時間内にオフィスに出社しましたが、SSH 経由でデバイスにアクセスできません。この問題を解決するにはどのようなアクションを実行する必要がありますか?

A. 正しい IP アドレスを使用するようにアクセス リストを変更します。

B. 正しい時間範囲を設定します。

C. アクセス リストを変更してサブネット マスクを修正します。

D. アウトバウンド方向のアクセス リストを設定します。

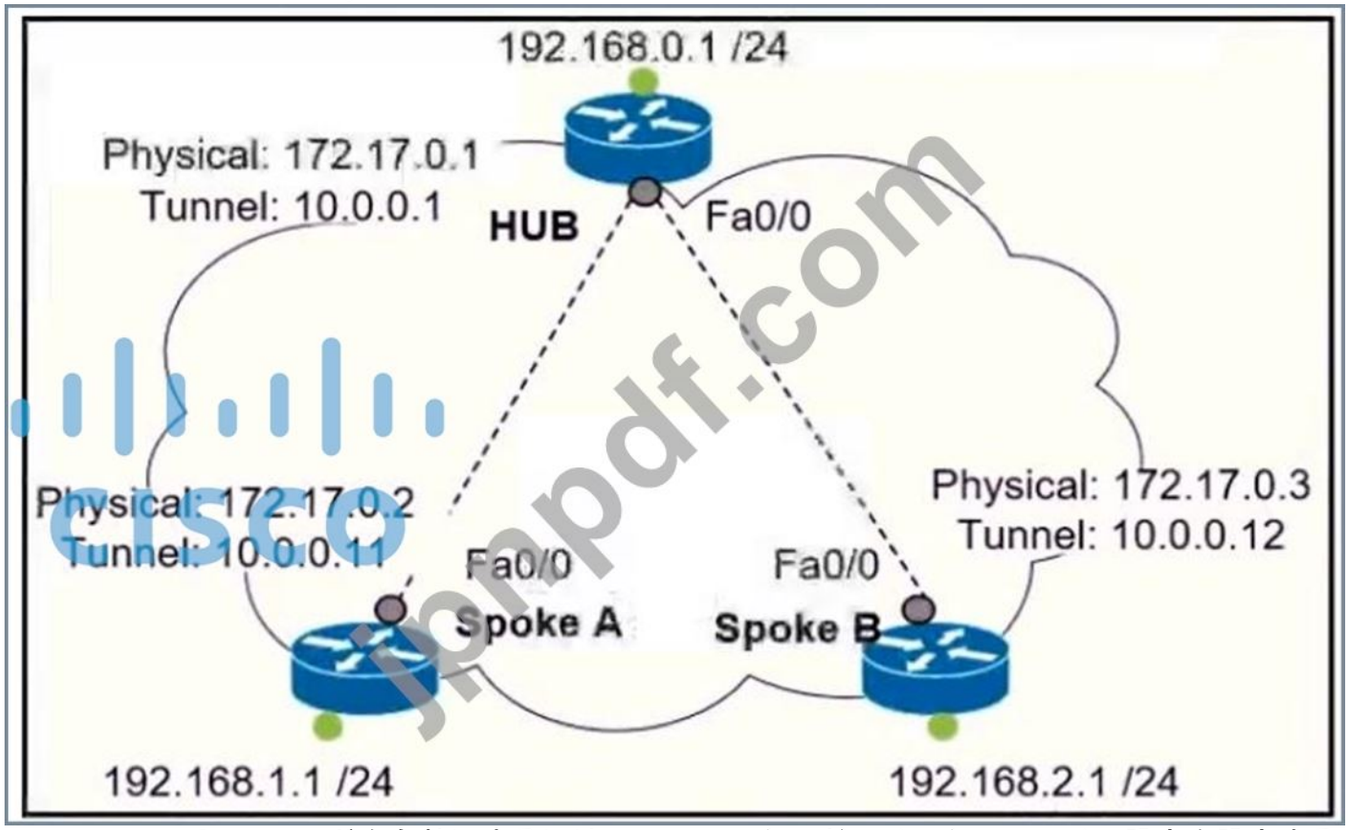
Answer: A (メーッセージを残す**)**

説明

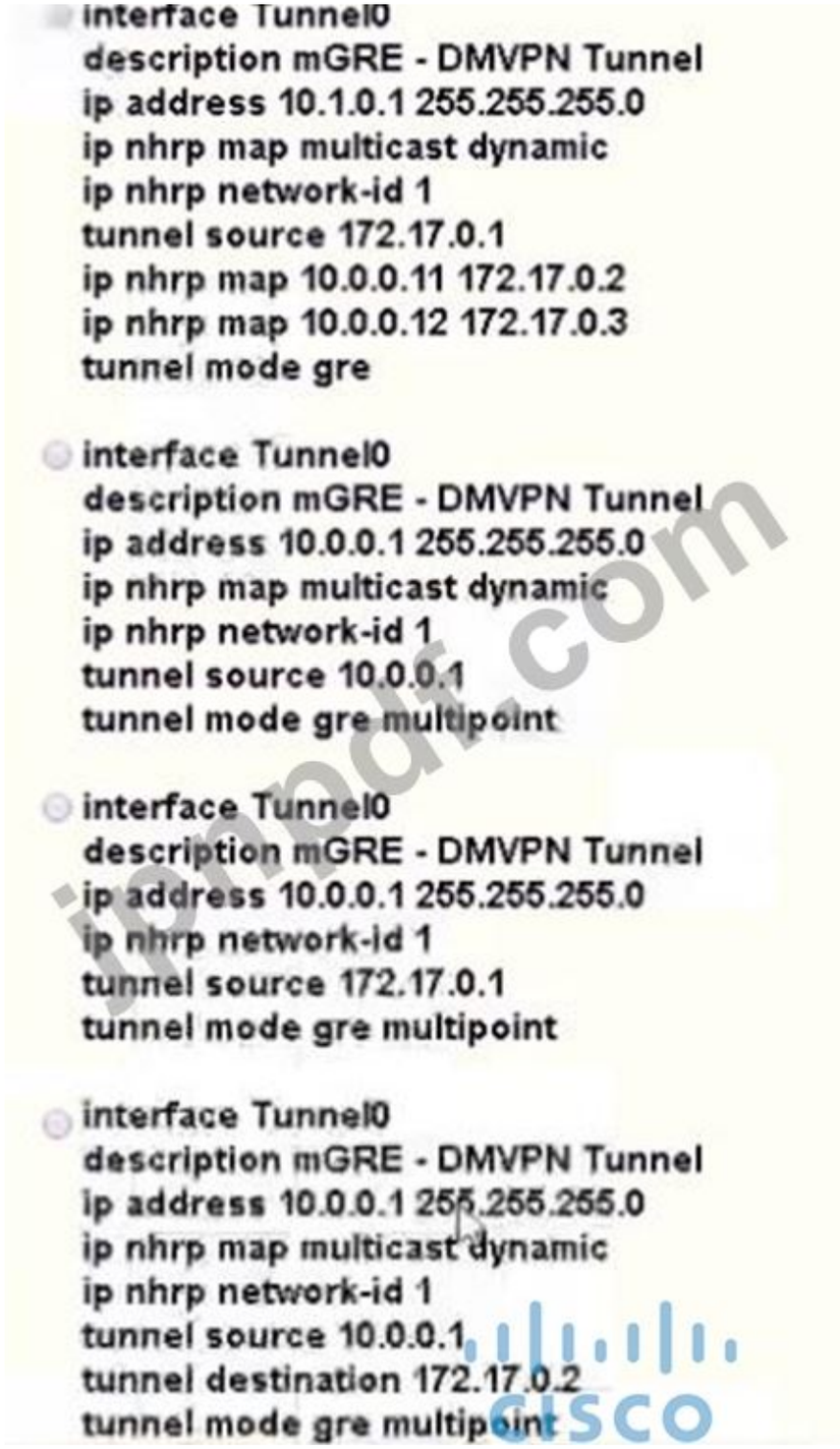
ACL には tcp 101 10.1.1.1 0.0.0.0 を許可する必要があります

最新問題: **208**

展示を参照してください。



MVPN with mGRE モードを有効にするには、HUB ルータでどのインターフェイス設定を設定する必要がありますか?



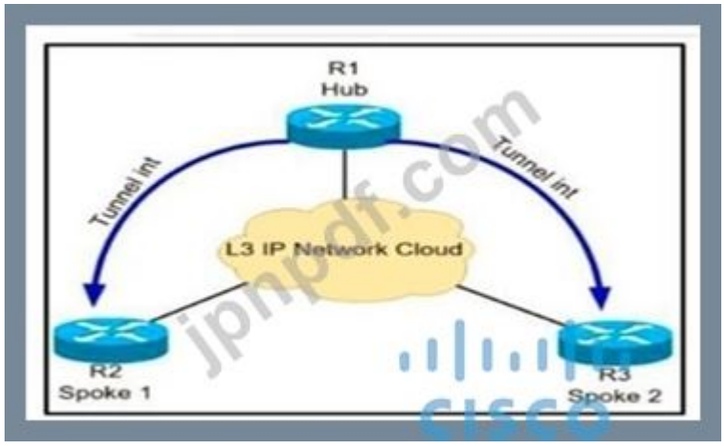
A. オプション A
B. オプション B
C. オプション C
D. オプション D

Answer: C (メーッセージを残す**)**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15 -mt/sec-conn-dmvpn-15-mt-book/sec-conn- dmvpn-dmvpn.html

最新問題: **209**

別紙を参照してください。
ネットワーク管理者は、ハブと 2 つのスポーク ルータの間に DMVPN トポロジを正常に設定しました。ハブを経由せずにスポーク 1 とスポーク 2 の間の直接通信を確立する必要がある 2 つのコンフィギュレーション コマンドはどれですか? (2 つ選択してください)。



A. ハブ ルータで、ip nhrp ショートカット コマンドを設定します。
B. スポーク ルータで、ip nhrp speech-tunnel コマンドを設定します。
C. ハブ ルーターで、ip nhrp redirect コマンドを設定します。
D. スポーク ルータで、ip nhrp ショートカット コマンドを設定します。
E. ハブ ルータで、tne Ip nhrp speech-tunnel コマンドを設定します。
Answer: C,D (メーッセージを残す)
説明
スポークツースポーク通信を設定するには、DMVPN フェーズ II またはフェーズ III を設定します。しかし、フェーズ II では、最初の数パケットがハブを通過します。ハブを完全に無視するには、DMVPN フェーズ III を使用する必要があります。
DMVPN フェーズ III はフェーズ 2 と同じですが、フェーズ 2 のいくつかの制限と複雑さが取り除かれています。また、使用する DMVPN ネットワーク設計の多様性が高まります。+ ハブの ip nhrp リダイレクト: 発信側スポークに、宛先スポークへのより適切なパスを探すように指示します。ハブ経由よりも。NHRP リダイレクト メッセージを受信すると、スポークはハブ経由で相互に通信し、送信した NHRP 解決要求に対する NHRP 応答を受け取ります。スポーク内の + ip nhrp ショートカット :スポーク上の CEF テーブルを上書きします。基本的に、リモート スポーク ネットワークのネクストホップ値を、デフォルトの初期ハブトンネル IP アドレスから NHRP で解決されたリモート スポーク トンネル IP アドレスにオーバーライドします)

展示を参照してください。FTP クライアントがパッシブ FTP を使用して FTP サーバーに接続しようとすると、ファイル転送が失敗します。問題はどのアクションで解決されますか?

A. FTP-SERVER アクセス リストを変更して、最後に確立されたものを削除します。

B. 1023 を超える TCP ポートを許可するように構成します。

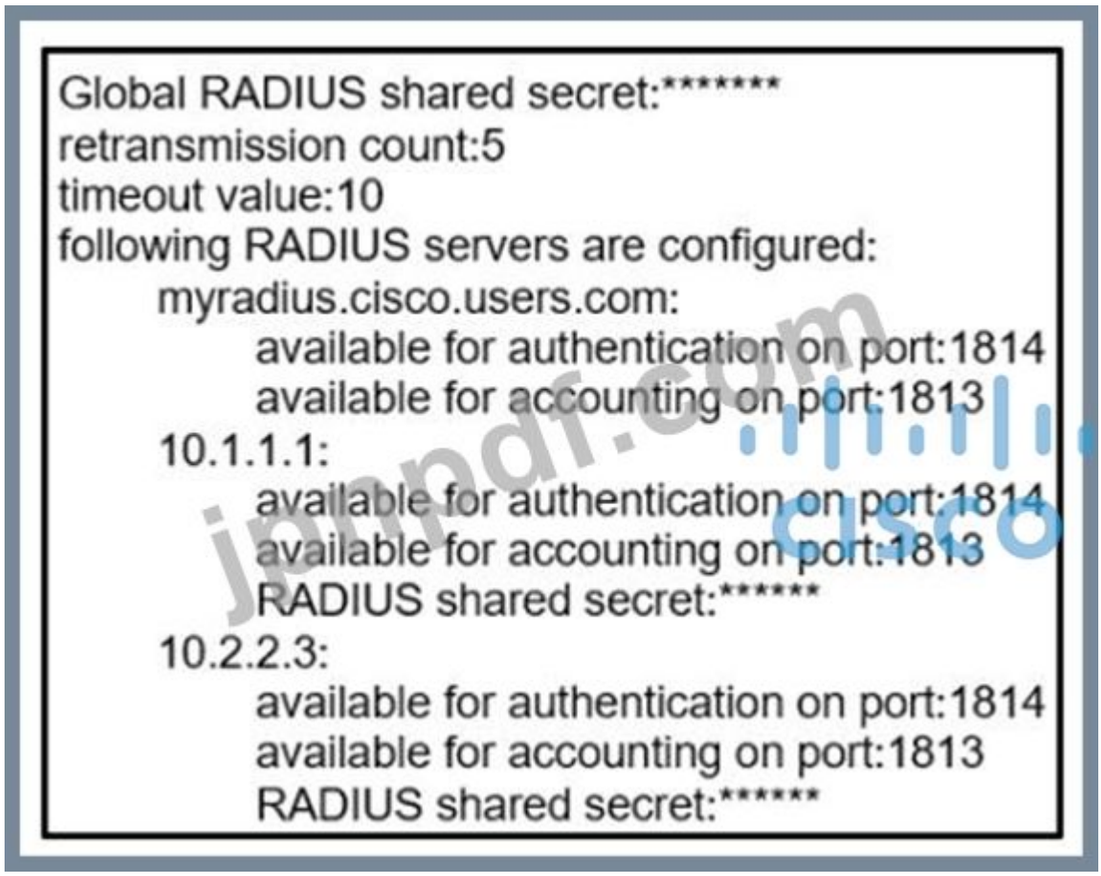
C. トラフィック フィルター FTP-SERVER をアウトバウンド方向に変更します。

D. アクティブな FTP トラフィックを構成します。

Answer: B (メーッセージを残す**)**

最新問題: **211**

展示を参照してください。



AAA サーバ 10.1.1.1 はデフォルトの認証およびアカウンティング設定で設定されていますが、スイッチはサーバと通信できません。この問題はどのアクションで解決しますか?

A. 認証ポートと一致します

B. アカウンティング ポートと一致します

C. タイムアウト値を修正します。

D. 共有秘密を修正します。

Answer: A (メーッセージを残す**)**

コマンドのデフォルト

アカウンティングポート: 1813

認証ポート: 1812

アカウンティング: 有効

認証: 有効

再送回数 :1回

アイドル時間: 0

サーバー監視: 無効

タイムアウト: 5秒

テストユーザー名: テスト

テストパスワード: テスト

参照 :

https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/radius-server-host.html

デフォルトでは、RADIUS は認証に UDP ポート 1812 を使用し、アカウンティングにポート 1813 を使用します。

上の図では、デフォルト ポートではない 10.1.1.1 の AAA サーバへの認証にポート 1814 が使用されていることがわかります。そのため、認証ポートをデフォルト値 1812 に調整する必要があります。

最新問題: **212**

IPv6 ファーストホップ セキュリティ機能を左側から右側の定義にドラッグ アンド ドロップします。

Answer:

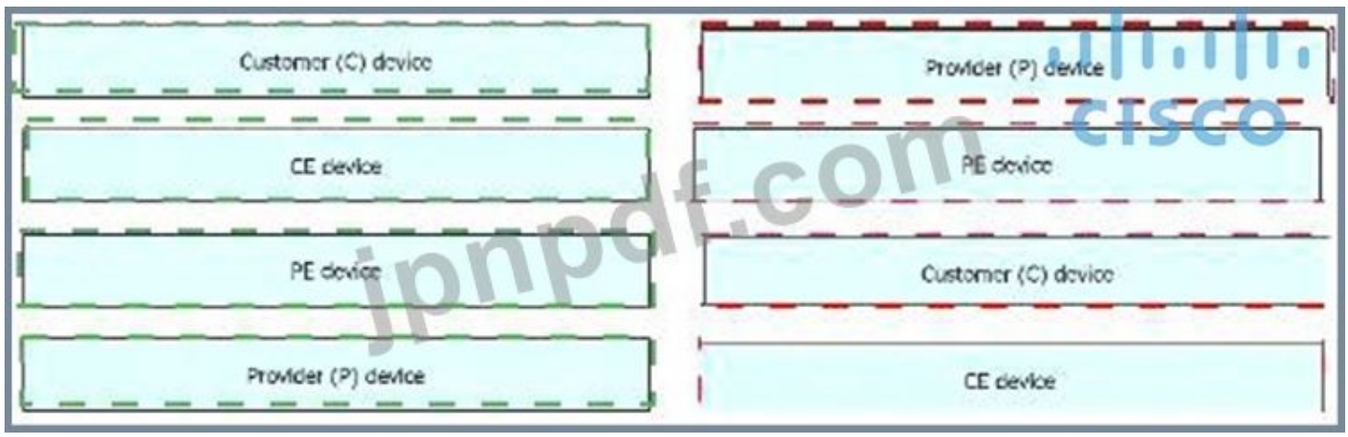
説明

グラフィカル ユーザー インターフェイス、チャートの説明が自動的に生成

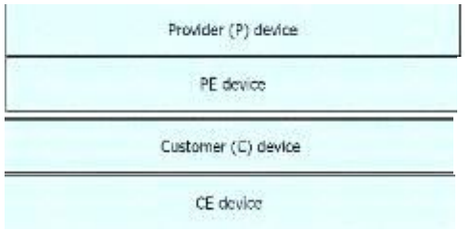
最新問題**: 213**

左側の MPLS VPN デバイス タイプを右側の定義にドラッグ アンド ドロップします。

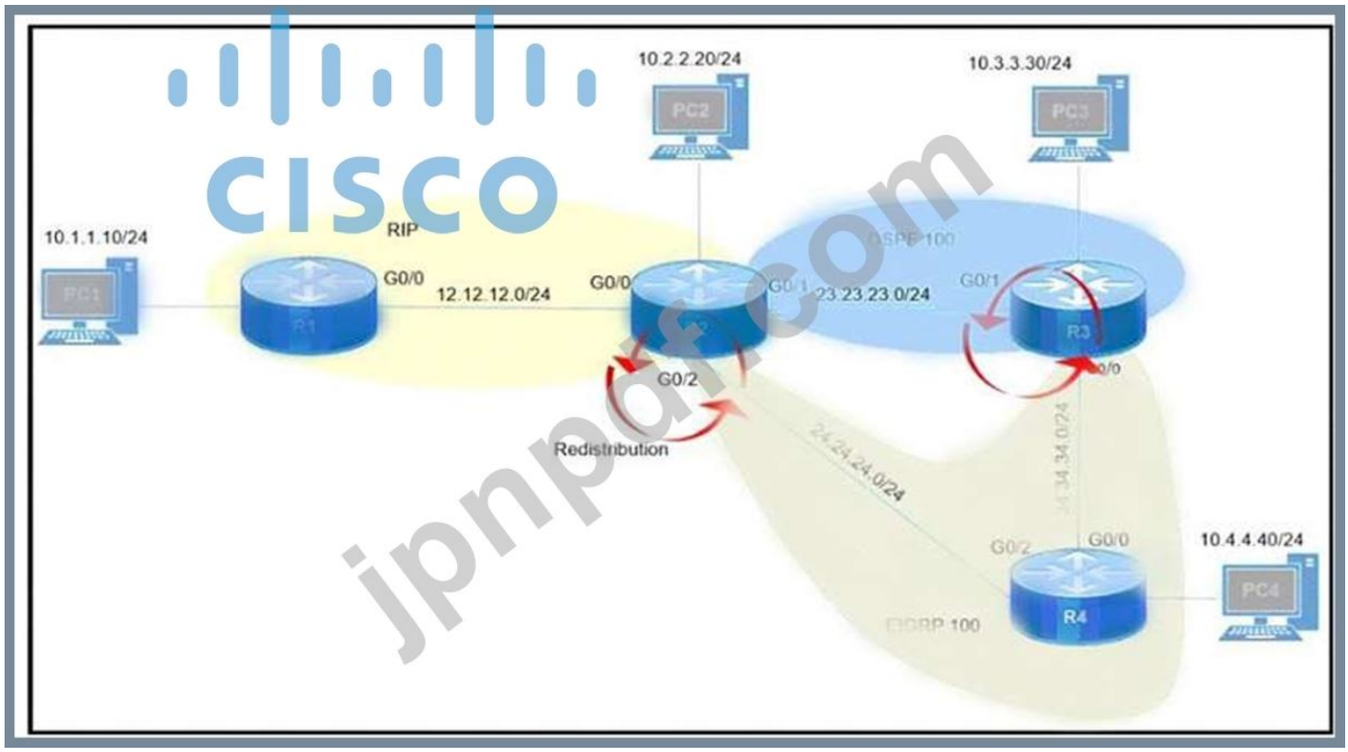
Answer:



説明

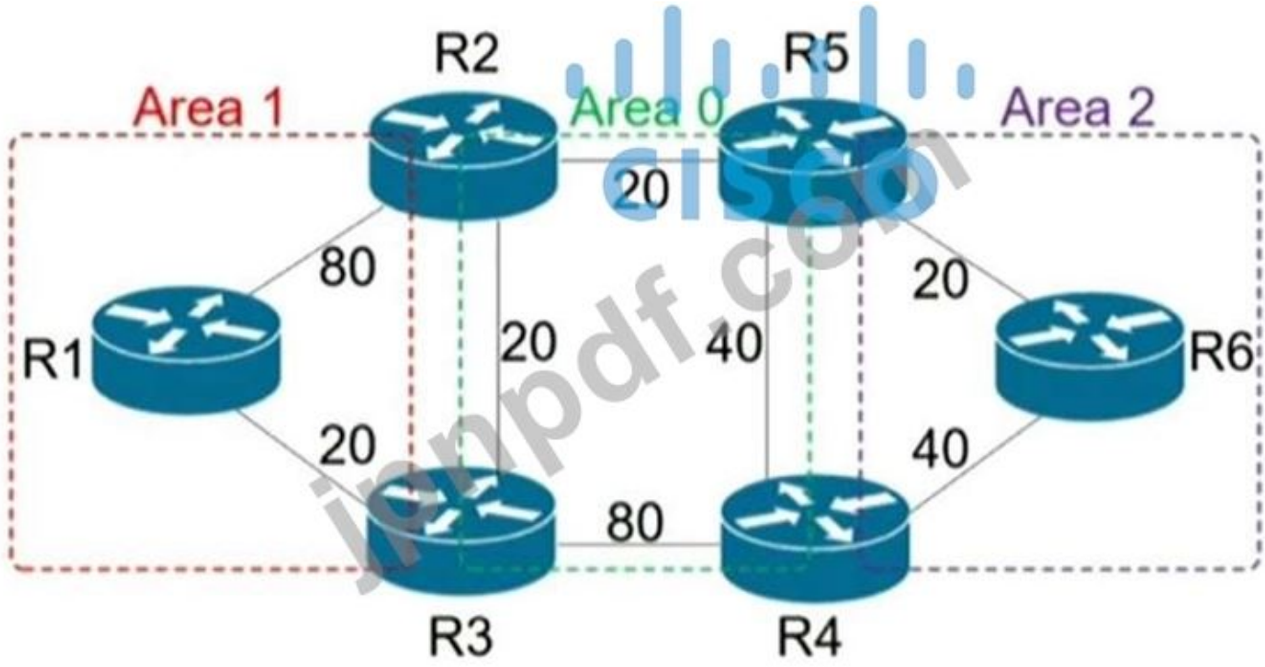


最新問題: **214**
展示を参照してください。



ルーティング プロトコル間で再配布が有効になっており、nowPC2、PC3、および PC4 は PC1 に到達できません。問題を解決する 2 つの解決策は何ですか? (2つお選びください。)
A. R2 の RIP に再配布するときに、RIP ルートをフィルタリングして RIP に戻します。
B. R2 の RIP に再配布するときに、OSPF ルートを EIGRP から RIP にフィルタリングします。
C. R2 の EIGRP に再配布するときに、RIP ルートを除くすべてのルートをフィルタリングします。
D. R2 の OSPF に再配布するときに、RIP および OSPF ルートをフィルタリングして EIGRP から OSPF に戻します。
E. R3 の OSPF に再配布するときに、EIGRP ルートを除くすべてのルートをフィルタリングします。
Answer: A,B (メーッセージを残す**)**
説明
PC2 ですら PC1 に到達できないため、R2 での RIP 再配布に問題があります。RIP は OSPF や EIGRP よりもアドミニストレーティブ ディスタンス (AD) 値が高いため、相互再配布を行うとループします。

最新問題: **215**
展示を参照してください。



R6 は、R5>R2>R1 を介して R1 に到達する必要があります。どのアクションで問題が解決しますか?

A. R2 と R3 の間のコストを 61 に増加します

B. R6-R5-R2 の間でコストを 2 に減らします。

C. R2-R3-R1 の間のコストを 61 に増加します

D. R2 と R1 の間のコストを 41 に減らします。

Answer: D (メーッセージを残す**)**

最新問題**: 216**

展示を参照してください。

```
*Sep 26 19:50:43.504: SNMP: Packet received via UDP from
192.168.1.2 on GigabitEthernet0/1SrParseV3SnmpMessage: No
matching Engine ID.

SrParseV3SnmpMessage: Failed.
SrDoSnmp: authentication failure, Unknown Engine ID

*Sep 26 19:50:43.504: SNMP: Report, reqid 29548, errstat 0,
erridx 0
internet.6.3.15.1.1.4.0 = 3
*Sep 26 19:50:43.508: SNMP: Packet sent via UDP to 192.168.1.2
process_mgmt_req_int: UDP packet being de-queued
```

問題を解決するために必要な情報を管理者に提供する 2 つのコマンドはどれですか? (2つお選びください。)

A. SNMP ユーザーを表示
B. デバッグ SNMP エンジン ID
C. デバッグ snmpv3 エンジン ID
D. SNMP パケットをデバッグします
E. nmpv3 ユーザーを示します
Answer: A,D (メーッセージを残す**)**
SNMPv3 ヘッダーには、通信を行うために一致する必要がある 3 つの
値、snmpEngineID、snmpEngineTime、snmpEngineBoots があります。受信したエラーは、EngineID 値に問題があることを示しています: 認証失敗、不明なエンジン ID」エンジン ID を指定するには、「show snmp user」コマンドを使用できます。次の例では、ユーザー名を abcd、エンジン ID: 00000090200000000C025808 として指定します。

「debug snmp packet」コマンドは、到着および応答中のすべての SNMP パケットを表示します。

最新問題**: 217**
エンジニアは、インストール中に Cisco DNA center エンタープライズ インターフェイスに対して間違ったデフォルト ゲートウェイを設定しました。
構成を修正するためにエンジニアはどのコマンドを実行する必要がありますか?
A. Sudi アップデート構成のインストール
B. Sudo magiev-config の更新
C. Sudo maglev インストール構成の更新
D. Sudo maglev の再インストール
Answer: B (メーッセージを残す**)**

最新問題**: 218**
エンジニアは、ルートに影響を与えるポリシーで非シスコのアクセス リストを設定しました

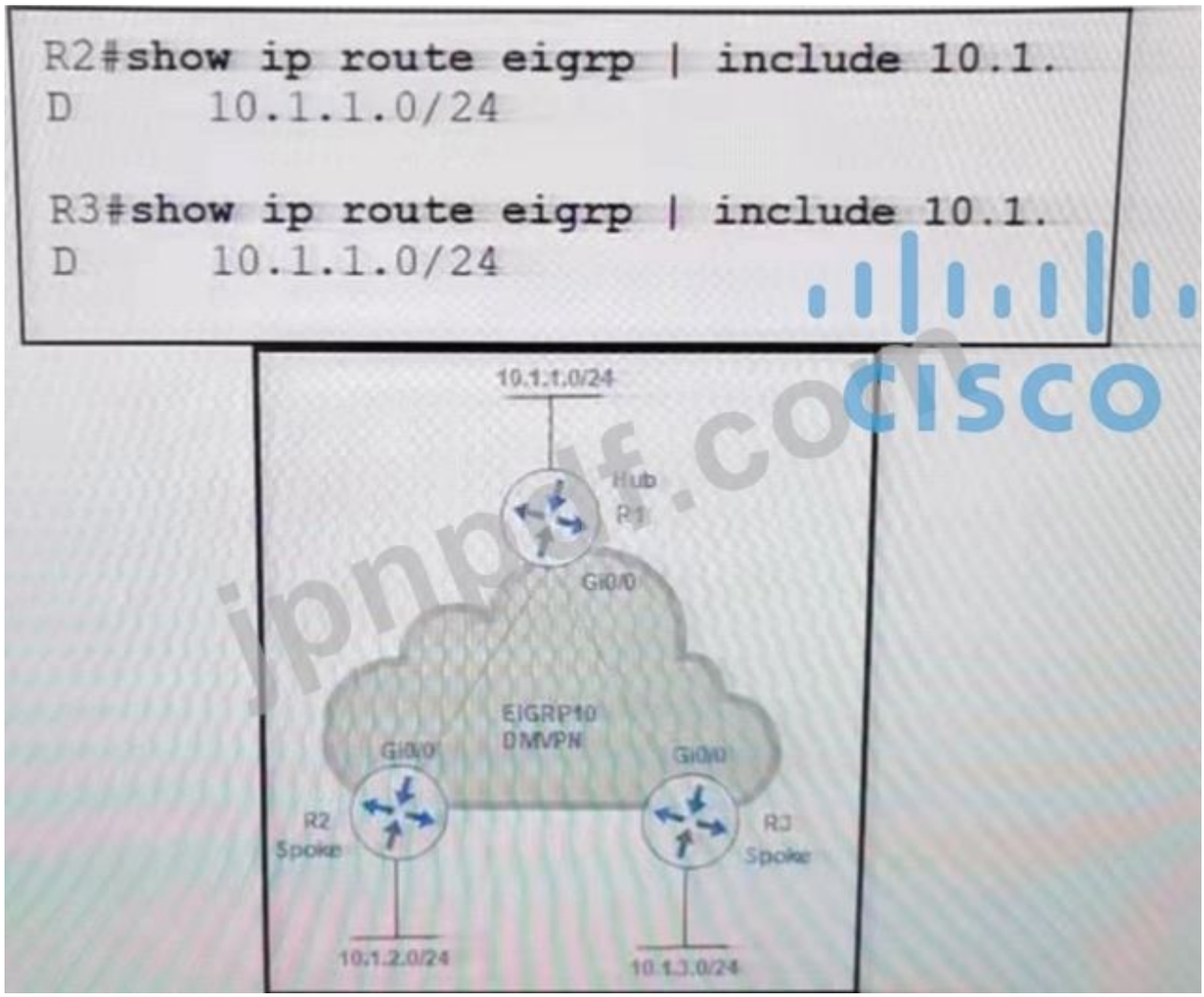
このルート マップ設定の 2 つの効果は何ですか? (2つお選びください。)

A. パケットはシーケンス 10 によって評価されません。
B. パケットはシーケンス 10 によって評価されます。
C. パケットはデフォルト ゲートウェイに転送されます。
D. パケットは通常のルート検索を使用して転送されます。
E. パケットはアクセス リストによってドロップされます。
Answer: B,C (メーッセージを残す**)**
説明
https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds-ce.html

最新問題**: 219**
展示を参照してください。

ACL は、ルータの受信ギガビット 0/1 インターフェイスに配置されます。ホスト
フローが許可されている場合でも、192.168.10.10 はホスト 192.168.100.10 に SSH 接続できません。このルーターへのフルアクセスを開かずに問題を解決するアクションはどれですか?
A. show access-list FILTER コマンドを実行して、SSH エントリに関連するヒット統計があるかどうかを表示します。
B. インターフェイスから ACL を一時的に削除して、フローが機能するかどうかを確認します。
C. SSH エントリを ACL の先頭に移動します
D. フローが機能するかどうかを確認するために、permit ip any any 行を ACL の先頭に一時的に移動します。
Answer: C (メーッセージを残す**)**

最新問題**: 220**
展示を参照してください。



エンジニアが DMVPN を設定し、R2 および R3 でハブ ロケーション プレフィックス 10.1.1.0724 を受信します。R3 プレフィックス 10 1.3.0/24 は R2 では受信されません。R2 プレフィックス 10.1,2.0/24 は R3 で受信されません。どのアクションが問題を留保しますか?

A. スプリット ホライズンにより、スポーク ルータ間でルートがアドバタイズされなくなります。これは、R1 のトンネル インターフェイスでコマンド no ip split-horizon eigrp 10 を使用して無効にする必要があります。

B. スポークツースポーク接続がありません。DMVPN 設定を変更して、R2 と R3 間のトンネル接続と、show ip eigrp neighbors コマンドを使用して確認したネイバー関係を有効にする必要があります。

C. スプリット ホライズンにより、スポーク ルータ間でルートがアドバタイズされなくなります。これは、R1 の Gi0/0 インターフェイスで no ip split-horizon eigrp 10 コマンドを使用して無効にする必要があります。

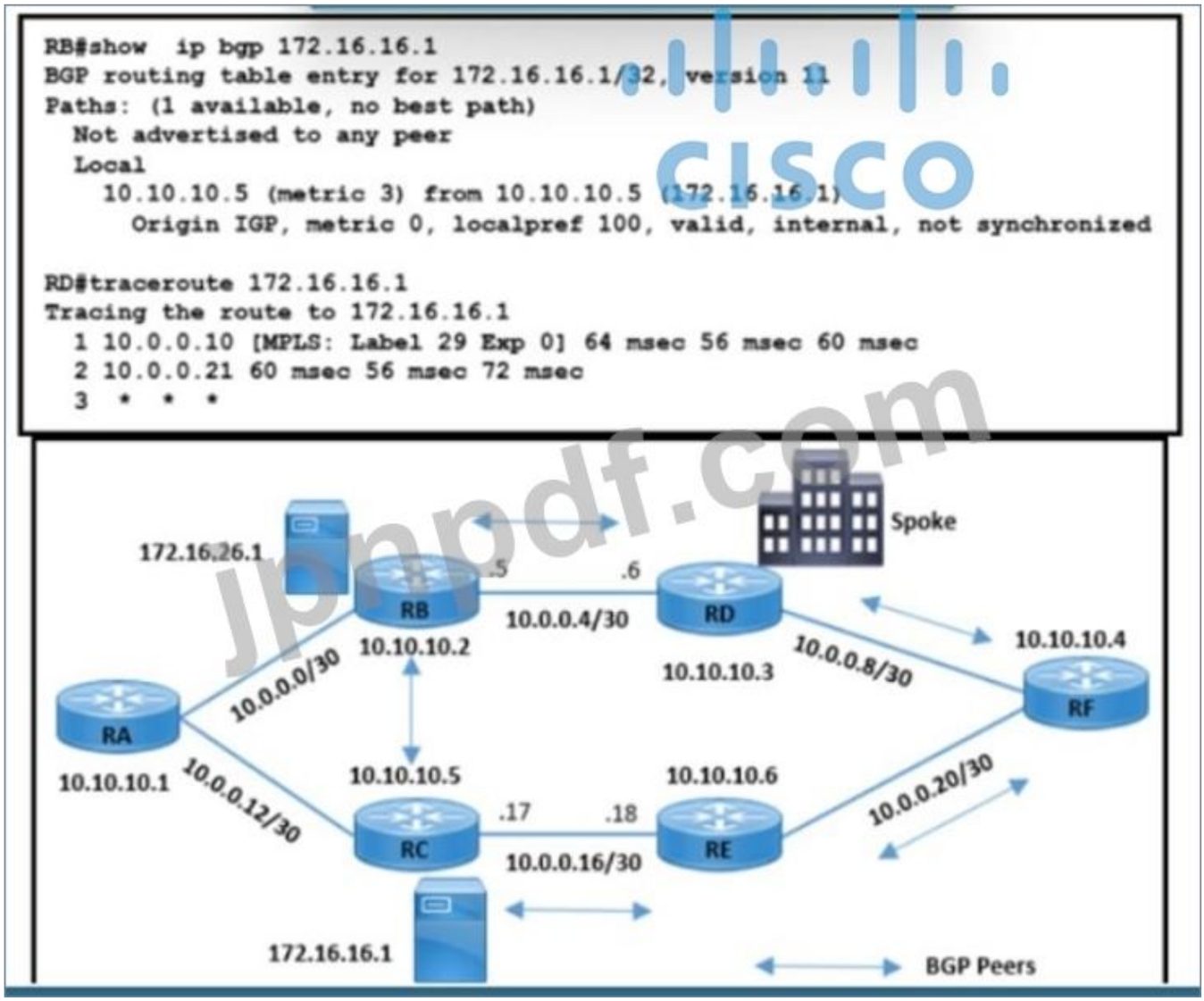
D. スポークツースポーク接続がありません。R2 と R3 の間に手動でネイバー関係を設定し、show ip eigrp neighbors コマンドの使用を確認して、DMVPN 設定を変更する必要があります。

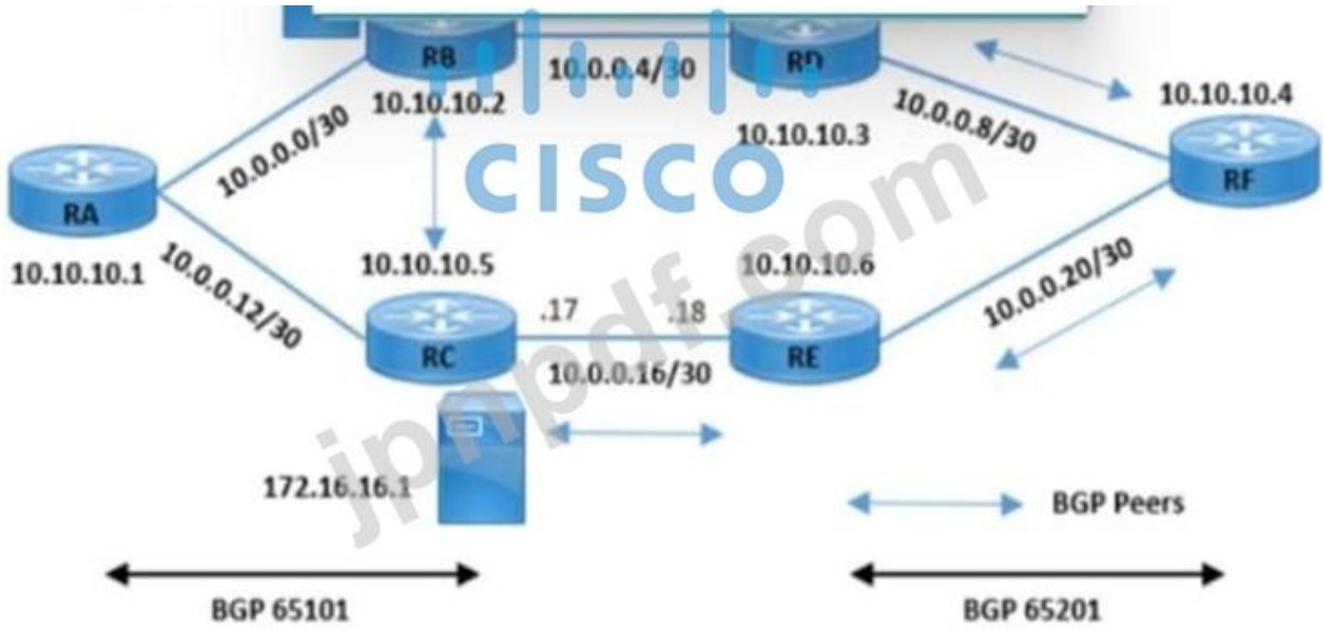
Answer: (解答を表示する**)**

このトポロジでは、ハブ ルータは、そのトンネル インターフェイス上で R2 スポーク ルータからアドバタイズメントを受信します。ここでの問題は、同じトンネル インターフェイス上で R3 スポークとの接続も存在することです。スプリット ホライズンを無効にしない場合、ハブは R2 から R3 へ、またはその逆へのルートを中継しません。これは、同じインターフェイス トンネル上でこれらのルートを受信したた

め、その同じインターフェイスをアドバタイズして戻すことができないためです (スプリット ホライズン ルール)。したがって、スポークが相互に認識していることを確認するために、ハブ ルータで splithorizon を無効にする必要があります。

最新問題: **221**
展示を参照してください。

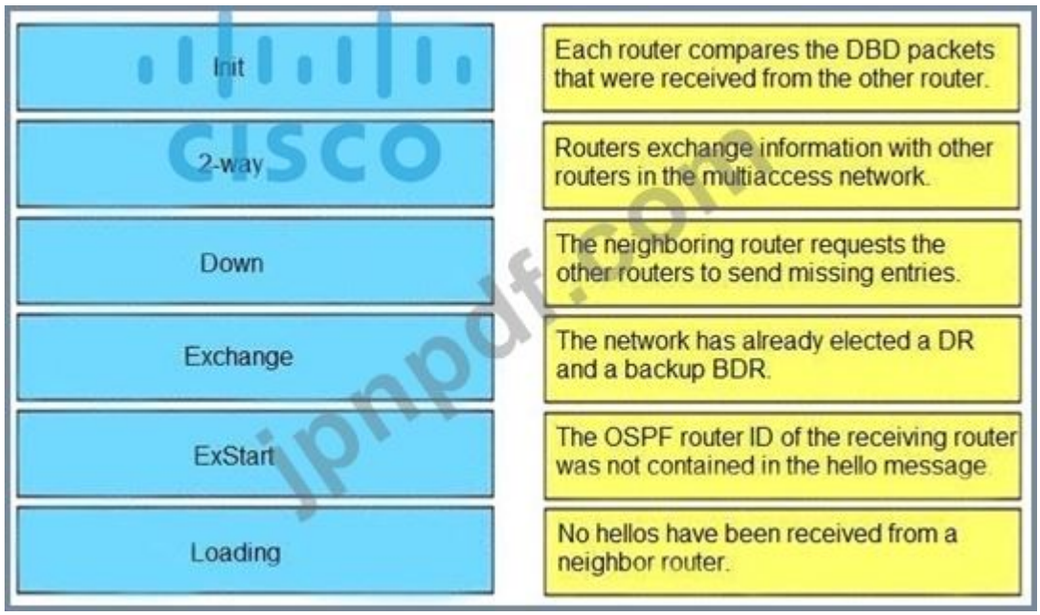




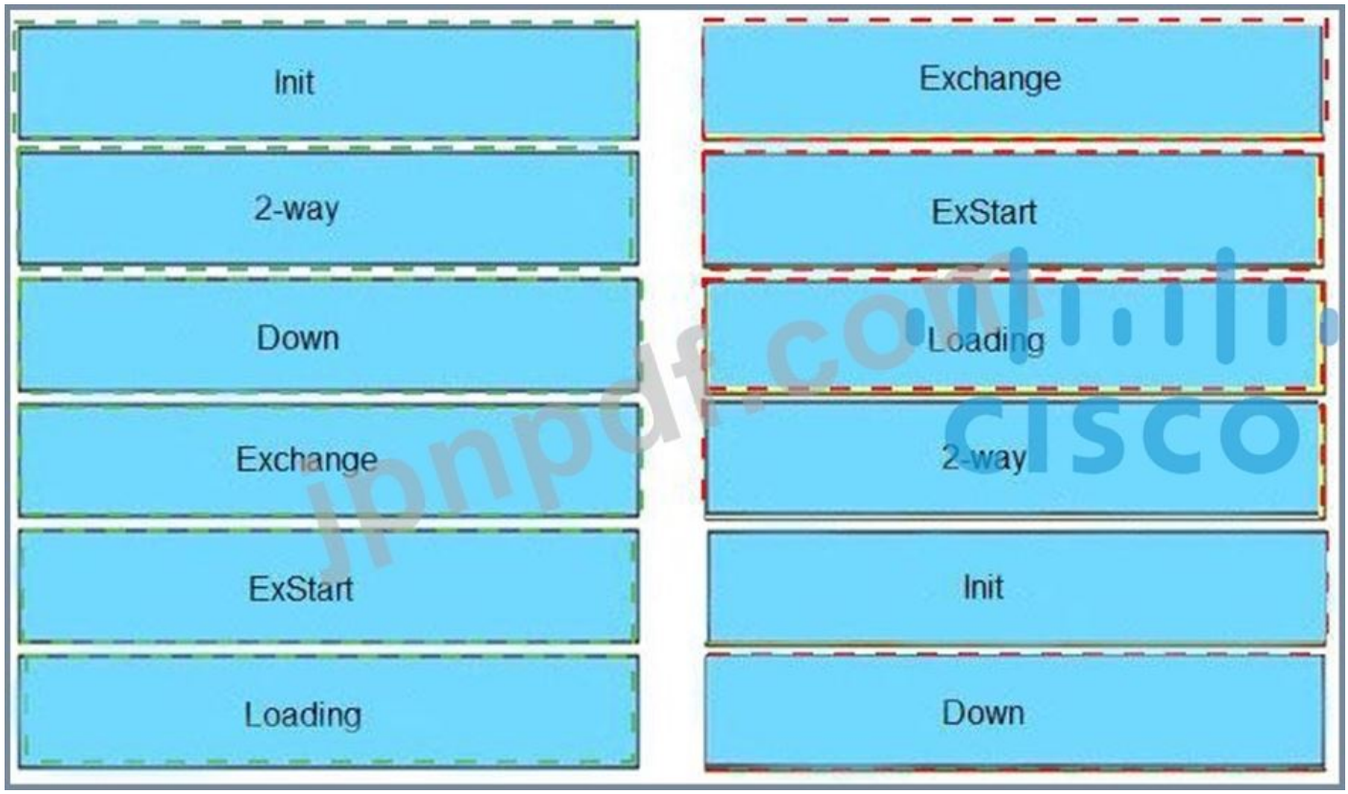
展示品を参照してください。お客様から、RC と RE の間のファイバー リンク障害に関する問題が報告されました。スポーク ロケーションを介して接続されているユーザーは、プライマリ電子メール サーバー (172.16.16.1) での切断とパケット ドロップに直面していますが、バックアップ電子メール サーバー (172.16) では問題はありません。.26.1）。すべてのルーター ループバック IP は、OSPF プロトコルを通じてアドバタイズされます。どの構成で問題が解決しますか?

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: C (メーッセージを残す**)**

最新問題**: 222**
OSPF 隣接状態を左側から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

下

これは、最初の OSPF ネイバー状態です。これは、このネイバーから情報 (hello) を受信していないが、この状態でも hello パケットをネイバーに送信できることを意味します。

完全隣接ネイバー状態の間、ルータが Router Dead Interval 時間 (デフォルトでは RouterDeadInterval = 4*HelloInterval) 以内にネイバーから hello パケットを受信しなかった場合、または手動で設定されたネイバーが設定から削除された場合、ネイバーは状態がフルからダウンに変わります。

試み

この状態は、環境内で手動で構成されたネイバーに対してのみ有効です。Attempt 状態では、ルータは

ポーリング間隔ごとにユニキャスト hello パケットをネイバーに送信しますが、デッド間隔内に hello を受信しなかったネイバーからのパケットが送信されます。

初期化

この状態は、ルータが近隣ルータから hello パケットを受信したが、受信ルータの ID が hello パケットに含まれていなかったことを示します。ルータが近隣ルータから hello パケットを受信した場合、有効な hello パケットを受信したことの確認として、送信者のルータ ID を hello パケットにリストする必要があります。

2ウェイ

この状態は、2 つのルーター間で双方向通信が確立されていることを示します。

双方向とは、各ルーターが他のルーターの hello パケットを認識していることを意味します。この状態は、Hello パケットを受信したルータが、受信した Hello パケットの近隣フィールド内で自身の Router ID を認識したときに達成されます。この状態で、ルーターはこのネイバーと隣接するかどうかを決定します。ブロードキャスト メディアおよび非ブロードキャスト マルチアクセス ネットワークでは、ルーターは指定ルーター (DR) とバックアップ指定ルーター (BDR) だけでいっぱいになります。他のすべての近隣ノードとの双方向状態が維持されます。ポイントツーポイント ネットワークおよびポイントツーマルチポイント ネットワークでは、接続されているすべてのルーターでルーターがいっぱいになります。

この段階の最後に、ブロードキャストおよび非ブロードキャスト マルチアクセス ネットワークの DR および BDR が選択されます。

DR 選出プロセスの詳細については、「DR 選出」を参照してください。

注: 初期状態のネイバーからデータベース記述子 (DBD) パケットを受信すると、双方向状態への移行が発生します。

エクススタート

DR と BDR が選出されると、ルーターとその DR および BDR の間で、リンク状態情報を交換する実際のプロセスが開始されます。(つまり、共有ネットワークまたはNBMAネットワーク)。

この状態では、ルーターとその DR および BDR はマスター/スレーブ関係を確立し、隣接関係形成のための最初のシーケンス番号を選択します。より高いルーター ID を持つルーターがマスターとなって交換を開始するため、シーケンス番号を増やすことができる唯一のルーターになります。このマスター/スレーブ関係のプロセスでは、最も高いルーター ID を持つ DR/BDR がマスターになると論理的に結論付けることができることに注意してください。DR/BDR の選択は、最高のルーター ID ではなく、ルーターに設定されたより高い優先順位によって純粋に行われる可能性があることに注意してください。したがって、DR がスレーブの役割を果たす可能性があります。また、マスター/スレーブの選択はネイバーごとに行われることにも注意してください。

交換

交換状態では、OSPF ルーターはデータベース記述子 (DBD) パケットを交換します。データベース記述子には、リンクステート アドバタイズメント (LSA) ヘッダーのみが含まれており、リンクステート データベース全体の内容を記述します。

各 DBD パケットには、マスターによってのみ増加できるシーケンス番号があり、スレーブによって明示的に確認されます。ルーターは、この状態でリンクステート要求パケットとリンクステート更新パケット (LSA 全体を含む) も送信します。受信した DBD の内容は、ルータのリンクステート データベースに含ま

れる情報と比較され、新しいリンクステート情報またはより現在のリンクステート情報が近隣ルータで利用可能かどうかが確認されます。
読み込み中
この状態で、リンク状態情報の実際の交換が行われます。DBD によって提供される情報に基づいて、ルーターはリンクステート要求パケットを送信します。次に、ネイバーは、要求されたリンクステート情報をリンクステート更新パケットで提供します。隣接関係中に、ルータが古い LSA または欠落している LSA を受信した場合、リンクステート要求パケットを送信してその LSA を要求します。すべてのリンクステート更新パケットが確認応答されます。
満杯
この状態では、ルーターは互いに完全に隣接しています。すべてのルーターとネットワーク LSA が交換され、ルーターのデータベースは完全に同期されます。
フルは OSPF ルーターの通常の状態です。ルーターが別の状態でスタックしている場合は、隣接関係の形成に問題があることを示しています。この唯一の例外は双方向状態であり、これはブロードキャストネットワークでは通常のことです。ルーターは、NBMA/ブロードキャスト メディアの DR および BDR で FULL 状態を実現し、ポイントツーポイントやポイントツーマルチポイントなどの残りのメディアですべてのネイバーで FULL 状態を実現します。
注: セグメント上のすべてのルーターで FULL 状態を達成する DR および BDR では、DR または BDR のいずれかでコマンドを入力すると、FULL/DROTHER が表示されます。これは単にネイバーが DR または BDR ではないことを意味しますが、コマンドが入力されたルータは DR または BDR であるため、ネイバーは FULL/DROTHER として表示されます。

最新問題: **223**
展示を参照してください。R2 はルート リフレクタであり、R1 と R3 はルート リフレクタ クライアントです。ルート リフレクタは、R1 から 172.16.25.0/24 へのルートを学習しますが、R3 にはアドバタイズしません。
ルートが公開されない理由は何ですか?

```
R1 #show ip bgp summary
BGP router identifier 192.168.1.1, local AS number 65000
<output omitted>
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.2     4 65000      28      28       22    0    0 00:21:31        0
R1#show ip bgp
BGP table version is 22, local router ID is 192.168.1.1
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
*>   172.16.25.0/24   209.165.200.225          0         32768 ?
R1#
```

```
R2 #show ip bgp summary
BGP router identifier 192.168.2.2, local AS number 65000
<output omitted>
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.1     4 65000      29      28        3    0    0 00:22:07        1
192.168.3.3     4 65000       7       8        3    0    0 00:02:55        0
R2#show ip bgp
BGP table version is 3, local router ID is 192.168.2.2
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
* i  172.16.25.0/24    209.165.200.225          0    100      0 ?
R2#
```

```
R3 #show ip bgp summary
BGP router identifier 192.168.3.3, local AS number 65000
BGP table version is 4, main routing table version 4
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.2     4 65000       8       7        4    0    0 00:03:08        0
R3#
```

A. R2 にはネクスト ホップへのルートがないため、R2 は他のクライアントにプレフィックスをアドバタイズしません。

B. ルート リフレクタのセットアップには、ルーター間の完全な IBGP メッシュが必要です。

C. ルート リフレクターのセットアップでは、クラスフル プレフィックスのみが他のクライアントにアドバタイズされます。

D. ルート リフレクターのセットアップでは、プレフィックスはあるクライアントから別のクライアントにアドバタイズされません。

Answer: A (メーッセージを残す**)**
セクション: レイヤ 3 テクノロジー
説明/参照: