

Cisco.300-410.v2022-09-08.q307

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:	307
バージョン:	v2022-09-08
アクセス数:	2984
ページビュー数:	3060
https://www.jpnpdf.com/Cisco.300-410.v2022-09-08.q307-mondaishu.html	

最新問題: 1

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
Desired
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2 *Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2
```

展示品をご覧ください。エンジニアは、ログメッセージを最小限に抑えるために、重大度に基づいてメッセージをフィルタリングしました。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5を構成します。
 - B. syslogレベル4を構成します。
 - C. syslogレベル3を構成します。
 - D. syslogレベル2を構成します。
- Answer: A (メッセージを残す)**

最新問題: 2

展示を参照してください。



エンジニアは、ISP1およびISP2への設定済みデフォルトルートの到達可能性を監視しています。利用可能な場合は、ISP1からのデフォルトルートが優先されます。この問題はどのように解決されますか？

- A. 頻度を定義してスケジュールすることによりIPSLAを開始します
- B. icmp-echoコマンドを使用して、両方のデフォルトルートを追跡します
- C. trackおよびipslaコマンドの番号を照合してIPSLAを開始します
- D. 両方のデフォルトルートに同じADを使用する

Answer: A ([メッセージを残す](#))

最新問題: 3

展示を参照してください。



AS690内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AS690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. 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。
- B. ルートマップが間違った方向に適用されています。
- C. 別のネイバーステートメントのローカルプリファレンス値が250を超えています。
- D. 別のネイバーステートメントの重み値が200を超えています。

Answer: B ([メッセージを残す](#))

最新問題: 4

展示を参照してください。

```
Router#show ip route
<output omitted>
Gateway of last resort is not set

    192.168.1.0/32 is subnetted, 1 subnets
O       192.168.1.1 [110/11] via 192.168.12.1, 16:56:40, Ethernet0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Loopback0
L       192.168.2.2/32 is directly connected, Loopback0
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, Ethernet0/1
L       192.168.3.1/32 is directly connected, Ethernet0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/24 is directly connected, Ethernet0/0
L       192.168.12.2/32 is directly connected, Ethernet0/0
Router#show running-config | section ospf
router ospf 1
  summary-address 10.0.0.0 255.0.0.0
  redistribute static subnets
  network 192.168.3.0 0.0.0.255 area 0
  network 192.168.12.0 0.0.0.255 area 0
Router#
```

エンジニアがネットワーク10.0.0.0/8のOSPFでサマリールートを生成しようとしています。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。サマリー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データベースにのみ表示され、ルーティングテーブルには表示されません。
- C. 10.0.0.0/8内にサブネットのルートがないため、サマリー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には表示されませんが、同じエリア内の他のOSPFルーターには表示されます。

Answer: C ([メッセージを残す](#))

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のみ、ASBRで使用する必要があります。ただし、要約されたルートを作成するための要件は次のとおりです。ASBRは、サマリールートのアドレス範囲を、そのASBR上のOSPFに再配布されたすべてのルートと比較して、従属サブネット (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つの従属サブネットが存在する場合、ASBRはサマリールートをアドバタイズします。

展示を参照してください。

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

プレフィックスリストは、ネットワーク10プレフィックスを除くEIGRPプロセスへのインバウンドルートフィルタリングのために作成されます。プレフィックスリストが適用された後、ネットワーク10プレフィックスはEIGRPからのルーティングテーブルに表示されません。どの構成で問題が解決しますか？

- A. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9 ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
- B. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8ge9。
- C. ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
- D. ip prefix-list EIGRP seq 5 permit 10.0.0.0/8 ge 9 no ip prefix-list EIGRP seq 20 permit 10.0.0.0/8

Answer: D ([メッセージを残す](#))

最新問題: 6

展示を参照してください。

```
Router# show tag-switching tdp bindings
(...)
tib entry: 10.10.10.1/32, rev 31
  local binding: tag: 18
  remote binding: tsr: 10.10.10.1:0, tag: imp-null
  remote binding: tsr: 10.10.10.2:0, tag: 18
  remote binding: tsr: 10.10.10.6:0, tag: 21
tib entry: 10.10.10.2/32, rev 22
  local binding: tag: 17
  remote binding: tsr: 10.10.10.2:0, tag: imp-null
  remote binding: tsr: 10.10.10.1:0, tag: 19
  remote binding: tsr: 10.10.10.6:0, tag: 22
```

MPLS VPNクラウドでimp-nullタグは何を表していますか？

- A. ラベルをポップします
- B. ラベルを付ける
- C. EXPビットを含める
- D. EXPビットを除外する

Answer: (解答を表示する)

説明

imp-null (implicit null) タグは、パケットを転送する前に、タグエントリをタグスタックからポップするようにアップストリームルータに指示します。

注 :ポップとは、上部のMPLSラベルを削除することを意味します

最新問題: 7

展示を参照してください。

```
ipv6 access-list inbound
permit tcp any any
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out
```

ネットワーク管理者は、TCPリターンフレームのみを許可するようにIPv6アクセスリストを設定しましたが、期待どおりに機能していません。この問題を解決する変更はどれですか？

ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out

ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out

ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in

ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in

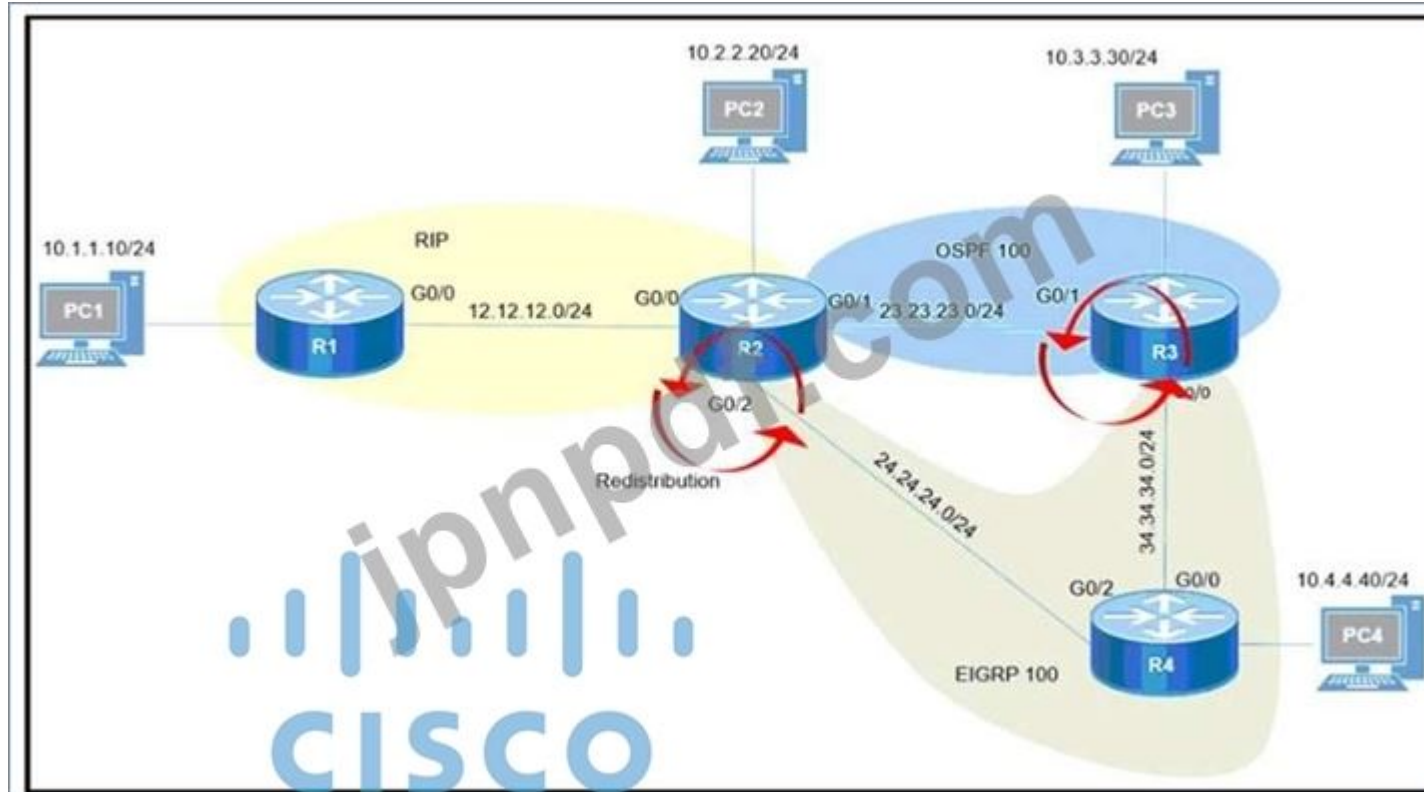
- A. オプションA
- B. オプションB
- C. オプションC
- D. オプションD

Answer: C (メッセージを残す)

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/122_55_se/configuration/guide/scg3750/swv6acl.html

最新問題: 8

展示を参照してください。



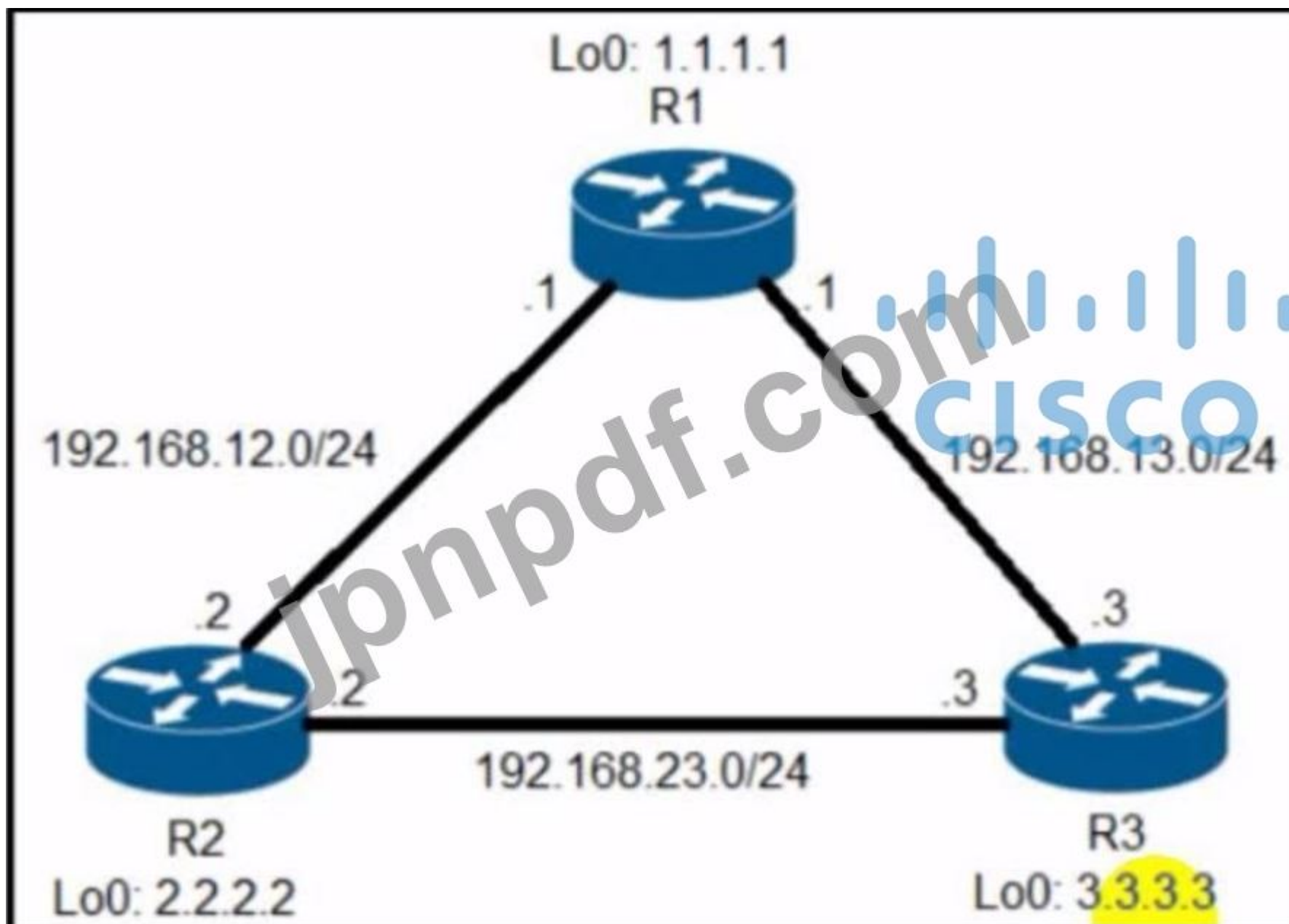
ルーティングプロトコル間で再配布が有効になり、PC2 PC3になり、PC4はPC1に到達できなくなります。問題を解決するための2つの解決策は何ですか？ 2つ選択してください。)

- A. R2でRIPに再配布するときに、RIPルートをRIPにフィルターで戻す
- B. R2のRIPに再配布するときに、OSPFルートをRIPFROMEIGRPにフィルタリングします。
- C. R2で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でOSPFに再配布するときに、EIGRPからOSPFに戻るRIPおよびOSPFルートをフィルタリングします
- E. R3で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,C (メッセージを残す)

PC2でさえPC1に到達できないため、R2でのRIPの再配布に問題があります。RIPはOSPFおよびEIGRPよりも管理距離 (AD) 値が高いため、相互再配布を行うときにループされます。

最新問題: 9



```
R2#show ip protocols | include eigrp|Maximum
```

```
Routing Protocol is "eigrp 1"
```

```
Maximum path: 4
```

```
Maximum hopcount 100
```

```
Maximum metric variance 1
```

```
R2#show ip eigrp topology 192.168.13.0/24
```

```
EIGRP-IPv4 Topology Entry for AS(1)/ID(2.2.2.2) for 192.168.13.0/24
```

```
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 1075200
```

```
Descriptor Blocks:
```

```
192.168.23.3 (FastEthernet0/1), from 192.168.23.3, Send flag is 0x0
```

```
Composite metric is (1075200/281600), route is Internal
```

```
Vector metric:
```

```
Minimum bandwidth is 2500 Kbit
```

```
Total delay is 2000 microseconds
```

```
Reliability is 255/255
```

```
Load is 255/255
```

```
Minimum MTU is 1500
```

```
Hop count is 1
```

```
Originating router is 3.3.3.3
```

```
192.168.12.1 (FastEthernet0/0), from 192.168.12.1, Send flag is 0x0
```

```
Composite metric is (2611200/281600), route is Internal
```

```
Vector metric:
```

```
Minimum bandwidth is 1000 Kbit
```

```
Total delay is 2000 microseconds
```

```
Reliability is 255/255
```

```
Load is 1/255
```

```
Minimum MTU is 1500
```

```
Hop count is 1
```

```
Originating router is 1.1.1.1
```

```
R2#show ip route 192.168.13.0
```

```
Routing entry for 192.168.13.0/24
```

```
Known via "eigrp 1", distance 90, metric 1075200, type internal
```

```
Redistributing via eigrp 1
```

```
Last update from 192.168.23.3 on FastEthernet0/1, 00:00:57 ago
```

```
Routing Descriptor Blocks:
```

```
* 192.168.23.3, from 192.168.23.3, 00:00:57 ago, via FastEthernet0/1
```

```
Route metric is 1075200, traffic share count is 1
```

```
Total delay is 2000 microseconds, minimum bandwidth is 2500 Kbit
```

```
Reliability 255/255, minimum MTU 1500 bytes
```

```
Loading 255/255, Hops 1
```

展示を参照してください。R2には、192.168.13.0/24に到達するための2つのパスがあります。ただし、トラフィックはR3を介してのみ送信されます。トラフィックが両方のパスを使用できるようにするアクションはどれですか？

- A. R2のインターフェイスFastEthernet0/0でbandwidth2000コマンドを設定します。
- B. R2のEIGRPプロセスでvariance4コマンドを設定します。
- C. R2のインターフェイスFastEthernet0/0でdelay1コマンドを設定します。
- D. R2のEIGRPプロセスでvariance2コマンドを設定します

Answer: [\(解答を表示する\)](#)

説明

「show ip eigrp topology...」コマンドの出力から、ネットワーク192.168.13.0/24が2つのルートを介して学習されたことがわかります。+ FD = 1075200およびAD = 281600の192.168.23.3 (R3)から。12.1 (R1)、FD = 2611200およびAD = 281600 (show ip route...」コマンドの出力から、最適な (および選択された)パスは経由であることがわかりました。192.168.23.3 (R3)。

EIGRPで両方のパス (不等コストロードバランシングと呼ばれる)を使用するには、R1を介した2番目のパスが実現可能性の条件を満たす必要があります。実現可能性条件は、ルートのアドバタイズされた距離 (AD)が、現在の後続ルートの実現可能距離よりも低くなければならないことを示しています。

この場合、2番目のパスはAD (281600)が最適パスのFD (1075200)よりも小さいため、実行可能な条件を満たす。したがって、「variance」コマンドを使用してロードバランシングを構成できます。

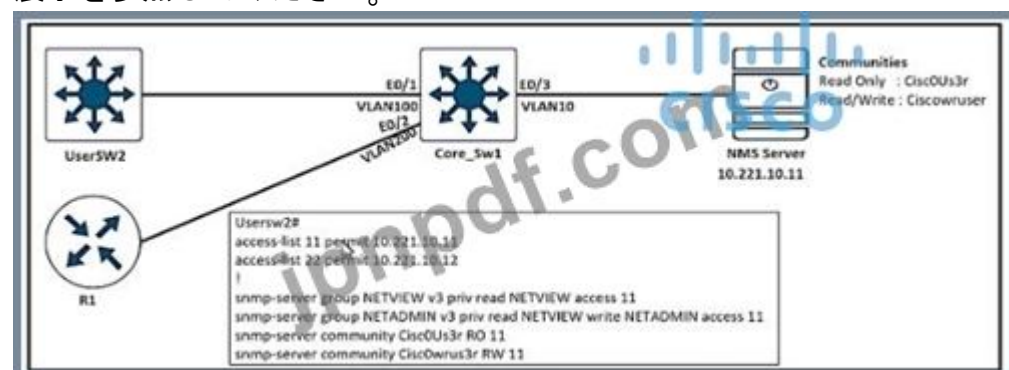
つまり、EIGRPは、ルーティングループを防止するための実現可能性条件を満たす場合に限り、metric < variance * best_metricのすべてのパスをローカルルーティングテーブルにインストールします。したがって、分散を計算できます

>メトリック法/best_metric = 2611200/1075200 = 2.4。

したがって、分散が2より大きい場合 (整数である必要があります)、ネットワークへのトラフィックを負荷分散できます。192.168.13.0/24。

最新問題: 10

展示を参照してください。



展示を参照してください。エンジニアがUserSW2スイッチでSNMP Communitiesを構成しましたが、SNMPサーバーは変更された構成をスイッチにアップロードできません。この問題を解決する構成はどれですか？

- A. snmp-server community Ciscowruser RW 11
- B. snmp-server group NETVIEW v2c priv read NETVIEW access 11
- C. snmp-server community CiscoUs3r RW 11
- D. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22

Answer: [A \(メッセージを残す\)](#)

最新問題: 11

別紙を参照してください。



ネットワーク管理者は、Cisco DNA Centerにルータを1つ追加し、ネットワークヘルスダッシュボードからその検出とヘルスを確認しました。ネットワーク管理者は、ルーターがまだ監視されていないものとして表示されていることを確認しました。Cisco DNA Centerにマウントするには、ルータに何を設定する必要がありますか。

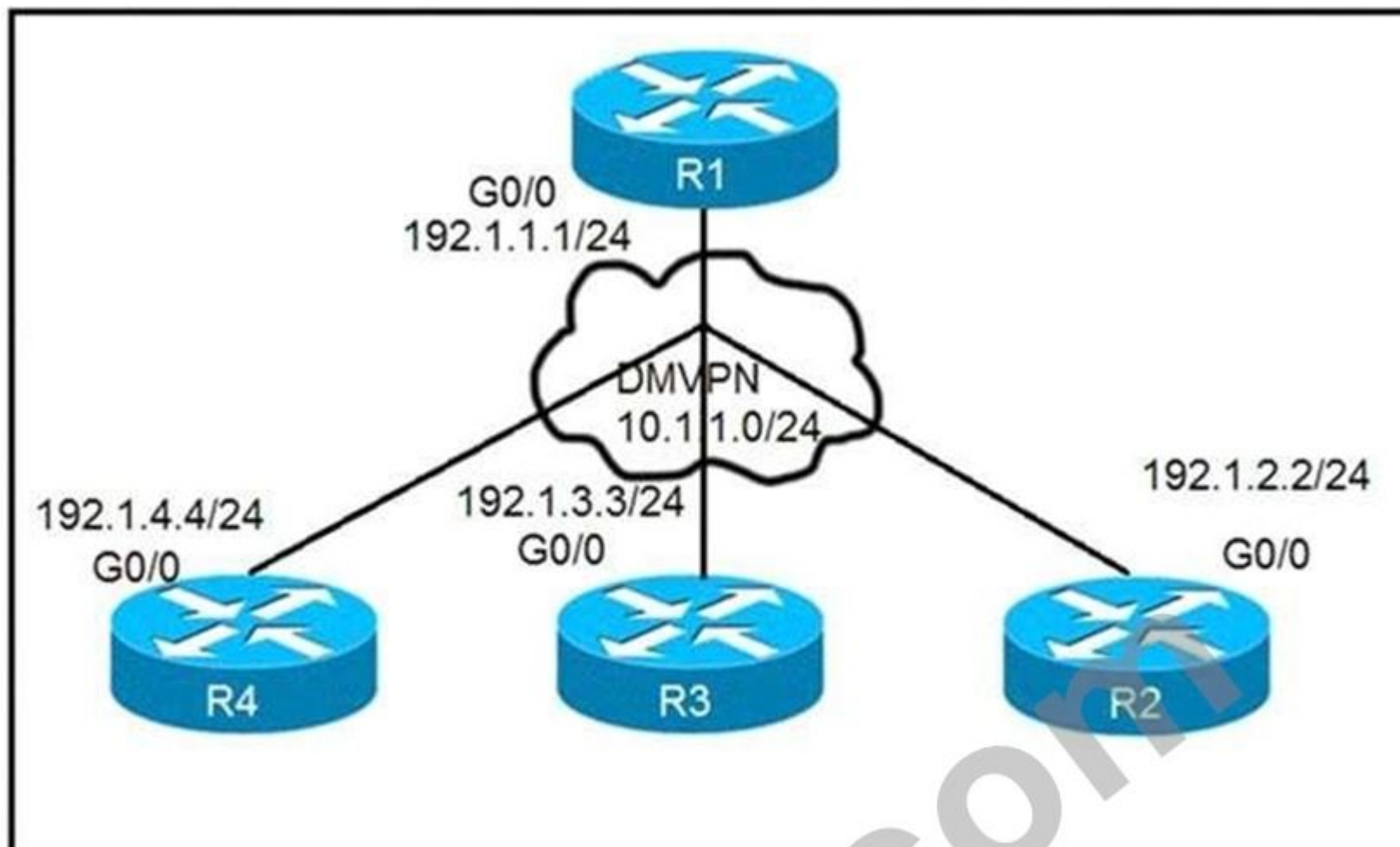
- A. NetFlowデータを使用してルーターを構成します
- B. テレメトリデータを使用してルーターを構成します
- C. CiscoDNA Centerに到達するためのルーティングを使用してルータを設定します
- D. SNMPV2cまたはSNMPV3トラップを使用してルーターを構成します

Answer: (解答を表示する)

監視されていない：監視されていないデバイスは、指定された時間範囲内にAssuranceがテレメトリデータを受信しなかったデバイスです。

最新問題: 12

展示品をご覧ください。



On R1:
R1(config)# interface tunnel 1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# tunnel source 192.1.1.1
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# ip nhrp network-id 111

On R2:
R2(config)# interface tunnel 1
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# tunnel source FastEthernet0/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# ip nhrp network-id 222
R2(config-if)# ip nhrp nhs 10.1.1.1
R2(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

On R3:
R3(config)# interface tunnel 1
R3(config-if)# ip address 10.1.1.3 255.255.255.0
R3(config-if)# tunnel source FastEthernet0/0
R3(config-if)# tunnel mode gre multipoint
R3(config-if)# ip nhrp network-id 333 R3(config-if)# ip nhrp nhs 10.1.1.1
R3(config-if)# ip nhrp map 10.1.1.1 192.1.1.1



```
On R4: R4(config)# interface tunnel 1
R4(config-if)# ip address 10.1.1.4 255.255.255.0
R4(config-if)# tunnel source FastEthernet0/0
R4(config-if)# tunnel mode gre multipoint
R4(config-if)# ip nhrp network-id 444
R4(config-if)# ip nhrp nhs 10.1.1.1
R4(config-if)# ip nhrp map 10.1.1.1 192.1.1.1
```

DMVPNのスポークツースポーク間にフェーズ3トンネルを確立することはできません。欠落している2つのコマンドはどれですか？ (2つ選択してください。)

- A. ハブルータにipnhrpredirectコマンドがありません。
- B. スポークルータにipnhrpショートカットコマンドがありません。
- C. ハブルータにipnhrpショートカットコマンドがありません。
- D. ハブルータにipnhrpmapコマンドがありません。
- E. スポークルータにipnhrpredirectコマンドがありません。

Answer: ([解答を表示する](#))

最新問題: 13

展示を参照してください。ネットワーク管理者は、TCPリターントラフィックのみを許可するようにIPv6アクセスリストを設定しましたが、期待どおりに機能していません。この問題を解決する変更はどれですか？

- A. ipv6アクセスリストインバウンド

tcp anyanysynを許可する

ipv6をすべてのログで拒否します

!

インターフェイスgi0/0

ipv6traffic-filterインバウンドイン

- B. ipv6アクセスリストインバウンド

tcp anyanysynを許可する

ipv6をすべてのログで拒否します

!

インターフェイスgi0/0

ipv6traffic-filterインバウンドアウト

- C. ipv6アクセスリストインバウンド

確立された任意のtcpを許可する

ipv6をすべてのログで拒否します

!

インターフェイスgi0/0

ipv6traffic-filterインバウンドアウト

- D. ipv6アクセスリストインバウンド

確立された任意のtcpを許可する

ipv6をすべてのログで拒否します

！

インターフェイスgi0/0

ipv6traffic-filterインバウンドイン

Answer: ([解答を表示する](#))

最新問題: 14

展示を参照してください。

```
service timestamps debug datetime msec
service timestamps log datetime
clock timezone MST -7 0
clock summer-time MST recurring
ntp authentication-key 1 md5 00101A0B0152181206224747071E 7
ntp server 10.10.10.10
```

R1#show clock

*06:13:44.045 MST Sun Dec 30 2018

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config) #logging host 10.10.10.20

R1(config) #end

R1#

*Dec 30 13:15:28: %SYS-5-CONFIG_I: Configured from console by console

R1#

*Dec 30 13:15:28: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.10.10.20 port 514 started – CLI initiated

管理者は、R1で変更が行われた後、システムログのタイムスタンプが時計と一致しなかったことに気づきました。このエラーの理由は何ですか？

- A. NTPサーバーでの認証エラーにより、タイムスタンプが正しくなくなります。
- B. システム時計が夏時間に正しく設定されていません。
- C. キーワードlocaltimeがtimestampserviceコマンドで定義されていません。
- D. NTPサーバーは別のタイムゾーンにあります。

Answer: B ([メッセージを残す](#))

最新問題: 15

展示を参照してください。

```
R1(config)# ip route 0.0.0.0 0.0.0.0 1.1.1.1
R1(config)# ip route 0.0.0.0 0.0.0.0 2.2.2.2 10
R1(config)# ip sla 1
R1(config)# icmp-echo 1.1.1.1 source-interface FastEthernet0/0
R1(config)# ip sla schedule 1 life forever start-time now

R1(config)# track 1 ip sla 1 reachability
```

IP SLAは、プライマリがダウンしているときにバックアップのデフォルトルートを使用するように設定されていますが、期待どおりに機能していません。どのコマンドで問題が解決しますか？

- A. R1 (config) #ip route 0.0.0.0.0.0.0.0.2.2.2.2
- B. R1 (config)#ip sla track 1
- C. R1 (config) #ip route 0.0.0.0.0.0.0.0.2.2.2.2 10 track 1
- D. R1 (config) #ip route 0.0.0.0.0.0.0.0.1.1.1.1 track 1

Answer: D ([メッセージを残す](#))

最新問題: 16

FastEthernet0/0で"inet"とラベル付けされたVRFを有効にする構成はどれですか。

A)

```
R1(config)# ip vrf Inet
R1(config-vrf)#ip vrf FastEthernet0/0
```

B)

```
R1(config)#ip vrf Inet FastEthernet0/0
```

C)

```
R1(config)# ip vrf Inet
R1(config-vrf)#interface FastEthernet0/0
R1(config-if)#ip vrf forwarding Inet
```

D)

```
R1(config)#router ospf 1 vrf Inet
R1(config-router)#ip vrf forwarding FastEthernet0/0
```

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

Answer: C ([メッセージを残す](#))

有効な 300-410 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の 300-410 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (80030%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 17

展示を参照してください。

```
Configuration output:
clock timezone PST -8
clock summer-time PDT recurring
service timestamps debug datetime
service timestamps log datetime
logging buffered 16000 debugging
ntp clock-period 17179272
ntp server 161.181.92.152

Debug output:
router#show clock
14:12:26.312 PDT Thu Apr 27 2019
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#exit

router#
Apr 27 21:12:28: %SYS-5-CONFIG_I: Configured from console by vty0
```

展示を参照してください。ネットワーク管理者は、統一されたタイムソースからシステムとログの同期時刻を取得するようにCiscoルーターでNTPを構成しました。構成が期待どおりに機能しませんでした。問題を解決するには、どのサービスを有効にする必要がありますか。

- A. サービスタイムスタンプログ日時ローカルタイムグローバルコマンドを入力します。
- B. サービスタイムスタンプログ日時同期グローバルコマンドを入力します。

C. service timestamps logdatetimeconsoleグローバルコマンドを入力します。

D. サービスタイムスタンプlogdatetimeclock-periodグローバルコマンドを入力します

Answer: (解答を表示する)

ネットワークタイムプロトコル (NTP)サーバーから時刻を取得するようにルータが設定されている場合、[localtime]オプションがservice timestamps logコマンドにない場合、ルータのログエントリの時刻はシステムクロックの時刻と異なる場合があります。この問題を解決するには、servicetimestampslogコマンドに[localtime]オプションを追加します。これで、システムクロックとログメッセージのタイムスタンプの間で時刻が同期されるはずですが。

最新問題: 18

MPLSVPNデバイスタイプを左から右の定義にドラッグアンドドロップします。

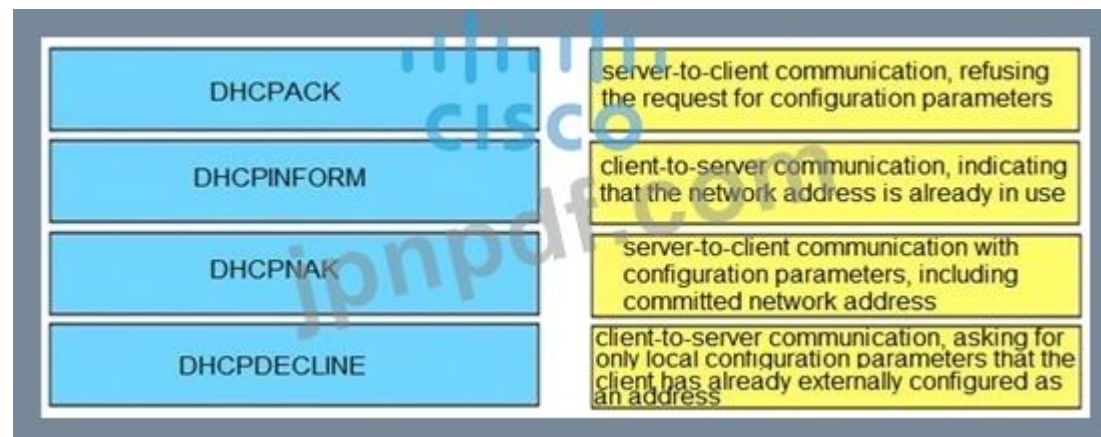


Answer:



最新問題: 19

DHCPメッセージを左側から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：

<https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html>

最新問題: 20

エンジニアは、会社のマルチエリアOSPF本社ルーターとサイトACiscoルーターをVRF liteで構成しました。各サイトルーターは、MPLSバックボーンのPEルーターに接続されています。

```

Head Office & Site A
ip cef
ip vrf abc
rd 101:101
!
interface FastEthernet0/0
ip vrf forwarding abc
ip address 172.16.16.X 255.255.255.252
!
router ospf 1 vrf abc
log-adjacency-changes
network 172.16.16.0 0.0.0.255 area 1

```

両方のサイトルーターの設定が完了した後、LSA 3,4、5、および7はいずれもサイトAルーターにインストールされていません。この問題を解決する構成はどれですか？

- A. サイトAの機能vrf-liteと、ルーターospf 1vrfabcの下に接続されているPEルーターを構成します。
- B. ルーターospf 1vrfabcの下の本社およびサイトAルーターで機能vrf-liteを設定します
- C. router ospf 1vrfabcで本社とサイトAのルーターに接続されている両方のPEルーターで機能vrf-liteを構成します。
- D. ルーターospf 1vrfabcの下で本社と接続されているPEルーターの機能vrf-liteを構成します

Answer: [\(解答を表示する\)](#)

最新問題: 21

展示を参照してください。

R1

```
ip prefix-list ccnp1 seq 5 permit 10.1.48.0/24 le 24
ip prefix-list ccnp2 seq 5 permit 10.1.80.0/24 le 32
ip prefix-list ccnp3 seq 5 permit 10.1.64.0/24 le 24
```

```
route-map ospf-to-eigrp permit 10
  match ip address prefix-list ccnp1
  set tag 30
route-map ospf-to-eigrp permit 20
  match ip address prefix-list ccnp2
  set tag 20
route-map ospf-to-eigrp permit 30
  match ip address prefix-list ccnp3
  set tag 10
```

エンジニアがルート101.80.65/32に30のタグを設定したかったのですが、失敗しました。問題はどのように修正されますか？

- A. プレフィックスリストccnp3を変更して、10.1.64.0 / 20le24を追加します。
- B. route-map ospf-to-eigrp permit 30を変更し、prefix-listccnp2と一致させます。
- C. プレフィックスリストccnp3を変更して、10.1.64.0 / 20ge32を追加します
- D. route-map ospf-to-eigrp permit 10を変更し、prefix-listccnp2と一致させます。

Answer: D ([メッセージを残す](#))

最新問題: 22

ルーティングポリシーにいくつかの変更を加えた後、AS45123のルーターがいくつかのサービス提供のトランジットASルーターとして使用されていることがわかります。AS 45123のブランチルーターがすべてのSPネイバーにローカルネットワークのみをアドバタイズすることを保証する構成はどれですか？

A)

```
ip as-path access-list 1 permit ^45123
|
router bgp 45123
  neighbor SP-Neighbors filter-list 1 out
```

B)

```
ip as-path access-list 1 permit .*
|
router bgp 45123
  neighbor SP-Neighbors filter-list 1 out
```

C)

```
ip as-path access-list 1 permit ^45123$
|
router bgp 45123
neighbor SP-Neighbors filter-list 1 out
```

D)

```
ip as-path access-list 1 permit ^$
|
router bgp 45123
neighbor SP-Neighbors filter-list 1 out
```

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

Answer: D ([メッセージを残す](#))

説明

デフォルトでは、BGPはすべてのプレフィックスを外部BGPネイバーにアドバタイズします。これは、マルチホーム (2つ以上のISPに接続されている) の場合、トランジットASになる可能性があることを意味します。たとえば、ISP3のプレフィックスをISP2にアドバタイズしたため、AS200のISP2は、AS100のルータにトラフィックを送信してAS300のISP3に到達できます。これは、ISP1のBGPルーティングテーブルに表示されるものです。

```
ISP1#show ip bgp
--output omitted--
Network          Next Hop          Metric LocPrf Weight Path
.....
*> 3.3.3.0/24    192.168.12.1          0 100 300 i
```

最新問題: 23

ネットワークエンジニアには、複数の従業員がネットワークパフォーマンス関連の問題を経験していることが通知され、帯域幅を大量に消費するアプリケーションが根本的な原因として特定されます。この速度低下の原因となっている特定のタイプのトラフィックを特定するには、送信元/宛先IPやレイヤー4ポート番号などの情報が必要です。エンジニアは、必要な情報を収集するためにどの機能を使用する必要がありますか？

- A. SNMP
- B. Cisco IOS EEM
- C. NetFlow
- D. Syslog
- E. WCCP

Answer: C ([メッセージを残す](#))

NetFlowフローのキーフィールド

ネットワークフローは、特定の送信元と宛先間のパケットの一方向ストリームとして識別されます。どちらも、ネットワーク層のIPアドレスと、トランスポート層の送信元および宛先ポート番号によって定義されます。

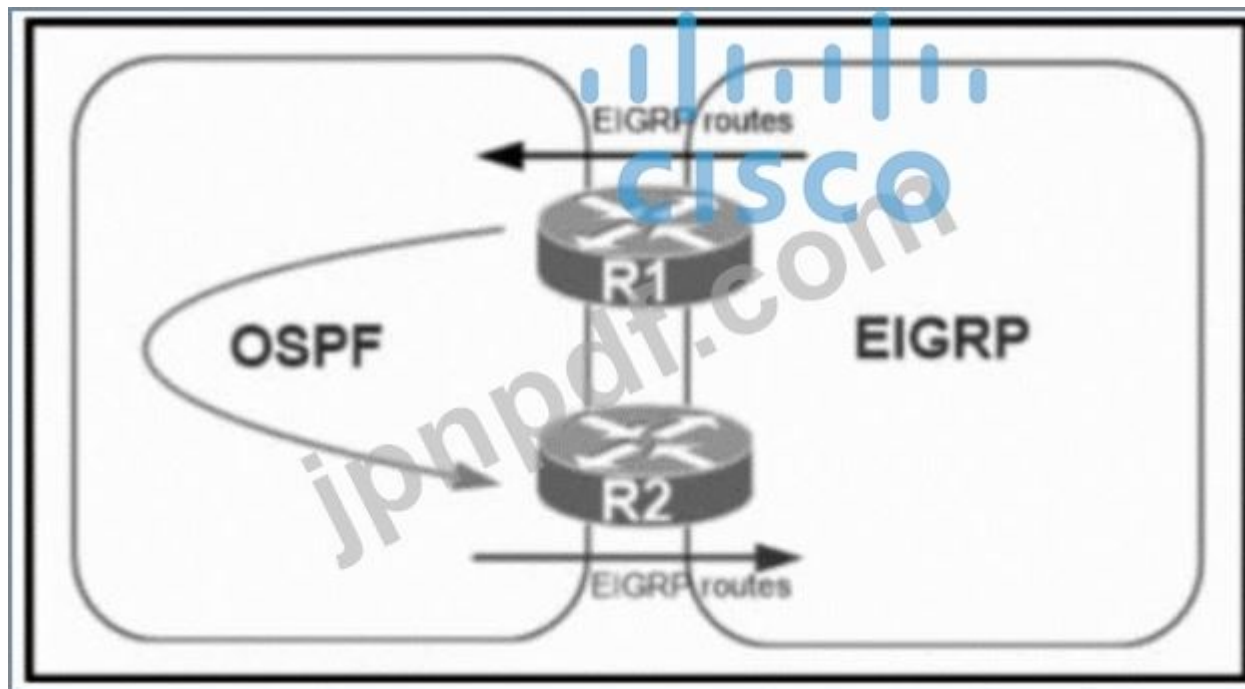
具体的には、フローは次のキーフィールドの組み合わせとして識別されます。

送信元IPアドレス

宛先IPアドレス

ソースレイヤー4のポート番号
宛先レイヤー4のポート番号
レイヤ3プロトコルタイプ
タイプオブサービス (ToS)
入力論理インターフェース

最新問題: 24



展示を参照してください。ネットワーク管理者がR1および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。問題を解決するアクションはどれですか？

- A. R1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。R2の同じタグを照合して、OSPFをEIGRPに再配布するときに拒否します。
- B. R1のOSPFドメインにEIGRPネットワークルートのプレフィックスリストを適用して、EIGRPルーティングドメインに伝播します。
- C. R1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。R2で同じタグを照合して、OSPFをEIGRPに再配布するときに許可します。
- D. EIGRPのサマリールートを実体化し、OSPFに再配布するときに特定のEIGRPルートを拒否します。

Answer: A ([メッセージを残す](#))

最新問題: 25

MPLSVPN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。

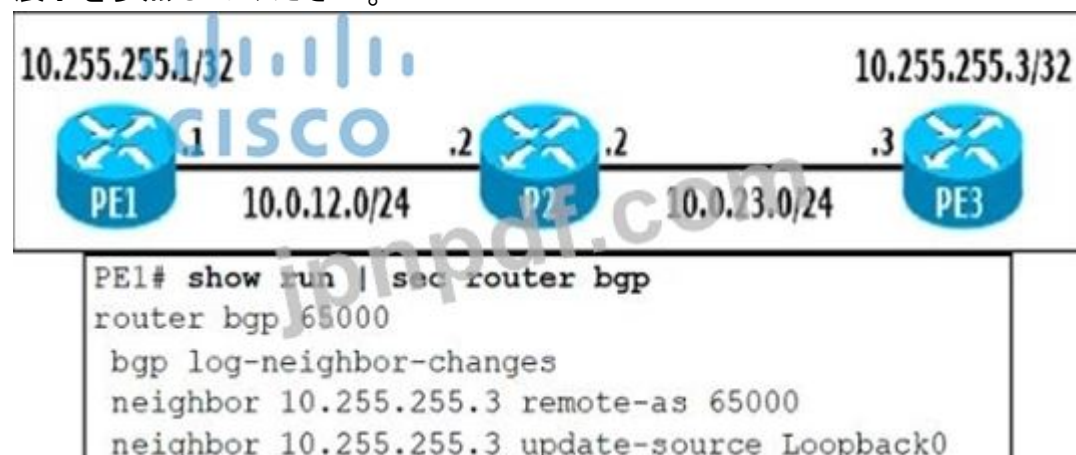
Customer (C) device	device in the core of the provider network that switches MPLS packets
CE device	device that attaches and detaches the VPN labels to the packets in the provider network
PE device	device in the enterprise network that connects to other customer devices
Provider (P) device	device at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

Answer:

Customer (C) device	Provider (P) device
CE device	PE device labels to the packets in the provider network
PE device	Customer (C) device connects to other customer devices
Provider (P) device	CE device that connects to the SP network

最新問題: 26

展示を参照してください。



```

|1/1/1 ms
PE1# debug ip tcp transactions
PE1# debug ip icmp

[...snip...]
*Feb 22 14:04:12.374: TCP: sending SYN, seq 379810712, ack 0
*Feb 22 14:04:12.374: TCP0: Connection to 10.255.255.3:179,
advertising MSS 1460
*Feb 22 14:04:12.374: TCP0: state was CLOSED -> SYNSENT [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: ICMP: dst (10.255.255.1) administratively
prohibited unreachable rcv from 10.0.12.2
*Feb 22 14:04:12.375: TCP0: ICMP destination unreachable
received
*Feb 22 14:04:12.375: Released port 21381 in Transport Port
Agent for TCP IP type 1 delay 240000
*Feb 22 14:04:12.375: TCP0: state was SYNSENT -> CLOSED [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: TCB 0xE35A92B8 destroyed

```

展示を参照してください。管理者は、問題を解決するアクションを確立できないPE1とPE3間のBGPピアリングのトラブルシューティングを行っていますか？

- A. PE3ルーブバックアドレスがPE1へのBGPピアリングのソースとして使用されていることを確認します
- B. PE1とPE3間のBGP通信をブロックするP2のトラフィックフィルタリングルールを削除します
- C. PE1がPE3とのセッションを確立できるように、P2でICMP到達不能の送信を無効にします
- D. PE1へのBGPセッションを確立するには、P2にPE3へのルートが必要です。

Answer: A ([メッセージを残す](#))

最新問題: 27

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を有効にすると、PC2、PC3、およびPC4はPC1に到達できなくなります。すべてのPCに到達できるように、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. RIPからEIGRPに再配布するときに、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のプロセスで管理距離100を設定します。
- D. 直接接続されたインターフェースをR2に再配布します。

Answer: [A \(メッセージを残す\)](#)

最新問題: 28

R2には、ローカルで発信されたプレフィックス192.168.130.0/24があり、次の設定があります。

```
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
```

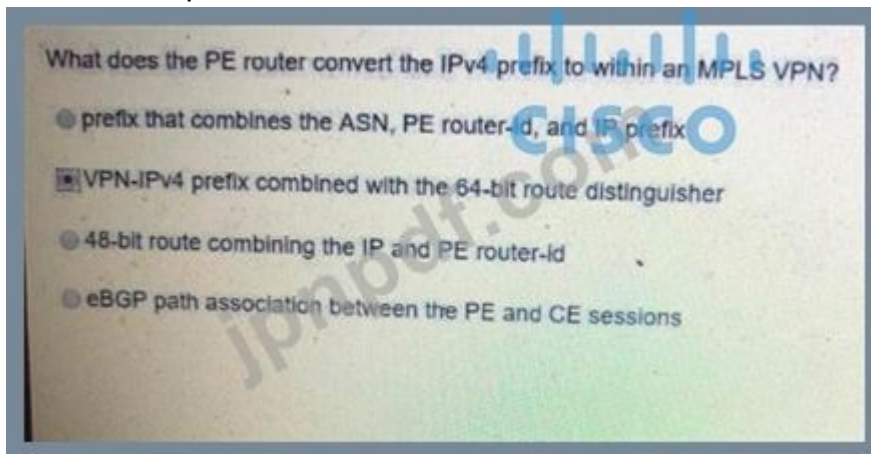
route-mapOUTコマンドをneighbor1.1.1.1route-map OUT outコマンドを使用してeBGPネイバーR1 (1.1.1.1)に適用すると、どのような結果になりますか。

- A. R1は、192.168.130.0 / 24を1つのASホップではなく、2つのASホップとして認識します。
- B. 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
- 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. R1は192.168.130.0/24以外のルートを受け入れません

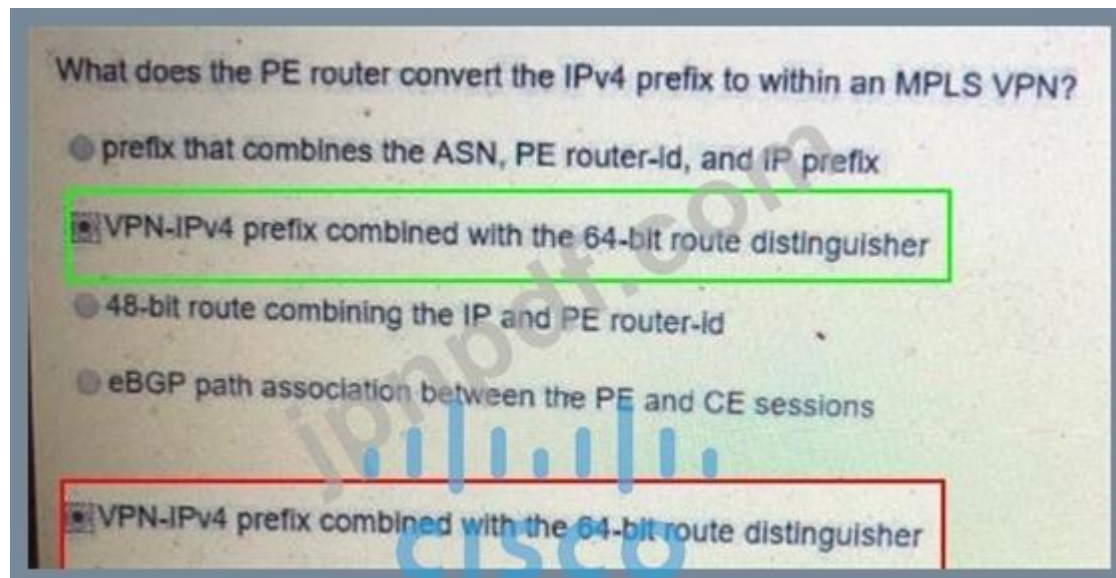
Answer: [\(解答を表示する\)](#)

最新問題: 29

PEルータはIpv4プレフィックスをMPLSVPN内で何に変換しますか？

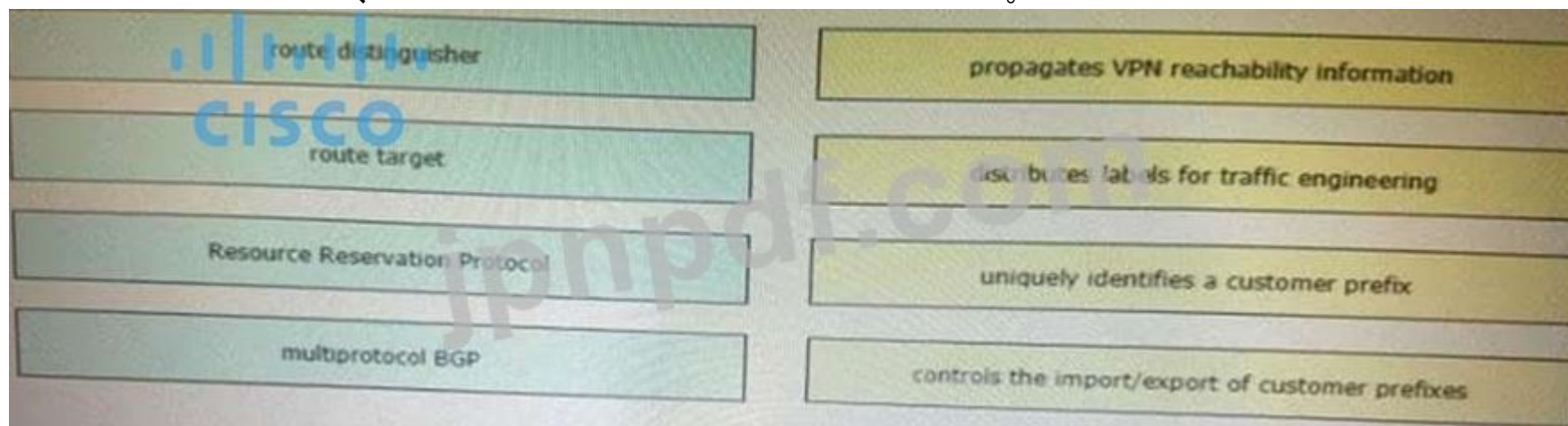


Answer:



最新問題: 30

MPLS VPNの概念を左から、右の正しい説明にドラッグアンドドロップします。



Answer:



説明

マルチプロトコルBGP=VPN到達可能性情報を伝播します

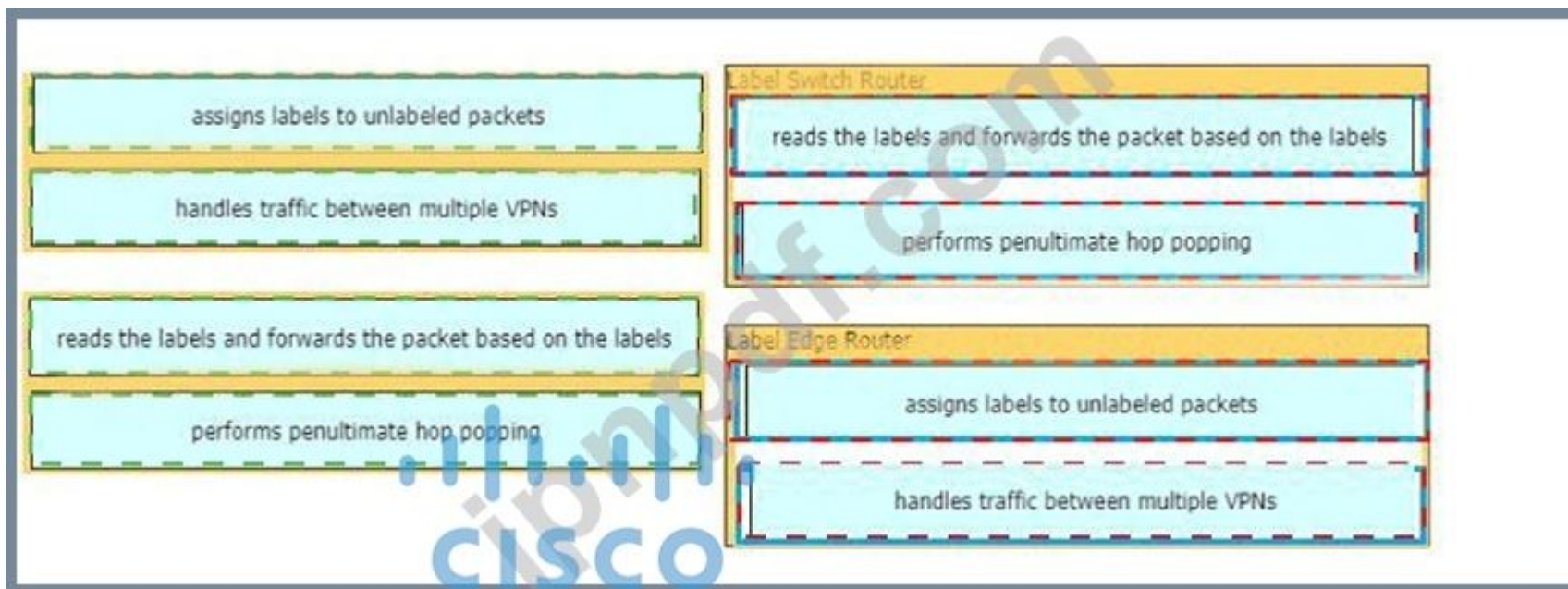
トラフィックエンジニアリング (TE)のラベルを配布するために使用されるリソース予約プロトコル (RSVP)=トラフィックエンジニアリングのラベルを配布するルート識別子=顧客プレフィックスを一意に識別するルートターゲット=顧客プレフィックスのインポート/エクスポートを制御する

最新問題: 31

操作を左から右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を実行します

ラベルエッジルーター :1ラベルとラベルなし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

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をGETする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (800**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **32**

展示を参照してください。

```
config t
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow exporter EXPORTER-1
destination 172.16.10.2
transport udp 90
exit
!
flow monitor FLOW-MONITOR-1
record v4_r1
exit
!
ip cef
!
interface Ethernet0/0.1
ip address 172.16.6.2 255.255.255.0
ip flow monitor FLOW-MONITOR-1 input
!
```

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. フローモニターが間違っただけに適用されています。
- B. フローモニターが間違っただけインターフェースに適用されています。
- C. フローエクスポートの宛先に到達できません。
- D. フローエクスポートは構成されていますが、使用されていません。

Answer: C ([メッセージを残す](#))

最新問題: 33

展示を参照してください。



エンジニアがR1でNetFlowを設定しましたが、NMSサーバーはR1のイーサネット0/0からのフローを確認できません。どの構成で問題が解決しますか？

- A. インターフェイスEthernet0 / 1
ipフローモニターFlowmonitor1入力
ip flowmonitorFlowmonitor1出力
- B. フローモニターFlowmonitor1
ソースEthernet0/0
- C. インターフェイスEthernet0 / 0
ipフローモニターFlowmonitor1入力
ip flowmonitorFlowmonitor1出力
- D. フローエクスポートーFlowAnalyzer1
ソースEthernet0/0

Answer: C (メッセージを残す)

最新問題: 34

アドレスを左側から右側の正しいIPv6フィルター目的にドラッグアンドドロップします。

<pre> permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443 </pre>	<pre> Permit NTP from this source 2001:0D8B:0800:200c::1f </pre>
<pre> permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514 </pre>	<pre> Permit syslog from this source 2001:0D88:0800:200c::1c </pre>
<pre> permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80 </pre>	<pre> Permit HTTP from this source 2001:0D8B:0800:200c::0fff </pre>
<pre> permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123 </pre>	<pre> Permit HTTPS from this source 2001:0D8B:0800:200c::07ff </pre>

Answer:

permit ip 2001:d8b:800:200c:: /117 2001:0DBB:800:2010::/64 eq 443	permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123
permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514	permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514
permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80	permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80
permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123	permit ip 2001:d8b:800:200c:: /117 2001:0DBB:800:2010::/64 eq 443

説明

permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123
permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514
permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80
permit ip 2001:d8b:800:200c:: /117 2001:0DBB:800:2010::/64 eq 443

HTTPとHTTPSはそれぞれTCPポート80と443で実行されるため、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。しかし、2001:d88:800:200c::c/126は2001:d88:800:200c:0:0:0:cから2001:d88:800:200c:0:0:0:fの範囲でしかないため、この質問にはいくつかのタイプミスがあるかもしれません。0:0:f(合辞つのホスト)。ホストは対象外です

2001:0D88:0800:200c::1f、2001:D88:800:200c::e/126についても同じで、

2001:d88:800:200c:0:0:0:cから2001:d88:800:200c:0:0:0:fであり、ホスト2001:0D88:0800:200c::1cは対象外です。

最新問題: 35

```
ip prefix-list DefaultRouteOnly seq 5 deny 0.0.0.0/0 le 32
```

```
ip prefix-list DefaultRouteOnly seq 10 permit 0.0.0.0/0
```

```
router eigrp ccnp
```

```
address-family ipv4 unicast autonomous-system 1
```

```
topology base
```

```
  distribute-list prefix DefaultRouteOnly out Tunnel0
```

展示を参照してください。管理者は、デフォルトルートのみを使用して任意のネットワークに到達するように、リモートの低リソースルーターへのルートアドバタイズメントを構成しましたが、失敗しました。この問題を解決するアクションはどれですか？

- A. シーケンス番号10の行をプレフィックスリストから削除します。
- B. distribute-listコマンドからprefixキーワードを削除します。
- C. distribute-listコマンドの方向をoutからinに変更します。
- D. シーケンス番号5の行をプレフィックスリストから削除します。

Answer: ([解答を表示する](#))

最新問題: 36

展示を参照してください。

```
ip prefix-list DefaultRouteOnly seq 5 deny 0.0.0.0/0 le 32
ip prefix-list DefaultRouteOnly seq 10 permit 0.0.0.0/0

router eigrp ccnp
 address-family ipv4 unicast autonomous-system 1
  topology base
  distribute-list prefix DefaultRouteOnly out Tunnel0
```

展示を参照してください。管理者は、デフォルトルートのみを使用して任意のネットワークに到達するように、リモートの低リソースルーターへのルートアドバタイズメントを構成しましたが、失敗しました。この問題を解決するアクションはどれですか？

- A. distribute-listコマンドからprefixキーワードを削除します。
- B. シーケンス番号5の行をプレフィックスリストから削除します。
- C. シーケンス番号10の行をプレフィックスリストから削除します。
- D. distribute-listコマンドの方向をoutからinに変更します。

Answer: ([解答を表示する](#))

最新問題: 37

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. Ipv6 access-list-Deny_Telnet sequence 10 deny tcp host 198A :0 :200C :: 1/64 host
201A :0 :205C :: 1/64 eq telnet
! int Gi0 / 0

6/39

Ipv6トラフィックフィルター-Deny_Telnetin

!

B. Ipv6 access-list-Deny_Telnet sequence 10 deny tcp host 198A :0 :200C :: 1/64 host
201A :0 :205C :: 1/64 eq telnet
! int Gi0 / 0

Ipv6アクセスマップDeny_Telnetin

!

C. Ipv6 access-list-Deny_Telnet sequence 10 deny tcp host 198A :0 :200C :: 1/64 host
201A :0 :205C :: 1/64 ! int Gi0 / 0

Ipv6アクセスマップDeny_Telnetin

!

D. Ipv6 access-list-Deny_Telnet sequence 10 deny tcp host 198A :0 :200C :: 1/64 host
201A :0 :205C :: 1/64 ! int Gi0 / 0

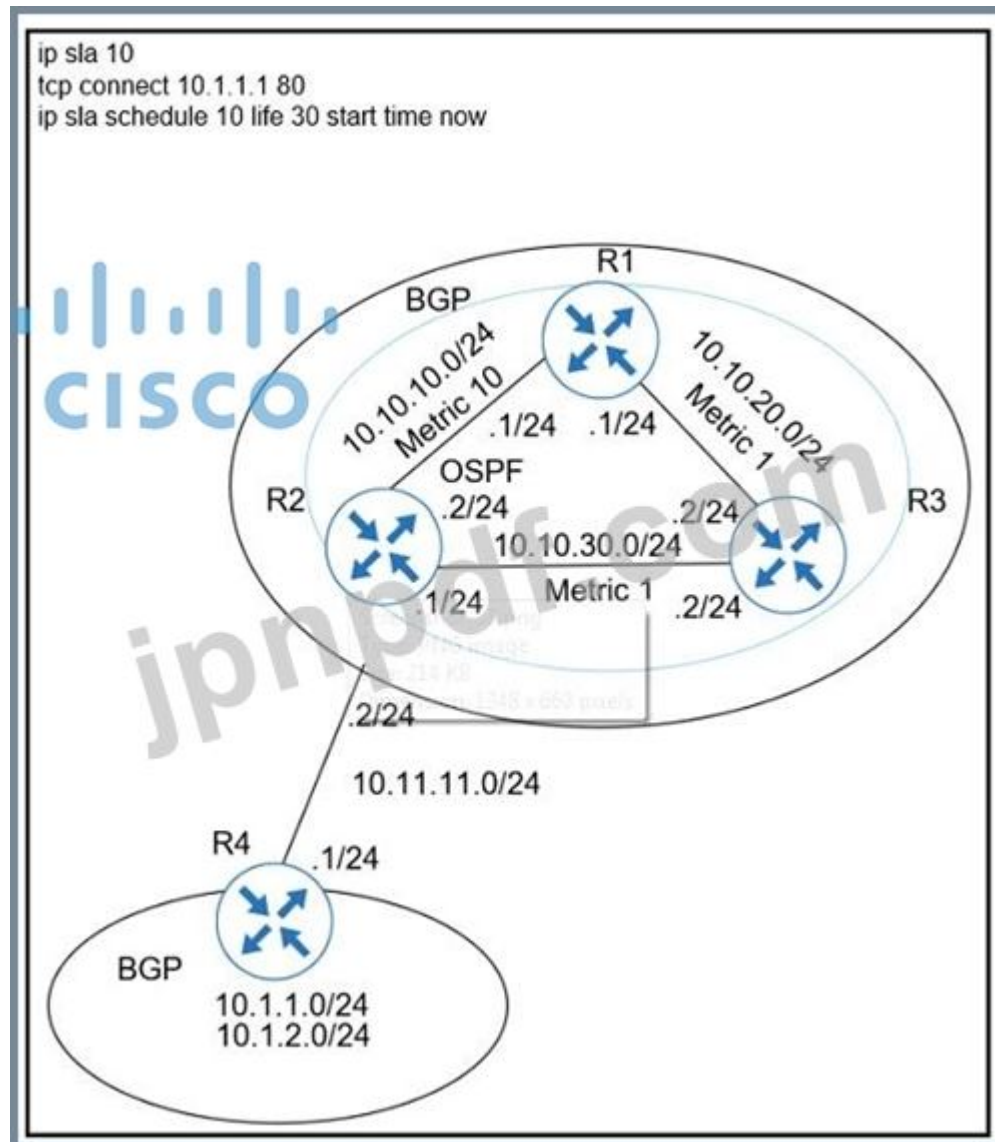
Ipv6トラフィックフィルター-Deny_Telnetin

!

Answer: A (メッセージを残す)

最新問題: 38

展示を参照してください。



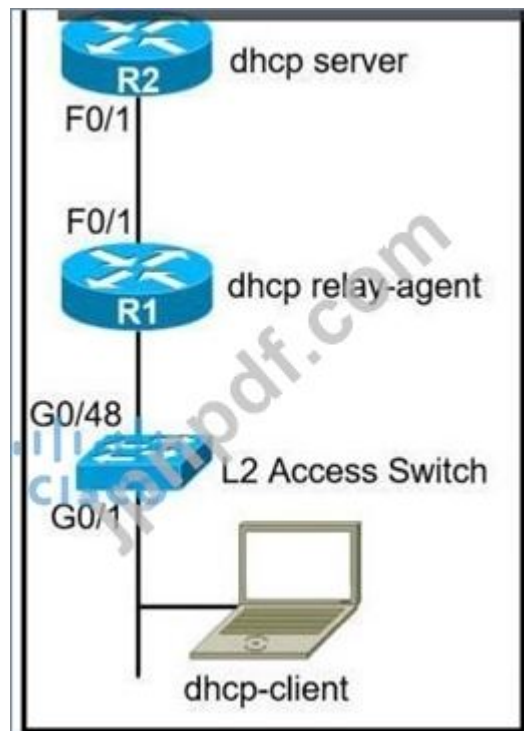
ユーザーは、IPアドレス10.1.1.1上の非SLAホストWebサーバーが展開前にHTTPセッションを受け入れるかどうかをテストするためにIPSLAプローブを設定しました。プローブが故障しています。プローブを成功させるために、ネットワーク管理者はどのアクションを推奨する必要がありますか？

- A. ホストのicmp-echoコマンドを追加します。
- B. 制御無効化オプションをtcp接続に追加します。
- C. ipslaスケジュールの頻度を永久に変更します。
- D. ipslascheduleコマンドを再発行します。

Answer: D ([メッセージを残す](#))

最新問題: 39

展示を参照してください。



ネットワーク管理者は、R1でDHCP検出パケットを確認できます。しかし、R2はDHCP要求に応答していません。R1関連のインターフェイスは、DHCPヘルパーアドレスで設定されます。PCがR2のFaO/1インターフェイスに直接接続されている場合、DHCPサーバーはDHCPプールからPCにIPアドレスとして割り当てます。この問題を解決する2つのコマンドはどれですか？ 2つ選択してください。)

- A. R1のip dhcp relayinformationenableコマンド
- B. R2でのipdhcpリレー情報trust-allコマンド
- C. R2でのip dhcption82コマンド
- D. R1でのservicedhcpコマンド
- E. R1でのservicedhcp-relayコマンド

Answer: C,D (メッセージを残す)

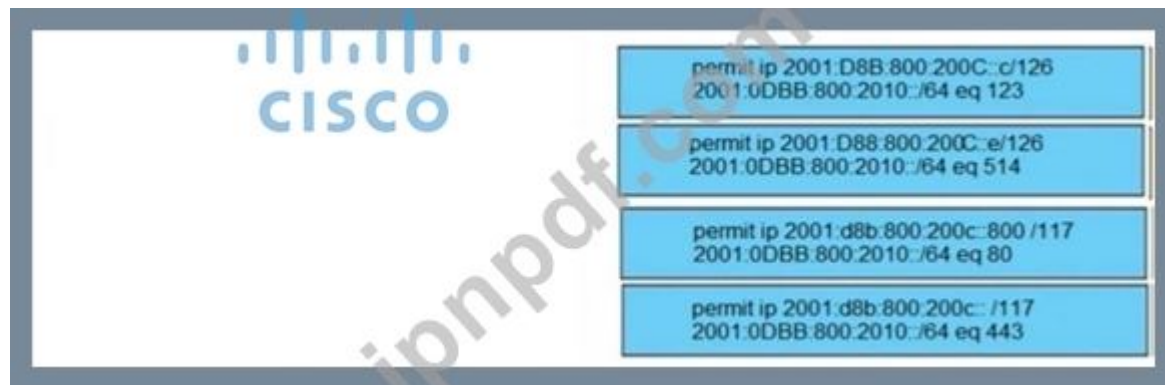
最新問題: 40

ドラッグアンドドロップの質問

アドレスを左側から右側の正しいIPv6フィルター目的にドラッグアンドドロップします。

<pre>permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443</pre>	<pre>Permit NTP from this source 2001:0D8B:0800:200c::1f</pre>
<pre>permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514</pre>	<pre>Permit syslog from this source 2001:0D88:0800:200c::1c</pre>
<pre>permit ip 2001:d8b:800:200c::800/117 2001:0DBB:800:2010::/64 eq 80</pre>	<pre>Permit HTTP from this source 2001:0D8B:0800:200c::0fff</pre>
<pre>permit ip 2001:D8B:800:200C::/126 2001:0DBB:800:2010::/64 eq 123</pre>	<pre>Permit HTTPS from this source 2001:0D8B:0800:200c::07ff</pre>

Answer:



最新問題: 41

ネットワーク管理者は、DMVPNネットワーク上に動的IPを備えた新しいスポークサイトを追加しました。スポークルータからDMVPNトンネルのトラフィックを渡す設定コマンドはどれですか。

- A. ip nhrp registerno-registration
- B. ipnhrp登録no-unique
- C. ipnhrp登録動的
- D. ipnhrp登録は無視します

Answer: B ([メッセージを残す](#))

最新問題: 42

展示を参照してください。

```
admin@linux:~$ scp script.py admin@198.51.100.64:script.py  
Password:  
Administratively disabled.  
admin@linux:~$ Connection to 198.51.100.64 closed by remote  
host.
```

ネットワーク管理者がローカルLinuxマシンで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アクションはどれですか？

- A. SSHサービスは、crypto keygeneratersaコマンドで有効にする必要があります。
- B. Pythonインタプリタは、最初にguestshellenableコマンドで有効にする必要があります。
- C. SCPサービスは、ip scpserverenableコマンドで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: A ([メッセージを残す](#))

最新問題: 43

MPLS用語を左側から右側の正しい定義にドラッグアンドドロップします。

PE	device that forwards traffic based on labels
P	path that the labeled packet takes
CE	device that is unaware of MPLS labeling
LSP	device that removes and adds the MPLS labeling

Answer:



最新問題: 44

展示を参照してください。

```
*Jun 24 08:54:51.530: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:52.525: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*Jun 24 08:54:52.528: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:53.215: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:54.998: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 24 08:54:55.006: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to UP
*Jun 24 08:54:55.998: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

R1はGigabitEthernet0/0を介してR2に接続されており、R2はR1にpingを実行できません。どのようなアクションで問題が解決しますか？

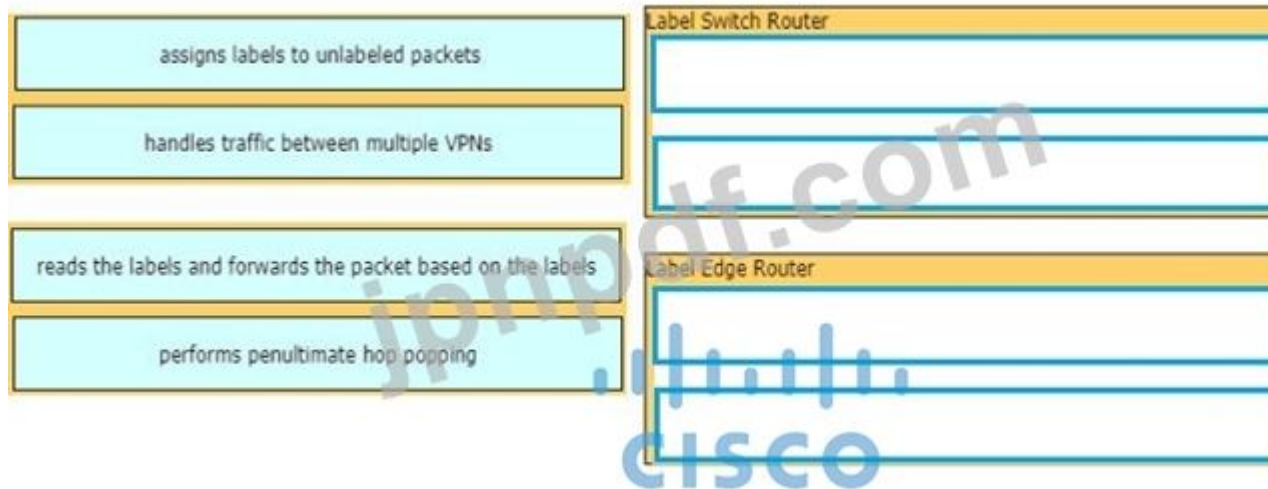
- A. ルータに設定されているルートダンプニングを修正します。
- B. サポートされていないため、SFPモジュールを交換してください。
- C. インターフェイスに設定されているIPイベントダンプニングを修正しました。
- D. 失敗したIPSLAプローブを修正します。

Answer: (解答を表示する)

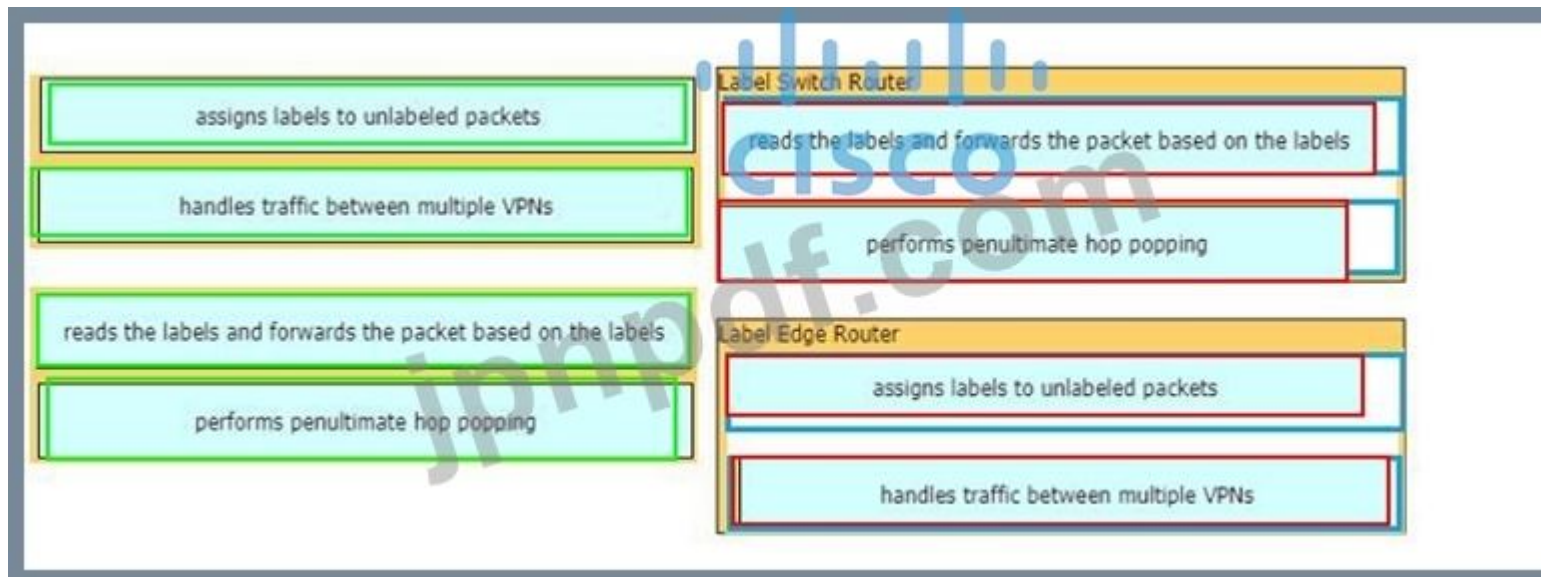
The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively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

最新問題: 45

操作を左から右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。

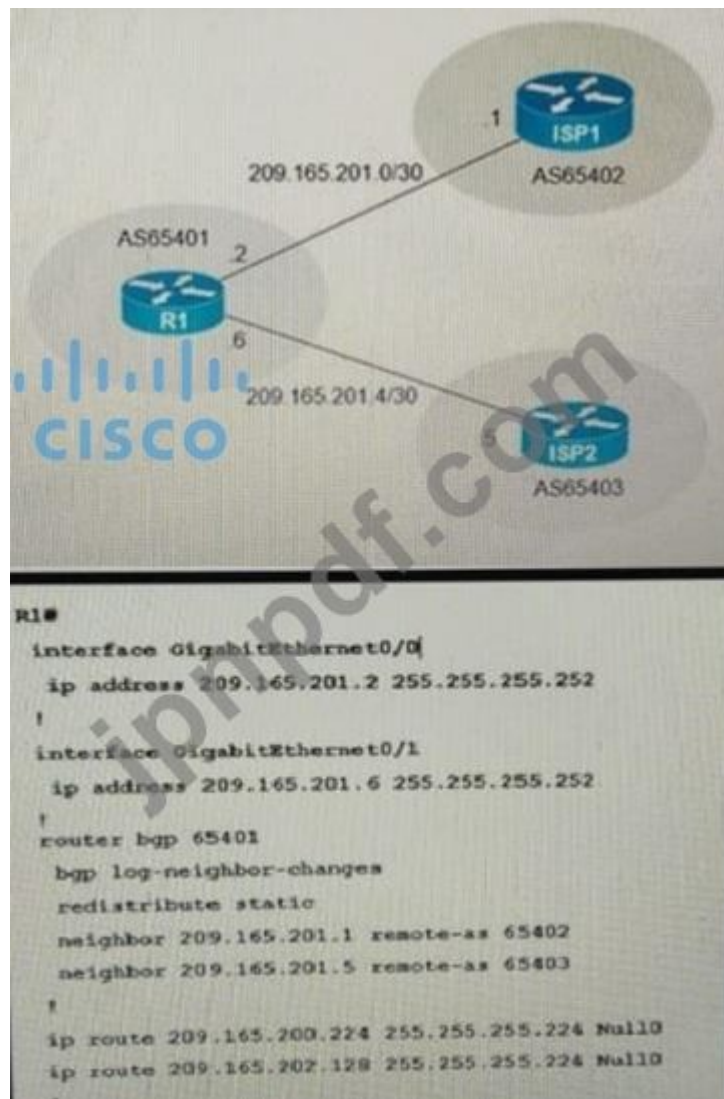


Answer:



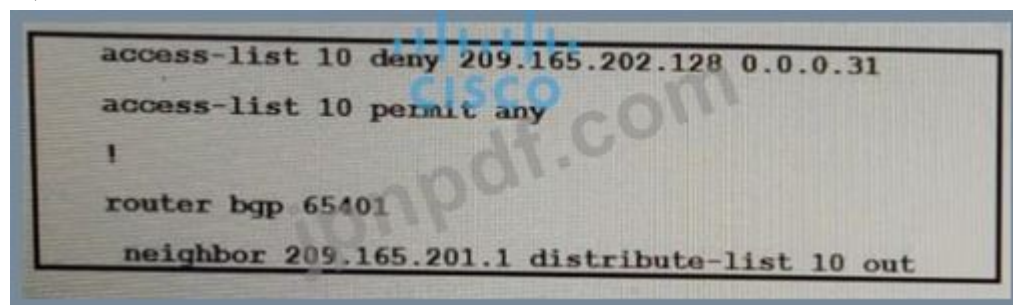
最新問題: 46

展示を参照してください。



自律システム番号AS65401の会社は、ARINからIPアドレスブロック209.165.200.224/27を取得しました。会社はより多くのIPアドレスを必要とし、ISP2からブロック209.165.202.128/27を割り当てられました。エンジニアはISP1であり、AS65401からISP2ルートを受信していると報告しています。R1のどの構成で問題が解決しますか？

A)



B)

```
access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
neighbor 209.165.201.1 distribute-list 10 in
```

C)

```
ip route 209.165.200.224 255.255.255.224 209.165.201.1
ip route 209.165.202.128 255.255.255.224 209.165.201.5
```

D)

```
ip route 0.0.0.0 0.0.0.0 209.165.201.1
ip route 0.0.0.0 0.0.0.0 100 209.165.201.5
```

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

Answer: ([解答を表示する](#))

説明

<https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/23675-27.html>

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 47

IPv6 First-HopSecurity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。

IPv6 DHCPv6 Guard	Block a malicious host and permit the router from a legitimate route.
IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents.
IPv6 Source Guard	Create a binding table that is based on NS and NA messages.
IPv6 RA Guard	Filter inbound traffic on Layer 2 switch ports that are not in the IPv6 binding table.
IPv6 ND Inspection	Create IPv6 neighbors connected to the device from information sources such as NDP snooping.

Answer:

IPv6 DHCPv6 Guard	IPv6 Source Guard
IPv6 Binding Table	IPv6 DHCPv6 Guard
IPv6 Source Guard	IPv6 ND Inspection
IPv6 RA Guard	IPv6 RA Guard
IPv6 ND Inspection	IPv6 Binding Table

最新問題: 48

展示を参照してください。



R1はIPSLAを使用して構成され、R6の背後にあるサーバーの可用性を確認しますが、失敗し続けました。どの構成で問題が解決しますか？

- A. R6 (config) #pslaレスポンドー
- B. R6 (config) #p sla responseer udp-echo ip address 10.10.10.1 port 5000
- C. R6 (config) #p access-list extended DDOS
- R6 (config ext-nac) #5 permit icmp host 10.66 66.66 host 10.10.10.1
- D. R6 (config) #p access-list extended DDOS
- R6 (config ext-nac) #5 permit icmp host 10.10.10.1 host 10.66.66.66

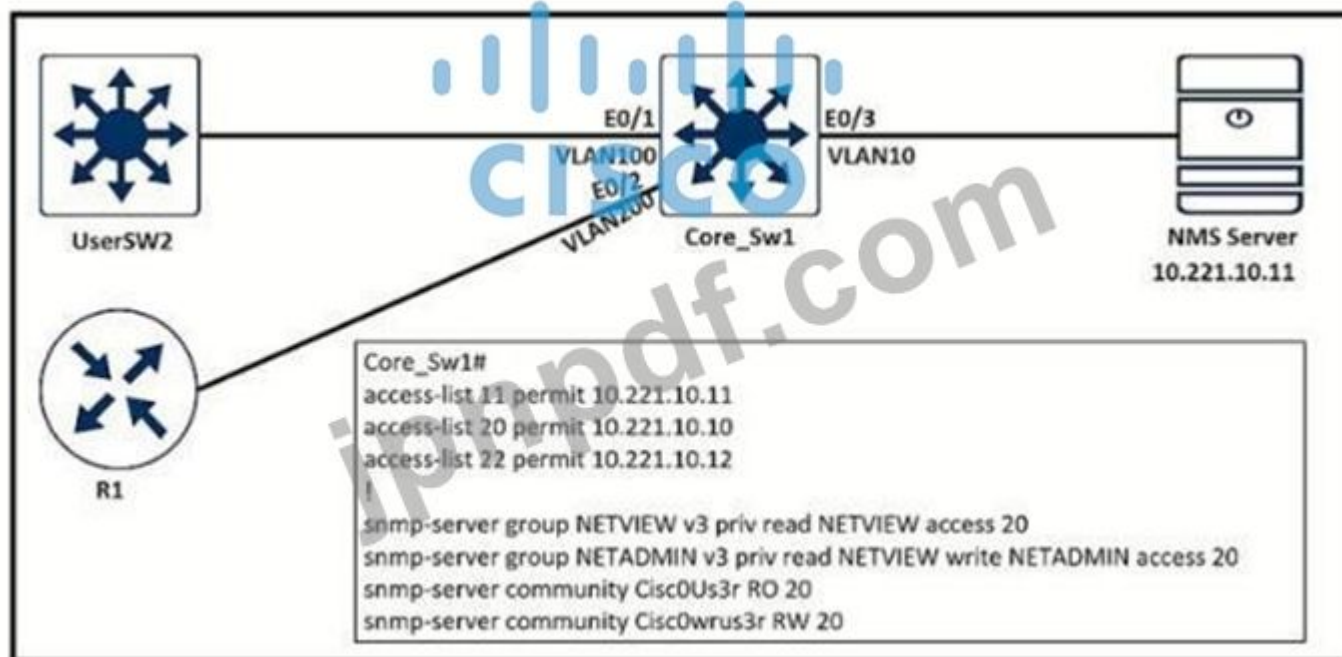
Answer: D (メッセージを残す)

このIPSLAトラッキングでは、IP SLAレスポンドーは必要ないため、R6のコマンド「pslaresponder」は必要ありません。

また、ACLがR6の両方のインターフェイスE0/0とE0/1でICMPパケットをブロックしているため、送信元10.10.10.1から宛先10.66.66.66へのICMPを許可する必要があります。

最新問題: 49

展示を参照してください。



エンジニアがCore_SW1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。この問題を解決する構成はどれですか？

- A. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22
- B. アクセスリスト20許可10.221.10.12
- C. snmp-server group NETVIEW v2c priv read NETVIEW access 20
- D. アクセスリスト20許可10.221.10.11

Answer: D ([メッセージを残す](#))

最新問題: 50

別紙を参照してください。

```

Ipv6 unicast-routing
!
Router ospfv3 4
  Router-id 192.168.1.1
!
Interface E 0/0
  Ipv6 enable
  Ip address 10.1.1.1 255.255.255.0
  Ospf3 4 area 0 ipv4
  No shut
!
Interface Loopback0
  Ipv6 enable
  Ipv4 172.16.1.1 255.255.255.0
  Ospf3 4 area 0 ipv4

```

ネットワーク管理者は、E0/0インターフェイスでIPv6用にブランチルーターを構成しました。隣接ルーターは要件を満たすように完全に構成されていますが、隣接ルーターの関係は確立されていません。IPv6ネイバーを起動するために、ブランチルーターの問題を修正するアクションはどれですか。

- A. address-family ipv4 unicastコマンドを使用して、ルータospfv34プロセスでIPv4アドレスファミリーを有効にします。
- B. no ipv6 enableコマンドを使用して、E0/0インターフェイスでIPv6を無効にします

C. address-family ipv4 unicastコマンドを使用して、E0/0インターフェイスでIPv4アドレスファミリーを有効にします。

D. E0/0インターフェイスでnoospfv3 area 0 ipv4コマンドを使用して、IPv4のOSPFを無効にします。

Answer: A (メッセージを残す)

説明

もう一度、シスコはOSPFv3設定に必要なIOS設定コマンドを変更しました。新しいOSPFv3設定では、以前の「ipv6routerospf」ルーティングプロセスコマンドおよび「ipv6ospf」インターフェイスコマンドの代わりに「ospfv3」キーワードが使用されます。

Open Shortest Path Firstバージョン3 (OSPFv3) アドレスファミリー機能により、IPv4とIPv6の両方のユニキャストトラフィックをサポートできます。この機能を使用すると、ユーザーはインターフェイスごとに2つのプロセスを持つことができますが、アドレスファミリー (AF) ごとに1つのプロセスしかありません。

最新問題: 51

展示を参照してください。

ネットワーク管理者は、TCPリターンフレームのみを許可するようにIPv6アクセスリストを設定しましたが、期待どおりに機能していません。この問題を解決する変更はどれですか？

ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out

ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log
interface gi0/0
ipv6 traffic-filter inbound out

ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in

ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in

A. オプションA

B. オプションB

C. オプションC

D. オプションD

Answer: C ([メッセージを残す](#))

説明

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/122_55_se/configuration/e/scg3750/swv6acl.html

最新問題: 52

展示を参照してください。

```
R1(config)# ip route 0.0.0.0 0.0.0.0 1.1.1.1
R1(config)# ip route 0.0.0.0 0.0.0.0 2.2.2.2 10
R1(config)# ip sla 1
R1(config)# icmp-echo 1.1.1.1 source-interface FastEthernet0/0
R1(config)# ip sla schedule 1 life forever start-time now

R1(config)# track 1 ip sla 1 reachability
```

IP SLAは、プライマリがダウンしているときにバックアップのデフォルトルートを使用するように設定されていますが、期待どおりに機能していません。どのコマンドで問題が解決しますか？

- A. R1 (config) #ip route 0.0.0.0 0.0.0.0 2.2.2.2 10 track 1
- B. R1 (config) #ip route 0.0.0.0 0.0.0.0 1.1.1.1 track 1
- C. R1 (config)#ip sla track 1
- D. R1 (config) #ip route 0.0.0.0 0.0.0.0 2.2.2.2

Answer: B ([メッセージを残す](#))

最新問題: 53

ネットワーク管理者は、NMSによって報告されたルーターのルートプロセッサの使用率の高い問題のトラブルシューティングを行っています。管理者は、ルーターにログインしてコントロールプレーンのポリシングを確認し、BGPプロセスが多数のルーティングパケットをドロップして数千を引き起こしていることを確認しました。頻繁に再計算するルートの。この問題を解決するソリューションはどれですか？

- A. BGP、conform-action set-prec-transmit、およびexceedactionset-clp-transmitのpirをポリシングします。
- B. BGPのpirを整形し、conform-action set-prec-transmitを実行し、actionset-frde-transmitを超えます。
- C. BGP、適合アクション送信、および超過アクション送信のサーをポリシングします。
- D. BGPのcirを形成します。適合アクション送信、および超過アクション送信。

Answer: B,C ([メッセージを残す](#))

最新問題: 54

展示を参照してください。

```
Global RADIUS shared secret:*****
retransmission count:5
timeout value:10
following RADIUS servers are configured:
  myradius.cisco.users.com:
    available for authentication on port:1814
    available for accounting on port:1813
  10.1.1.1:
    available for authentication on port:1814
    available for accounting on port:1813
  RADIUS shared secret:*****
  10.2.2.3:
    available for authentication on port:1814
    available for accounting on port:1813
  RADIUS shared secret:*****
```

AAAサーバ10.1.1.1はデフォルトの認証およびアカウントング設定で設定されていますが、スイッチがサーバと通信できません。この問題を解決するアクションはどれですか。

- A. 認証ポートと一致します
- B. アカウント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 (メッセージを残す)

コマンドのデフォルト

アカウントングポート :1813

認証ポート :1812

アカウントング : 有効

認証 : 有効

再送信回数 :1

アイドル時間 :0

サーバー監視 : 無効

タイムアウト :5秒

ユーザー名のテスト :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

最新問題: 55

Cisco DNA Centerでデバイスをプロビジョニングすると、エンジニアには「デバイスを選択できません。テンプレートと互換性がありません」というエラーメッセージが表示されます。

エラーの理由は何ですか？

- A. テンプレートの構成が正しくありません。
- B. テンプレートのソフトウェアバージョンがデバイスのソフトウェアバージョンと異なります。
- C. テンプレートへの変更はコミットされませんでした。

D. テンプレートのフィルタリングに使用されたタグがデバイスタグと一致しません。

Answer: ([解答を表示する](#))

タグを使用してテンプレートをフィルタリングする場合は、テンプレートを適用するデバイスに同じタグを適用する必要があります。そうしないと、プロビジョニング中に次のエラーが発生します。-デバイスを選択できません。テンプレートとの互換性はありません。

参照：

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-10/user_guide/b_cisco_dna_center_ug_1_2_10/b_dnac_ug_1_2_10_chapter_0111.html

最新問題: 56

R2には、ローカルで発信されたプレフィックス192.168.130.0/24があり、次の設定があります。

```
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
```

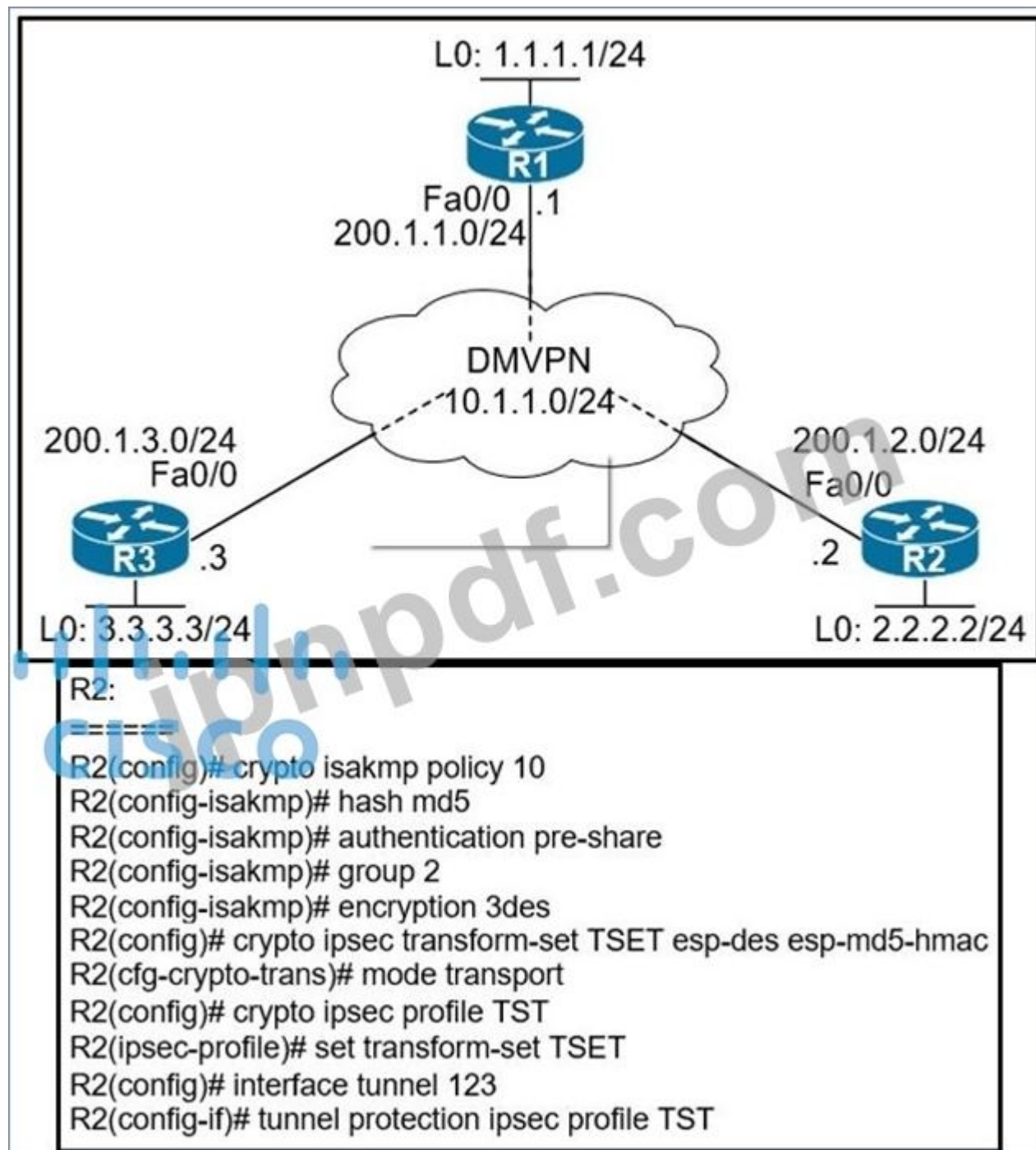
route-mapOUTコマンドをneighbor1.1.1.1route-map OUT outコマンドを使用してeBGPネイバーR1 (1.1.1.1)に適用すると、どのような結果になりますか。

- A. R1は、192.168.130.0 / 24を1つのASホップではなく、2つのASホップとして認識します。
- B. 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
- 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. R1は192.168.130.0/24以外のルートを受け入れません

Answer: ([解答を表示する](#))

最新問題: 57

展示品をご覧ください。



DMVPNが構成されている場合、トンネルソースとしてループバックを使用するスポークツースポーク通信を許可する構成はどれですか。

- A. ハブでcrypto isakmpkeyciscoアドレス0.0.0.0を設定します。
- B. ハブでcryptoisakmpキーCiscoアドレス200.1.0.0255.255.0.0を設定します。
- C. スポークにcrypto isakmpkeyciscoアドレス200.1.0.0255.255.0.0を設定します。
- D. スポークにcrypto isakmpkeyciscoアドレス0.0.0.0を設定します。

Answer: ([解答を表示する](#))

説明

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

最新問題: 58

展示を参照してください。

```
Cat3850-Stack-2# show policy-map
```

```
Policy Map LIMIT_BGP
```

```
Class BGP
```

```
drop
```

```
Policy Map SHAPE_BGP
```

```
Class BGP
```

```
Average Rate Traffic Shaping
```

```
cir 10000000 (bps)
```

```
Policy Map POLICE_BGP
```

```
Class BGP
```

```
police cir 1000k bc 1500
```

```
conform-action transmit
```

```
exceed-action transmit
```

```
Policy Map COPP
```

```
Class BGP
```

```
police cir 1000k bc 1500
```

```
conform-action transmit
```

```
exceed-action drop
```

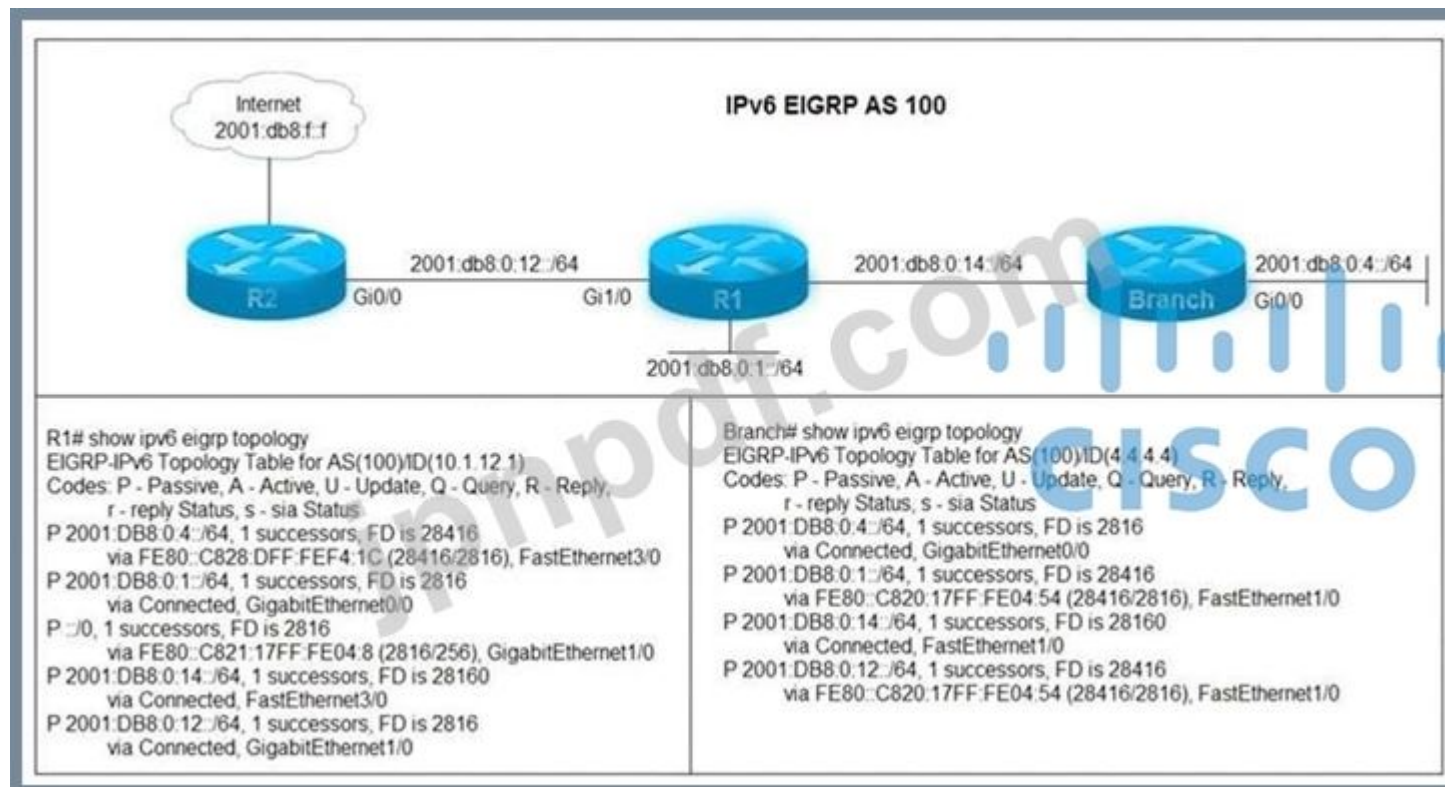
CPU宛てのBGPトラフィックを1Mbpsに制限し、より高速で送信されるBGPトラフィックを無視するコントロールプレーンポリシーはどれですか。

- A. ポリシーマップSHAPE_BGP
- B. ポリシーマップLIMIT_BGP
- C. ポリシーマップPOLICE_BGP
- D. ポリシーマップCOPP

Answer: D ([メッセージを残す](#))

最新問題: 59

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ために、IPv6ルータEIGRP100コンフィギュレーションモードで発行されるコマンドはどれですか。

- A. R1でeigrpスタブコマンドを発行します。
- B. R1でnoeigrpスタブコマンドを発行します
- C. R2でnoeigrpスタブコマンドを発行します。
- D. R2でeigrpスタブコマンドを発行します。

Answer: B ([メッセージを残す](#))

最新問題: 60

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つ選択してください。)

- A. debug snmpv3 engine-id
- B. showsnmpv3ユーザー
- C. debug snmp engine-id
- D. snmpユーザー
- E. snmpパケットをデバッグします

Answer: B,D (メッセージを残す)

最新問題: 61

```
ipv6 access-list inbound
permit tcp any any
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound out
```

展示を参照してください。ネットワーク管理者は、TCPリターントラフィックのみを許可するようにIPv6アクセスリストを設定しましたが、期待どおりに機能していません。この問題を解決する変更はどれですか？

- A. ipv6アクセスリストインバウンド
tcp anyanysynを許可する

ipv6をすべてのログで拒否します

！

インターフェイスgi0/0

ipv6traffic-filterインバウンドイン

B. ipv6アクセスリストインバウンド

確立された任意のtcpを許可する

ipv6をすべてのログで拒否します

！

インターフェイスgi0/0

ipv6traffic-filterインバウンドアウト

C. ipv6アクセスリストインバウンド

確立された任意のtcpを許可する

ipv6をすべてのログで拒否します

！

インターフェイスgi0/0

ipv6traffic-filterインバウンドイン

D. ipv6アクセスリストインバウンド

tcp anyanysynを許可する

ipv6をすべてのログで拒否します

！

インターフェイスgi0/0

ipv6traffic-filterインバウンドアウト

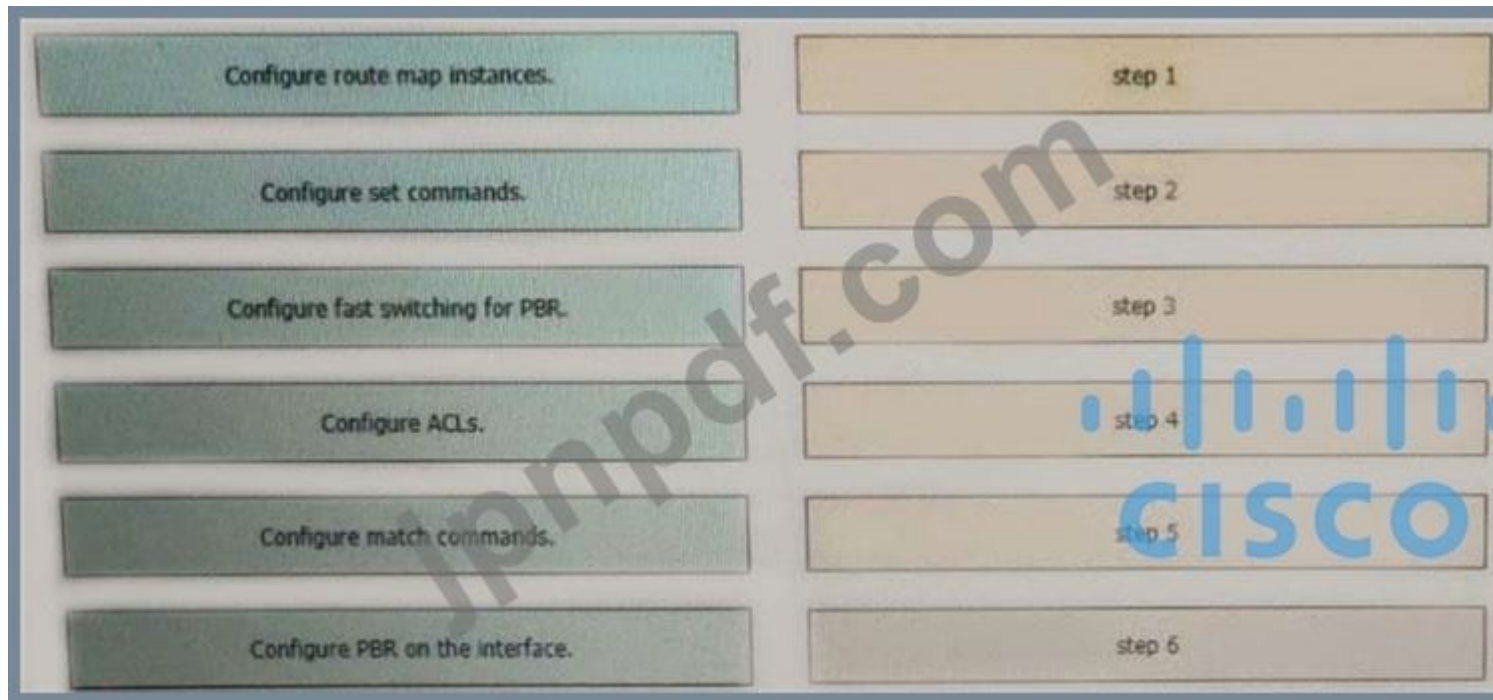
Answer: ([解答を表示する](#))

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード:

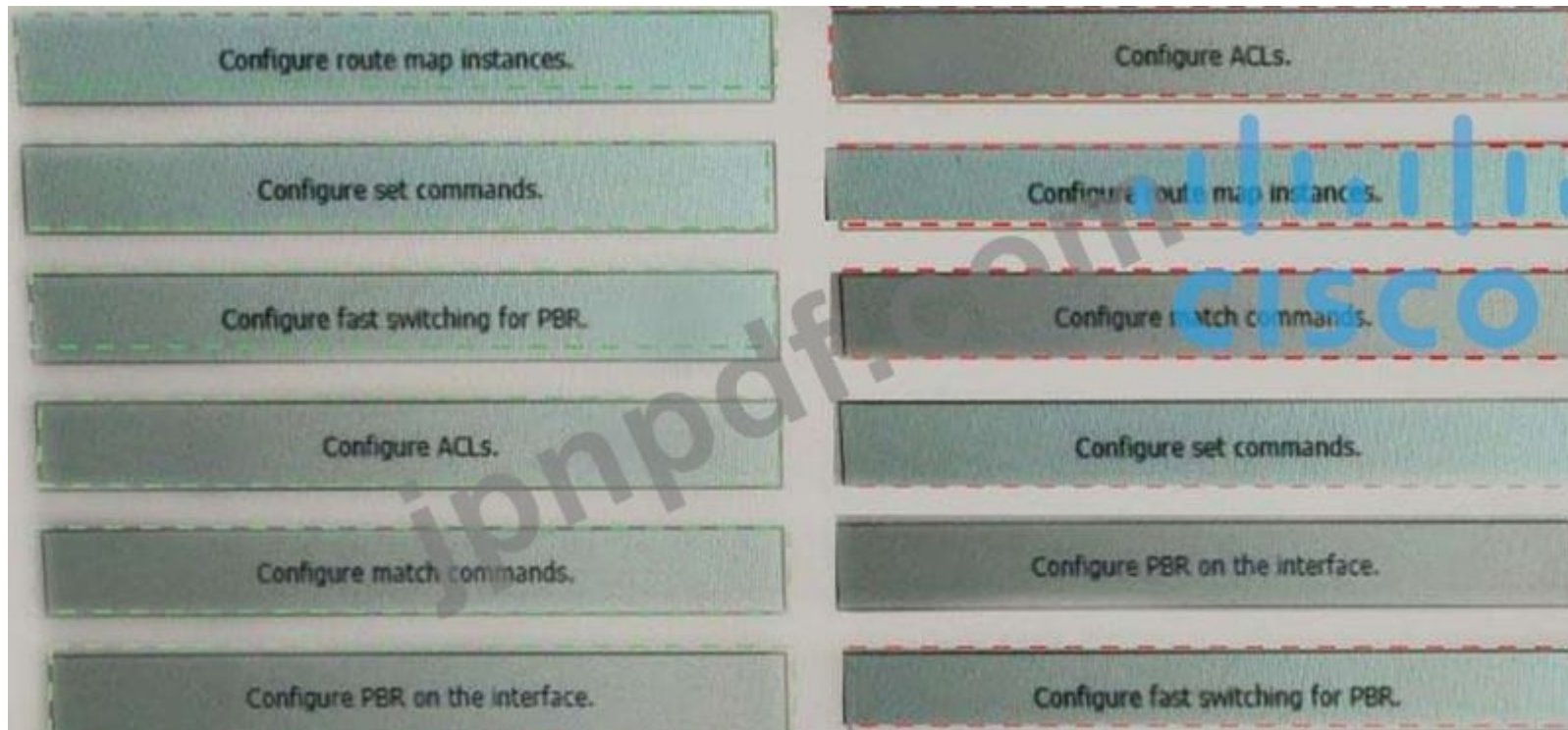
Freepdfdumps)

最新問題: **62**

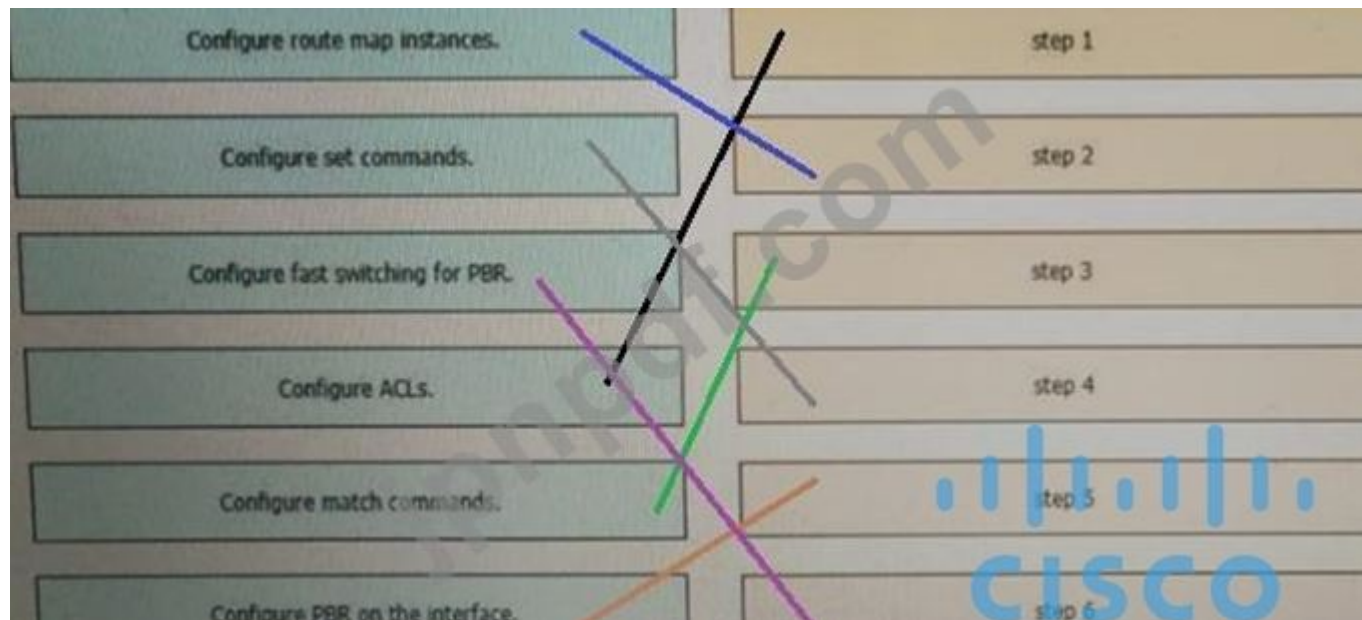
アクションを左側から右側の正しい順序にドラッグアンドドロップして、通常のルーティングパスに基づくパケット転送に従わないようにポリシーを構成します。



Answer:



説明



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

最新問題: 63

展示を参照してください。

```
BRANCH-RTR#
router eigrp 100
 network 10.4.31.0 0.0.0.7
 network 10.100.100.1 0.0.0.0
 distribute-list route-map FILTER-IN in FastEthernet0/0
 eigrp router-id 10.100.100.1
!
ip prefix-list 102 seq 10 permit 10.1.1.100/32
!
route-map FILTER-IN deny 10
 match ip address prefix-list 102
!
```

ジュニアエンジニアがブランチルータの設定を更新しました。変更直後、エンジニアはヘルプデスクから、支店の担当者がネットワークの宛先に到達できないという電話を受けます。どの構成がサービスを復元し、10.1.1.100 / 32をブロックし続けますか？

- A. route-map FILTER-IN deny 5
- B. ip prefix-list 102 seq 15 permit 0.0.0.0/32 le 32
- C. ip prefix-list 102 seq 5 permit 0.0.0.0/32 le 32
- D. ルートマップFILTER-IN許可20

Answer: ([解答を表示する](#))

説明

ルートマップで「deny」キーワードを使用することにより、prefix-listで指定されたプレフィックスを除外できます。

ただし、プレフィックスリストには暗黙の「denyall」ステートメントがあるため、ルートマップで「permit」キーワードを使用して他のプレフィックスを許可する必要があります。

最新問題: 64

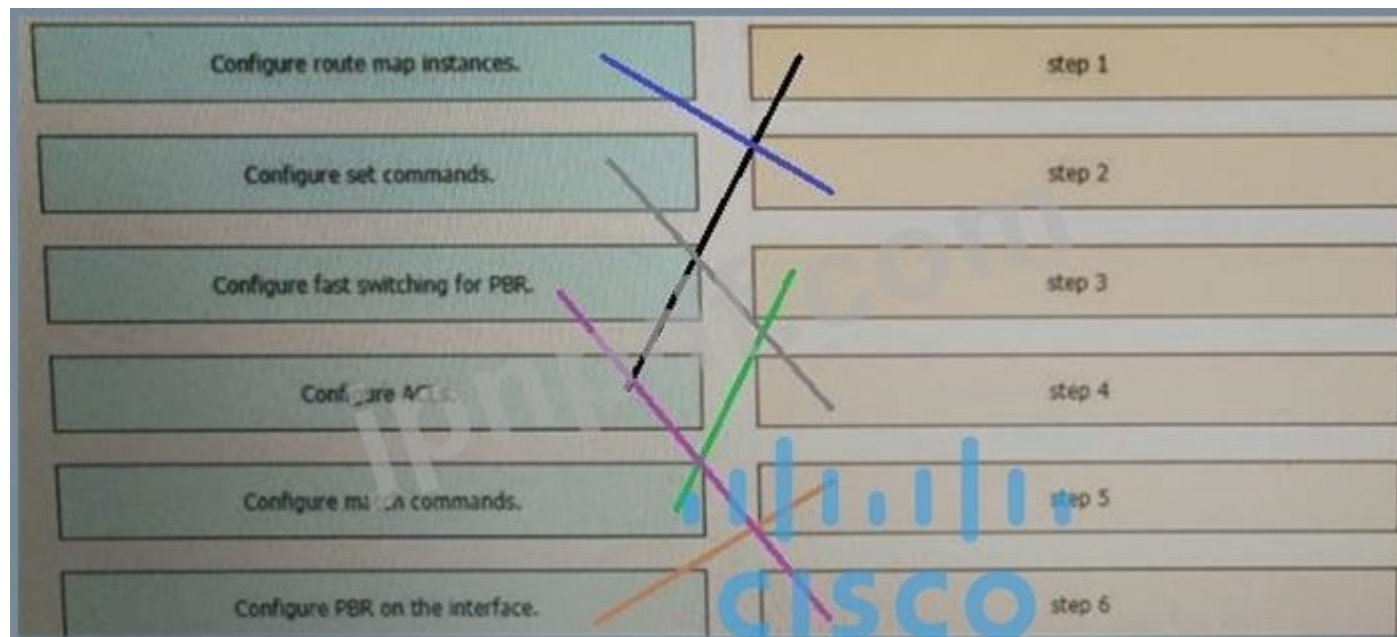
アクションを左側から右側の正しい順序にドラッグアンドドロップして、通常のルーティングパスに基づくパケット転送に従わないようにポリシーを構成します。

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

Answer:

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

説明



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

最新問題: 65

エンジニアが、インストール中にCiscoDNACenterエンタープライズインターフェイスに誤ったデフォルトゲートウェイを設定しました。構成を修正するには、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. sudomaglev-configアップデート
- B. sudo maglev install config update
- C. sudomaglevの再インストール
- D. sudo update config install

Answer: A (メッセージを残す)

セクション :インフラストラクチャサービス

説明/参照 :

最新問題: 66

LDPセッションの形成に使用されるトランスポート層プロトコルはどれですか？

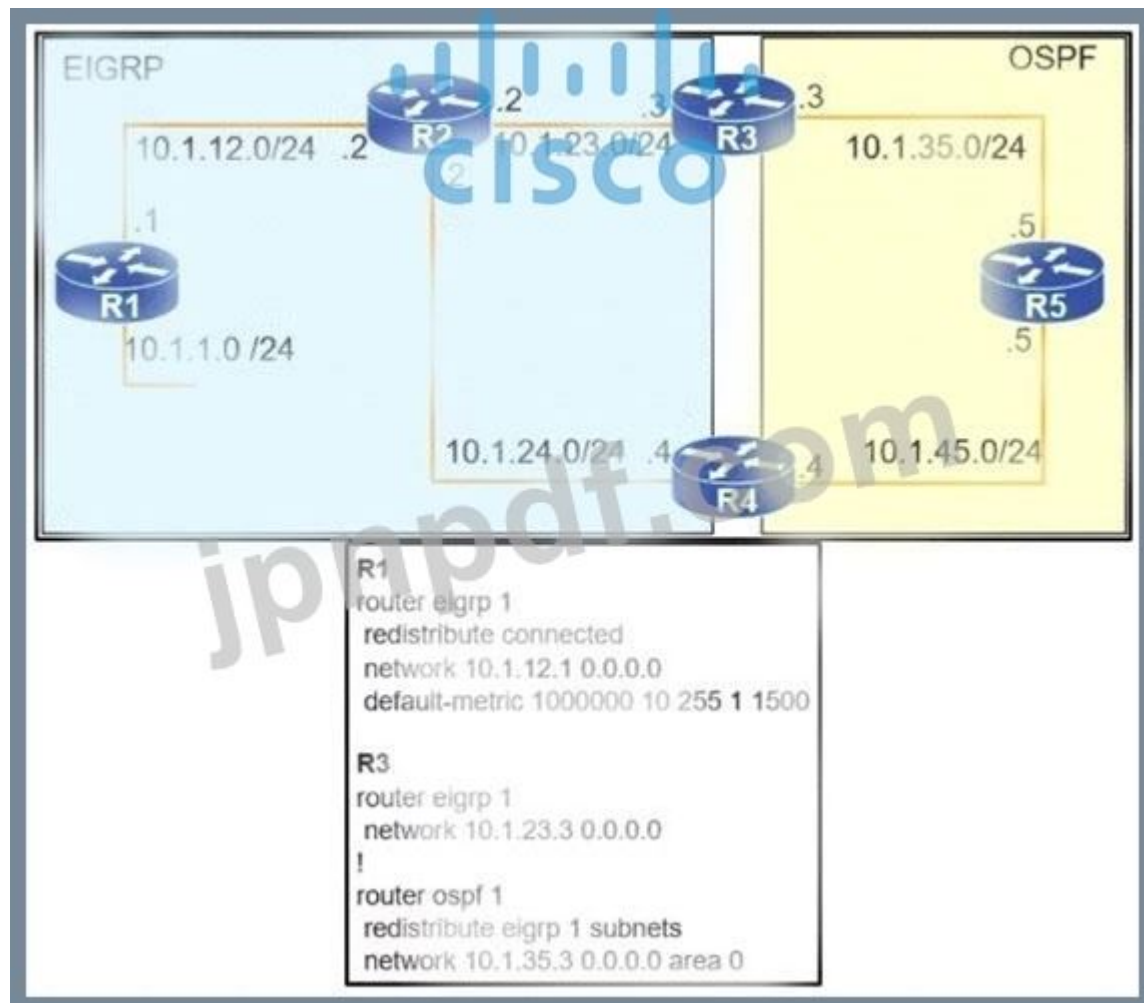
- A. UDP
- B. SCTP
- C. TCP
- D. RDP

Answer: C (メッセージを残す)

LDPは、ネイバーを検出するために、helloメッセージを既知のUDPポート (646)にマルチキャストします。検出が完了すると、TCP接続 (ポート646)が確立され、LDPセッションが開始されます。LDPキープアライブは、セッションの正常性を保証します。LDPセッションのおかげで、LDPメッセージはFECに必要なラベルマッピングを作成します。撤回メッセージは、FECを破棄する必要がある場合に使用されます。

最新問題: 67

展示を参照してください。



R5からネットワーク10.1.1.0/24に到達可能性を提供するために、ネットワーク管理者はEIGRPをR3のOSPFに再配布しますが、R4がR5を介して.....パスを使用して10.1.1.0/24に到達していることに気が付きます。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、問題を修正するアクションはどれですか？

- A. R5でOSPFの管理距離を200に変更します。
- B. 外部EIGRPの管理距離を90に変更します。
- C. OSPFのR4に向けてR5のアウトバウンド配布リストを適用します。

Answer: B ([メッセージを残す](#))

最新問題: 68

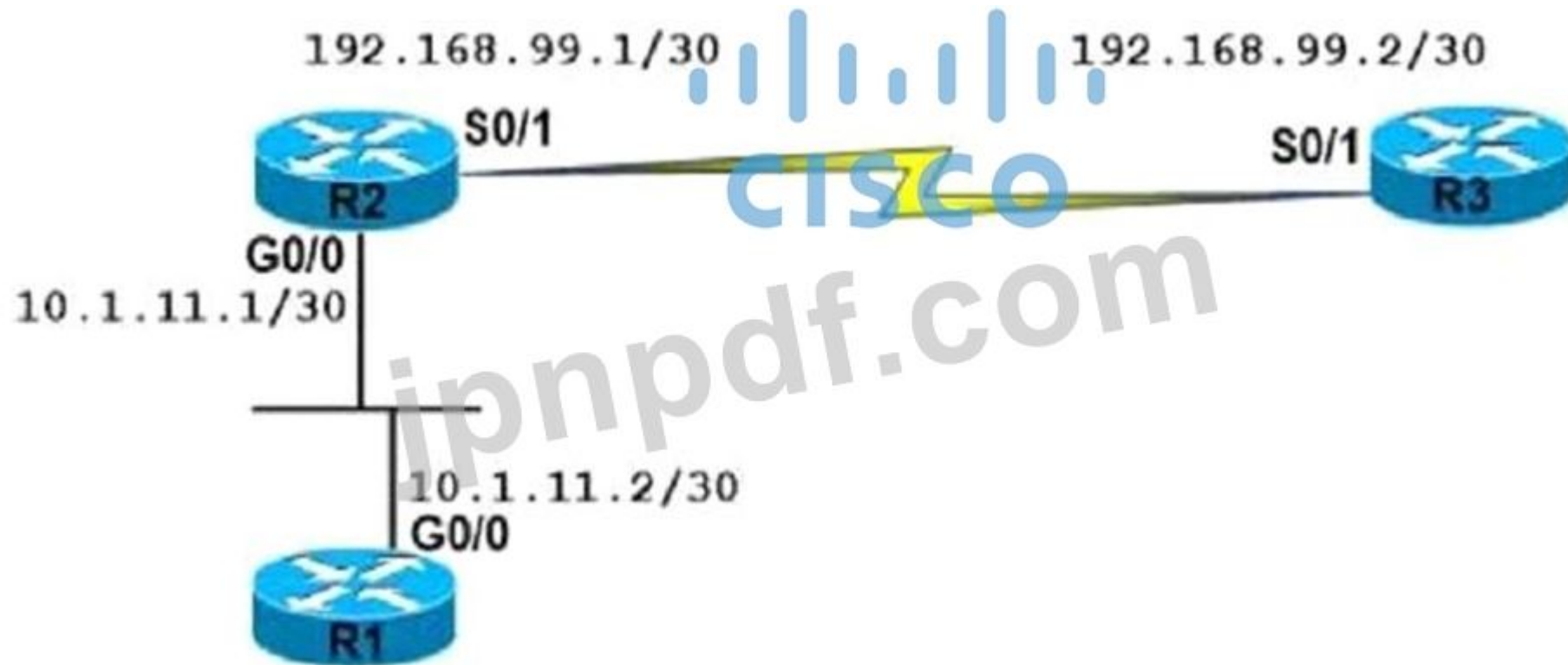
展示を参照してください。

```

R2# show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
192.168.99.2     1    EXCHANGE/      -          00:00:36   192.168.99.1  Serial0/1
router-6#

R3# show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
192.168.99.1     1    EXSTART/       -          00:00:33   192.168.99.2  Serial0/1

```



R2とR3の間のOSPFネイバー関係は、EXCHANGE/EXSTART状態でスタックしていることを示しています。ネイバーはR1とR2の間に確立されます。ネットワークエンジニアはR2からR3に、またはその逆にpingを実行できますが、ネイバーはまだダウンしています。問題を解決するアクションはどれですか？

- A. ISPネットワークのレイヤー2/レイヤー3の接続性の問題を復元します。
- B. インターフェイスでOSPFを有効にします。これは必須です。
- C. 両方のルーターインターフェイスを管理上「シャットダウンしてからシャットダウンしない」。
- D. 両方のルーターインターフェイスでMTUを一致させるか、MTUを無視します。

Answer: [\(解答を表示する\)](#)

最新問題: 69

展示を参照してください。

```

R1#show policy-map control-plane
Control Plane
Service-policy input: CoPP
Class-map: PERMIT (match-all)
 50 packets, 3811 bytes
 5 minute offered rate 0000 bps
 Match: access-group 100
Class-map: ANY (match-all)
 210 packets, 19104 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: access-group 199
 drop
Class-map: class-default (match-any)
 348 packets, 48203 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: any

R1#show access-list 100
Extended IP access list 100
 10 permit udp any any eq 23 (100 matches)
 20 permit tcp any any eq telnet (5 matches)
 30 permit tcp any eq telnet any (10 matches)

R1#show access-list 199
Extended IP access list 199
 10 deny tcp any eq telnet any (50 matches)
 50 permit ip any any (1 match)

R1#show running-config | section line vty
line vty 0 4
 login
 transport input telnet ssh
 transport output telnet ssh

```

SSHによるルーターR1へのアクセスを制限する2つのアクションはどれですか？ (2つ選択してください。)

- A. 行vtyでトランスポート出力sshを設定し、アクセスリスト100からシーケンス20を削除します。
- B. 行vtyでトランスポート出力sshを設定し、アクセスリスト199からシーケンス10を削除します。
- C. アクセスリスト100からシーケンス10を削除し、シーケンス20を追加してアクセスリストへの任意のeqtelnetを拒否します。
- D. 行vtyでトランスポート入力sshを設定し、アクセスリスト100からシーケンス30を削除します。
- E. service-policyCoPPからclass-mapANYを削除します

Answer: A,C (メッセージを残す)

最新問題: 70

展示を参照してください。

```
R1#show policy-map control-plane
Control Plane
Service-policy input: CoPP
Class-map: PERMIT (match-all)
 50 packets, 3811 bytes
 5 minute offered rate 0000 bps
 Match: access-group 100
Class-map: ANY (match-all)
 210 packets, 19104 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: access-group 199
 drop
Class-map: class-default (match-any)
 348 packets, 48203 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: any

R1#show access-list 100
Extended IP access list 100
 10 permit udp any any eq 23 (100 matches)
 20 permit tcp any any eq telnet (5 matches)
 30 permit tcp any eq telnet any (10 matches)

R1#show access-list 199
Extended IP access list 199
 10 deny tcp any eq telnet any (50 matches)
 50 permit ip any any (1 match)

R1#show running-config | section line vty
line vty 0 4
 login
 transport input telnet ssh
 transport output telnet ssh
```

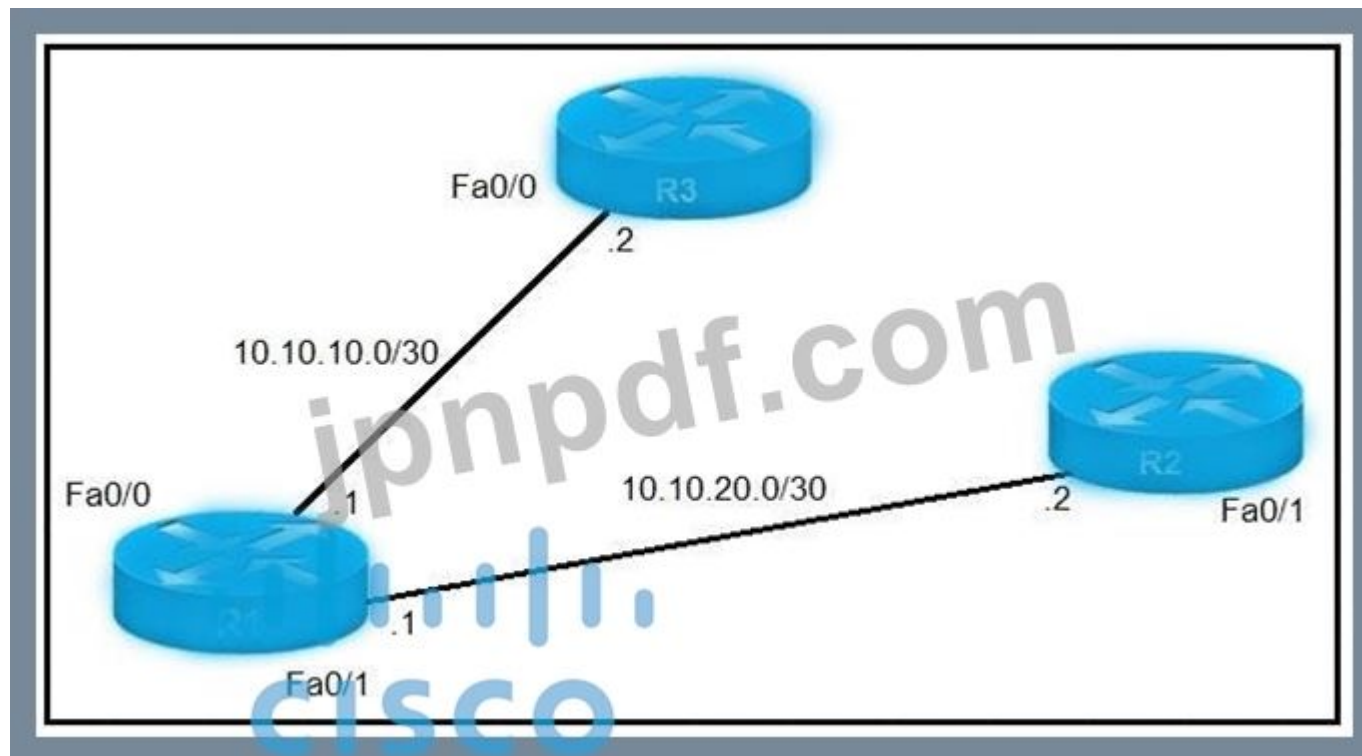
SSHによるルーターR1へのアクセスを制限する2つのアクションはどれですか？ (2つ選択してください。)

- A. 行vtyでトランスポート出力sshを設定し、アクセスリスト199からシーケンス10を削除します。
- B. 行vtyでトランスポート出力sshを設定し、アクセスリスト100からシーケンス20を削除します。
- C. service-policyCoPPからclass-mapANYを削除します
- D. アクセスリスト100からシーケンス10を削除し、シーケンス20を追加して、アクセスリスト199への任意のeqtelnetのtcpを拒否します。
- E. 行vtyでトランスポート入力sshを設定し、アクセスリスト100からシーケンス30を削除します。

Answer: ([解答を表示する](#))

最新問題: 71

展示を参照してください。



IP SLAがルータR1に設定され、Fa0/0がルータR3Fa0/0インターフェイスとの到達可能性を失った場合にデフォルトルートを変更できるようになりました。ルートがルータR2を通過するように変更されました。この問題のトラブルシューティングに使用されるデバッグコマンドはどれですか？

- A. デバッグIPフロー
- B. debug ip sla error
- C. デバッグIPルーティング
- D. ipパケットをデバッグします

Answer: C (メッセージを残す)

説明

debug ip routingこのコマンドは、ルーティングテーブルに関連するメッセージのデバッグを有効にします。

最新問題: 72

アドレスを左側から右側の正しいIPv6フィルター目的にドラッグアンドドロップします。

<pre>permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443</pre>	<pre>Permit NTP from this source 2001:0D8B:0800:200c::1f</pre>
<pre>permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514</pre>	<pre>Permit syslog from this source 2001:0D88:0800:200c::1c</pre>
<pre>permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80</pre>	<pre>Permit HTTP from this source 2001:0D8B:0800:200c::0fff</pre>
<pre>permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123</pre>	<pre>Permit HTTPS from this source 2001:0D8B:0800:200c::07ff</pre>

Answer:

```
permit ip 2001:d8b:800:200c::/117
2001:0DBB:800:2010::/64 eq 443

permit ip 2001:D88:800:200C::e/126
2001:0DBB:800:2010::/64 eq 514

permit ip 2001:d8b:800:200c::800 /117
2001:0DBB:800:2010::/64 eq 80

permit ip 2001:D8B:800:200C::c/126
2001:0DBB:800:2010::/64 eq 123
```

```
permit ip 2001:D8B:800:200C::c/126
2001:0DBB:800:2010::/64 eq 123

permit ip 2001:D88:800:200C::e/126
2001:0DBB:800:2010::/64 eq 514

permit ip 2001:d8b:800:200c::800 /117
2001:0DBB:800:2010::/64 eq 80

permit ip 2001:d8b:800:200c:: /117
2001:0DBB:800:2010::/64 eq 443
```

説明

同じ回答はすでに以下で更新されています：

```
permit ip 2001:D8B:800:200C::c/126
2001:0DBB:800:2010::/64 eq 123

permit ip 2001:D88:800:200C::e/126
2001:0DBB:800:2010::/64 eq 514

permit ip 2001:d8b:800:200c::800 /117
2001:0DBB:800:2010::/64 eq 80

permit ip 2001:d8b:800:200c:: /117
2001:0DBB:800:2010::/64 eq 443
```

HTTPとHTTPSはそれぞれTCPポート80と443で実行されるため、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。しかし、2001:d88:800:200c::c/126は2001:d88:800:200c:0:0:0:cから2001:d88:800:200c:0:0:0:fの範囲でしかないため、この質問にはいくつかのタイプミスがあるかもしれません。0:0:f（合議つのホスト）。ホスト2001:0D88:0800:200c::1fは対象外です。2001:D88:800:200c::e/126についても同じで、2001:d88:800:200c:0:0:0:cから2001:d88:800:200c:0:0:0:fであり、ホスト2001:0D88:0800:200c::1cをカバーしていません。

最新問題: 73

```

R1
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
router eigrp 100
 no auto-summary
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.2 FastEthernet0/0

R2
interface Loopback0
 ip address 172.16.2.2 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0
router eigrp 100
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.1 FastEthernet0/0
 passive-interface FastEthernet0/0

```

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. passive-interfaceコマンドをR1構成に追加して、R2構成と一致させます。
- B. R1構成と一致するように、noauto-summaryコマンドをR2構成に追加します。
- C. 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。
- D. 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。

Answer: C (メッセージを残す)

最新問題: 74

展示を参照してください。

```

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) #

```

コンソールに接続している管理者は、リモートユーザーがログインしたときにデバッグメッセージを表示しません。リモートログインに対してデバッグメッセージが表示されるようにするアクションはどれですか。

- A. transportinputsshコンフィギュレーションコマンドを入力します。
- B. terminalmonitorexecコマンドを入力します。
- C. loggingconsoleデバッグ設定コマンドを入力します。
- D. aaanew-model構成コマンドを入力します。

Answer: C ([メッセージを残す](#))

説明

ロギングコンソールは、デフォルトの隠しコマンドです。

最新問題: 75

VRFインスタンスの2つの特徴は何ですか？ 2つ選択してください)

- A. 顧客サイトをさまざまなVRFに関連付けることができます。
- B. All VRFsは、顧客のルーティングテーブルとCEFテーブルを共有します。
- C. インターフェイスは1つのVRFに関連付ける必要があります
- D. 各VRFには、異なるルーティングテーブルとCEFテーブルのセットがあります。
- E. Pデバイスに接続されたカスタマーサイトのVPNメンバーシップによって定義されます。

Answer: C,D ([メッセージを残す](#))

最新問題: 76

別紙を参照してください。

```
ip dhcp excluded-address 172.16.16.1 172.16.16.2
!  
ip dhcp pool 0  
network 172.16.16.0 255.255.255.0  
domain-name cisco.com  
dns-server 172.16.16.2  
lease 30
```

```
interface Ethernet0/0  
ip address 10.1.1.1 255.255.255.252  
ip access-group 100 in
```

```
access-list 100 deny  udp any any  
access-list 100 permit ip any any
```

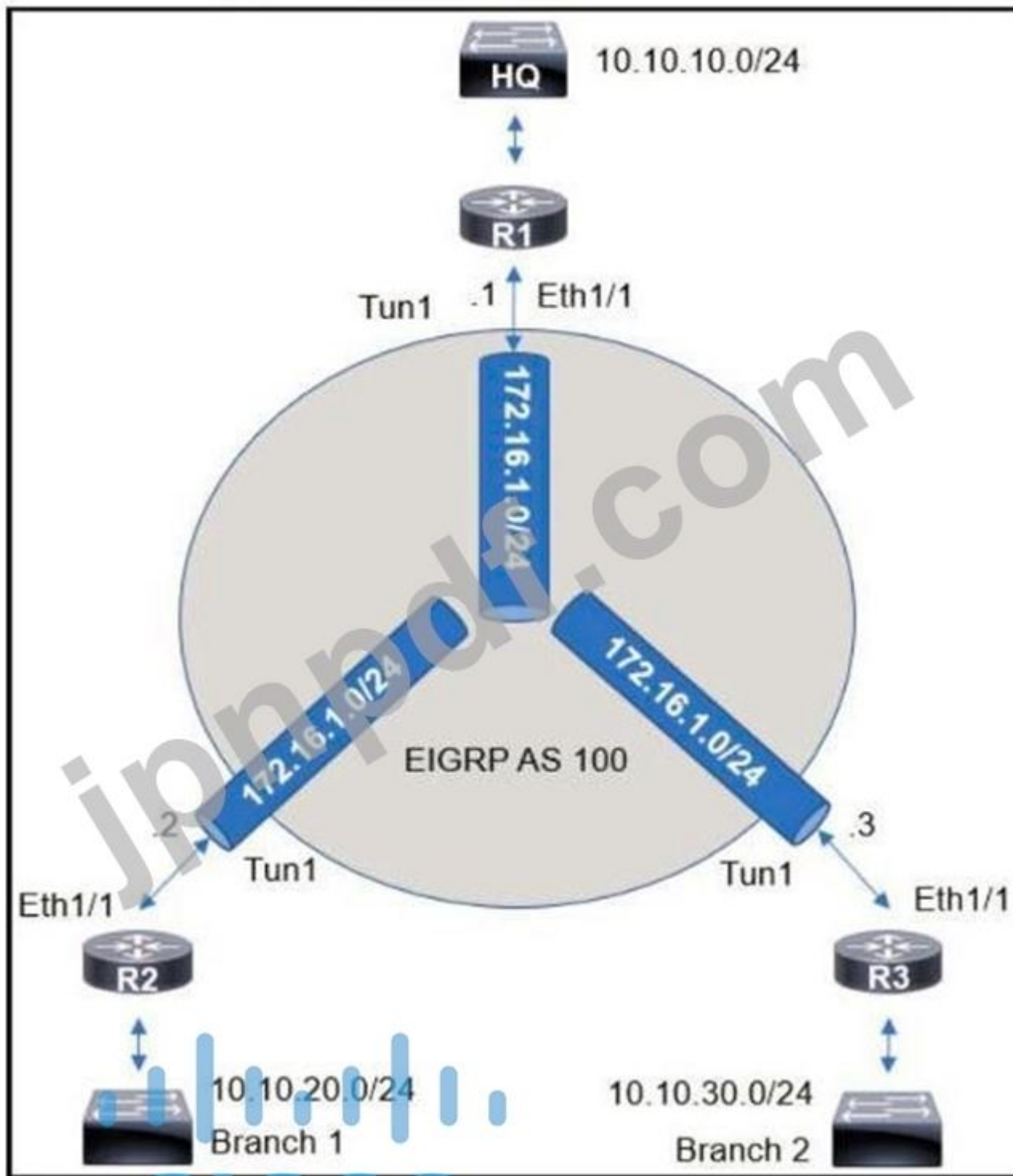
クライアントが動的IPアドレスを割り当てることができる2つの構成はどれですか？

- A. 最初の行としてaccess-list 100 permit udp any anyeq68を設定します
- B. 最初の行としてaccess-list 100 permit udp any anyeq69を設定します
- C. 最初の行としてaccess-list 100 permit udp any anyeq61を設定します
- D. 最初の行としてaccess-list 100 permit udp any anyeq86を設定します
- E. 最初の行としてaccess-list 100 permit udp any anyeq67を設定します

Answer: A,E ([メッセージを残す](#))

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 77



エンジニアは、ブランチ1とブランチ2をHQブランチ1に接続するためにDMVPN接続を設定し、ブランチ2は相互に通信できません。この問題を解決するには、どの変更を行う必要がありますか？

- R1(config)#int eth1/1
R1(config-if)#no ip split-horizon eigrp 100
- R2(config)#router eigrp 100
R2(config-router)#neighbor 172.16.1.3
- R3(config)#router eigrp 100
R3(config-router)#neighbor 172.16.1.2
- R1(config)#int tunnel 1
R1(config-if)#no ip split-horizon eigrp 100

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

Answer: ([解答を表示する](#))

説明

```
R1 (config)#int tunnel 1
```

```
R1 (config-if) no ip split-horizon eigrp 100
```

最新問題: 78

BFD制御パケットをネットワークに接続する前にローカルシステムが必要とする最小の時間ギャップはどれくらいですか？

- A. マルチを検出する
- B. 必要な最小エコーRX間隔
- C. 必要な最小TX間隔
- D. 必要な最小RX間隔

Answer: ([解答を表示する](#))

必要な最小TX間隔 :これは、ローカルシステムがBFD制御パケットを送信するとき使用する最小間隔 (マイクロ秒単位)であり、ジッタが適用されていないものです。値ゼロは予約されています。

必要な最小エコーRX間隔 :これは、このシステムがサポートできる受信BFDエコーパケット間の最小間隔 (マイクロ秒単位)であり、送信者によって適用されるジッタを差し引いたものです。この値がゼロの場合、送信システムはBFDEchoパケットの受信をサポートしていません。

最新問題: 79

展示を参照してください。ネットワーク管理者は、統一されたタイムソースからシステムとログの同期時刻を取得するようにCiscoルーターでNTPを構成しました。構成が期待どおりに機能しませんでした。問題を解決するには、どのサービスを有効にする必要がありますか。

- A. サービスタイムスタンプログ日時ローカルタイムグローバルコマンドを入力します。
- B. サービスタイムスタンプログ日時同期グローバルコマンドを入力します。

C. service timestamps log datetimeconsoleグローバルコマンドを入力します。

D. サービスタイムスタンプlog datetimeclock-periodグローバルコマンドを入力します

Answer: (解答を表示する)

ネットワークタイムプロトコル (NTP)サーバーから時刻を取得するようにルータが設定されている場合、[localtime]オプションがservice timestamps logコマンドにない場合、ルータのログエントリの時刻はシステムクロックの時刻と異なる場合があります。この問題を解決するには、service timestampslogコマンドに[localtime]オプションを追加します。これで、システムクロックとログメッセージのタイムスタンプの間で時刻が同期されるはずですが。

最新問題: 80

展示を参照してください。

The screenshot shows the Cisco DNA Center interface. At the top, there's a table with columns: Priority, Issue Type, Device Role, Company, Stack Count, Site Count (Area), and Device Count. Below this, there's a section for 'Layer 2 loop symptoms' with a filter and a table showing 'Open Issues'. The table has columns for Area, Site, Device, and Issue Count. Below that, there's a section for 'Potential Loop Details' with a filter and a table showing 'Loop Details'. The table has columns for Device, Role, Port in loop, Duplex, and VLAN in loop.

Priority	Issue Type	Device Role	Company	Stack Count	Site Count (Area)	Device Count
High	Layer 2 loop symptoms	DISTRIBUTION	Cisco	46	1	2

Area	Site	Device	Device Type	Issue Count
1	USA/JP	SF-D9300-1	Class Catalyst 9300 Switch	24
2	USA/JP	SF-D9300-2	Class Catalyst 9300 Switch	24

Device	Role	Port in loop	Duplex	VLAN in loop
SF-D9300-1	DISTRIBUTION	GigabitEthernet1/0/13	Full	30-33
SF-D9300-1	DISTRIBUTION	GigabitEthernet1/0/13	Full	30-33
SF-D9300-1	DISTRIBUTION	GigabitEthernet1/0/23	Full	30-33
SF-D9300-1	ACCESS	GigabitEthernet1/0/23	Full	30-33

```
interface GigabitEthernet1/0/13
  switchport trunk allowed vlan 30-33
  switchport mode trunk
!
interface GigabitEthernet1/0/23
  switchport trunk allowed vlan 30-33
  switchport mode trunk
```

エンジニアは、DNACを使用してレイヤー2ループを識別します。SF-D9300-1スイッチの問題を修正するコマンドはどれですか？

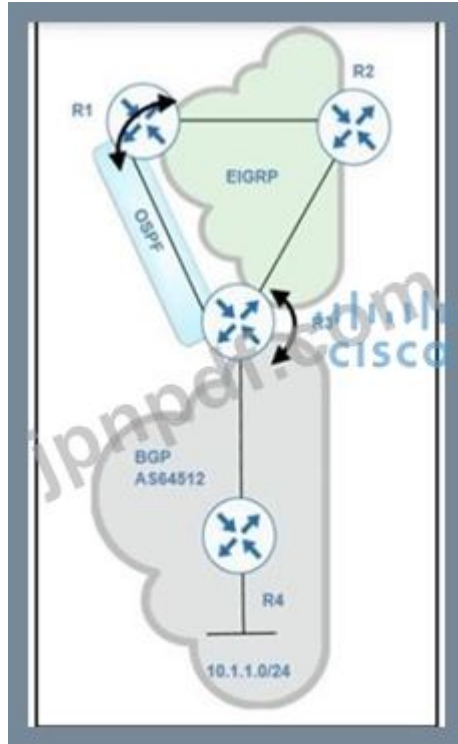
- A. スパニングツリーアップリンクファストなし
- B. スパニングツリーループガードのデフォルト
- C. スパニングツリーバックボーン高速
- D. スパニングツリーPortFast bpduguard

Answer: D (メッセージを残す)

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dnacenter/tech_notes/b_dnac_sda_lan_automation_deployment.html

最新問題: 81

出品物をご参照ください。



ルーティングプロトコルは、R3とR1で相互に再配布されます。ユーザーは、10.1.1.0/24プレフィックスでホストされているサービスへの断続的な接続を報告します。show ip route profileコマンドを実行すると、R3でルーティングアップデートの大幅な変更が通知されます。サービスをどのように安定させる必要がありますか？

- A. BGPの使用に関する問題は、別のプロトコルを使用してR3のEIGRPに再配布することで解決する必要があります。
- B. R3でiBGPの管理距離を200から100に減らすことにより、ルーティンググループを修正する必要があります
- C. R3でOSPFの管理距離を110から80に減らすことにより、ルーティンググループを修正する必要があります
- D. iBGPの使用に関する問題は、R3とR4の間でeBGPを実行することで修正する必要があります

Answer: B (メッセージを残す)

説明

再配布後、R3は2つのパスを介してネットワーク10.1.1.0/24について学習します。+内部BGP (BGP) ADが200 およびメトリック0)のR4からアドバタイズされます+ OSPF ADが110 (E2)のR1からアドバタイズされます および

20) したがって、R3はOSPFを介してADが低いパスを選択します

ただし、これはR3-> R2->R1->R3から受信されるループパスです。したがって、R4からアドバタイズされたルートが期限切れになると、ループされたパスもすぐに期限切れになり、R3はR4からのメインパスを再インストールします。これが断続的な接続の原因です。この問題を解決するために、iBGPのADを110未満の値に下げて、OSPFアドバタイズされたルートよりも優先されるようにすることができます。

最新問題: 82

お客様から、PCからローカルプリンターID 401987778に印刷できないとサポートデスクに報告されました。

Cisco DNA Center Assuranceを使用して問題を診断するには、どのツールを使用する必要がありますか。

- A. デバイストレース
- B. ACLトレース
- C. パストレース
- D. アプリケーショントレース

Answer: C (メッセージを残す)

最新問題: 83

アドレスを左側から右側の正しいIPv6フィルター目的にドラッグアンドドロップします。

<pre>permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443</pre>	<pre>Permit NTP from this source 2001:0D8B:0800:200c::1f</pre>
<pre>permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514</pre>	<pre>Permit syslog from this source 2001:0D88:0800:200c::1c</pre>
<pre>permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80</pre>	<pre>Permit HTTP from this source 2001:0D8B:0800:200c::0ff</pre>
<pre>permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123</pre>	<pre>Permit HTTPS from this source 2001:0D8B:0800:200c::07ff</pre>

Answer:

<pre>permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443</pre>	<pre>permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123</pre>
<pre>permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514</pre>	<pre>permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514</pre>
<pre>permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80</pre>	<pre>permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80</pre>
<pre>permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123</pre>	<pre>permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443</pre>

説明

同じ回答はすでに以下で更新されています :

```
permit ip 2001:D8B:800:200C::c/126
2001:0DBB:800:2010::/64 eq 123

permit ip 2001:D88:800:200C::e/126
2001:0DBB:800:2010::/64 eq 514

permit ip 2001:d8b:800:200c::800 /117
2001:0DBB:800:2010::/64 eq 80

permit ip 2001:d8b:800:200c:: /117
2001:0DBB:800:2010::/64 eq 443
```

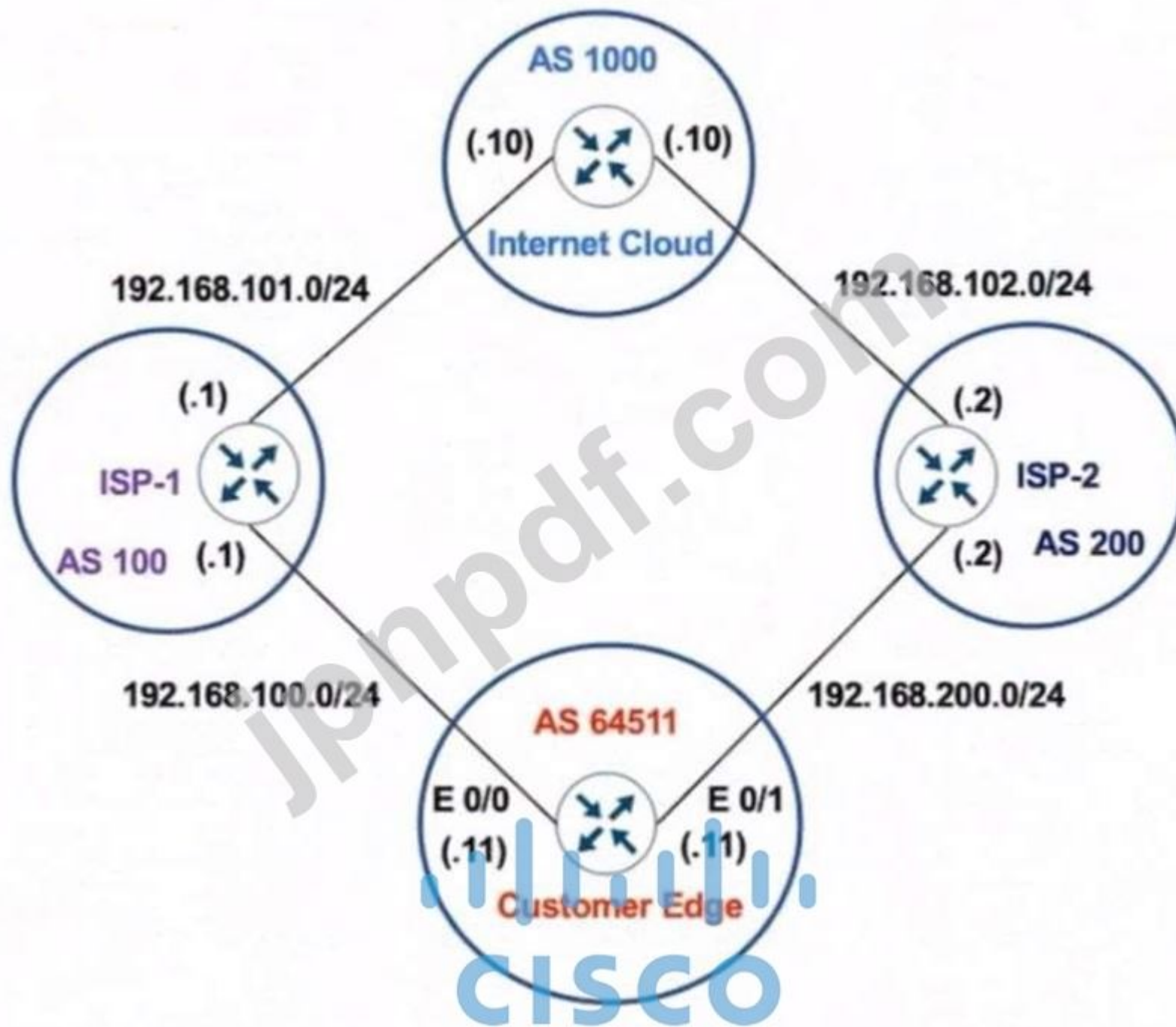
HTTPとHTTPSはそれぞれTCPポート80と443で実行されるため、覚えておく必要があります。

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。しかし、2001:d88:800:200c::c/126は2001:d88:800:200c:0:0:0:cから2001:d88:800:200c:0:0:0:fの範囲でしかないので、この質問にはいくつかのタイプミスがあるかもしれません。0:0:f（合誹つのホスト）。ホスト2001:0D88:0800:200c::1fは対象外です。2001:D88:800:200c::e/126についても同じで、

2001:d88:800:200c:0:0:0:cから2001:d88:800:200c:0:0:0:fであり、ホスト2001:0D88:0800:200c::1cをカバーしていません

。

最新問題: 84



展示を参照してください。ネットワーク管理者は、要約されたルートのみをISP-1 (AS 100) およびISP-2 (AS 200) に送信するようにカスタマーエッジルーター (AS 64511) を構成しました。

ルーター-bgp64511

ネットワーク172.16.20.0マスク255.255.255.0

ネットワーク172.16.21.0マスク255.255.255.0

ネットワーク172.16.22.0マスク255.255.255.0

ネットワーク172.16.23.0マスク255.255.255.0

集約アドレス172.16.20.0255.255.252.0

この構成の後。ISP-1とISP-2は、引き続き特定のルートとサマリールートを受信します。どの構成で問題が解決しますか？

A. ルーター-bgp 64511

集約アドレス172.16.20.0255.255.252.0要約のみ

B. ルーター-bgp 64511

ネイバー192.168.100.1要約のみ

ネイバー192.168.200.2要約のみ

C. インターフェースE 0/0

```
ip bgpsuppress-mapBLOCK_SPECIFIC
```

!

インターフェースE0/1

```
ip bgpsuppress-mapBLOCK_SPECIFIC
```

!

```
ip prefix-list PL_BLOCK_SPECIFIC permit 172.16.20.0/22 ge 24
```

!

ルートマップBLOCK_SPECIFIC許可10

一致するIPアドレスプレフィックスリストPL_BLOCK_SPECIFIC

D. ip prefix-list PL_BLOCK_SPECIFIC deny 172.16.20.0/22 ge 22

```
ip prefix-list PL_BLOCK_SPECIFIC permit 172.16.20.0/22
```

!

ルートマップBLOCK_SPECIFIC許可10

一致するIPアドレスプレフィックスリストPL_BLOCK_SPECIFIC

!

ルーターbgp64511

集約アドレス172.16.20.0255255.252.0サプレッションマップBLOCKSPECIFIC

Answer: A (メッセージを残す)

説明

集約アドレスコマンドがBGPルーティング内で使用される場合、集約されたアドレスは、より具体的なルートとともにアドバタイズされません。この規則の例外は、summary-onlyコマンドの使用によるものです。summary-onlyキーワードは、より具体的なルートを抑制し、要約されたルートのみをアナウンスします。

最新問題: 85

展示を参照してください。

```
aaa new-model
aaa authentication login default none
aaa authentication login telnet local
!
username cisco password 0 ocsic
!
line vty 0
password LetMeIn
login authentication telnet
transport input telnet
line vty 1
password LetMeIn
transport input telnet
```

クレデンシャルを左側から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、失敗したログイン試行をvtyに解決します。頻度とスケジュールを定義することにより、すべてのクレデンシャルがufSLAであるとは限りません。

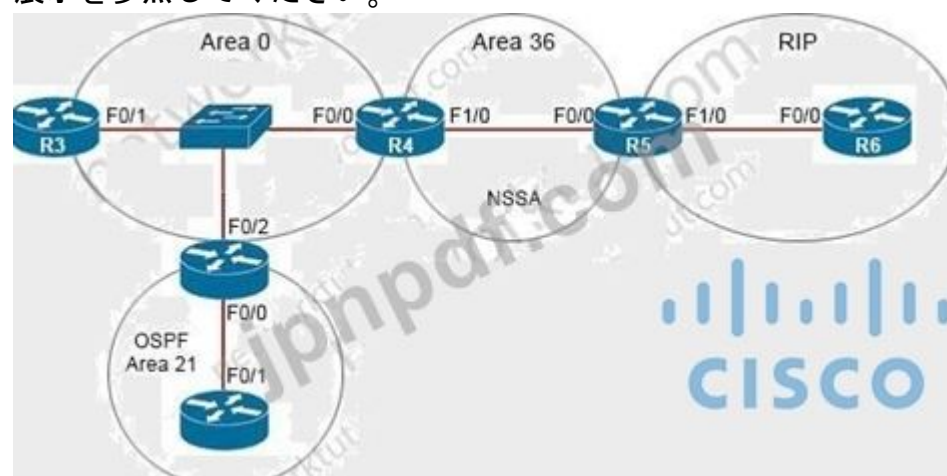


Answer:



最新問題: 86

展示を参照してください。



```

R5# show ip ospf 1 | begin Area 36
Area 36
Number of interfaces in this area is 2
It is a NSSA area
Area has no authentication
SPF algorithm last executed 00:32:46.376 ago
SFF algorithm executed 13 times
Area ranges are
172.16.0.0/16 Passive-Advertise

```

ネットワークエンジニアは、R5のOSPFドメインへのRIPルートの要約を設定しましたが、R4には4つの異なる172.16.0.0/24ネットワークがあります。問題を解決するアクションはどれですか？

A. R5 (config)#router ospf 1

R5 (config-router)#no area

R5 (config-router) #summary-address 172.16.0.0 255.255.252.0

B. R4 (config)#router ospf 99

R4 (config-router)#network 172.16.0.0 0.255.255.255 area 56

```
R4 (config-router)#area 56 range 172.16.0.0 255.255.255.0
C. R4 (config)#router ospf 1
R4 (config-router)#no area
R4 (config-router) #summary-address 172.16.0.0 255.255.252.0
D. R5 (config)#router ospf 99
R5 (config-router)#network 172.16.0.0 0.255.255.255 area 56
R5 (config-router)#area 56 range 172.16.0.0 255.255.255.0
```

Answer: ([解答を表示する](#))

説明

エリア36はNSSAであるため、R5はASBRであるため、`summary-address`コマンドを使用して外部ルートを要約できます。コマンド `area-area-id-range`はABRでのみ使用できるため、正しくありません。

要約は、R4ではなくR5であるASBRで実行する必要があるため、正解は `R5 (config)#router ospf 1`で開始する必要があります。

注：`no area`コマンドは、既存の `area ...`コマンド (`area 56 range ...`コマンドなど)を削除するために使用されます。

最新問題: 87

示す：

```
policy-map COPP-7600
class COPP-CRITICAL-7600
  police cir 2000000 bc 62500
  conform-action transmit
  exceed-action transmit
!
class class-default
  police cir 200000 bc 6250
  conform-action transmit
  exceed-action drop
!
class-map match-all COPP-CRITICAL-7600
  match access-group name COPP-CRITICAL-7600
!
ip access-list extended COPP-CRITICAL-7600
  permit ip any any eq http
  permit ip any any eq https
```

Coppポリシーが適用された後、BGPはフラッピングしています。問題を解決するための2つの解決策は何ですか？
(2つ選択してください)

- A. COPP-CRITICAL-7600ACLでBGPを設定します
- B. デフォルトクラスでCIRの値を高く設定して、トラフィックのピーク時にさらに多くのパケットを許可します

C. クラスCOPP-CRITICAL-7600でCIRの値を高く設定します

D. クラスCOPP-CRITICAL-7600で、2色のポリサーの代わりに3色のポリサーを構成します

E. IP CEFtoCoPPポリシーとBGPを機能するように構成します

Answer: A,B (メッセージを残す)

ポリシーマップCOPP-7600は ACL条件に基づいて)HTTPおよびHTTPSトラフィックのみをレート制限するため、BGPパケットはクラス「class-default」で処理され、超過したBGPパケットはドロップされます。したがって、この問題を解決するには2つの方法があります。

+ 「permit tcp any any eq bgp」というステートメントを使用してBGPをACLに追加します

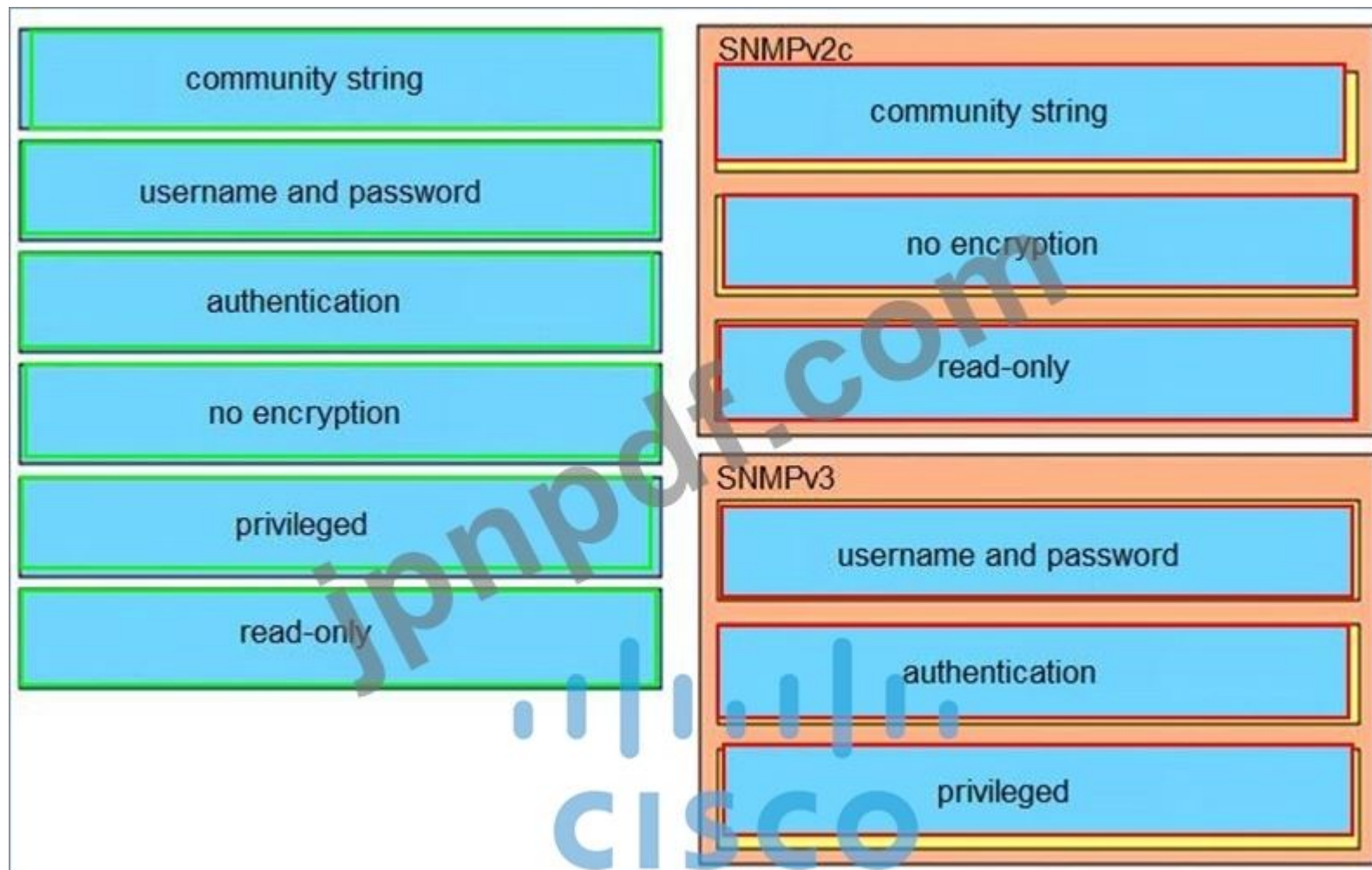
+ 2MbpsはWebトラフィックには低すぎるため、デフォルトクラスでCIRの値を高く設定します (http&https)

最新問題: 88

Cisco IOSデバイスのSNMP属性を左側から、右側の正しいSNMPv2cまたはSNMPv3カテゴリにドラッグアンドドロップします。

community string	SNMPv2c
username and password	
authentication	
no encryption	
privileged	SNMPv3
read-only	

Answer:



最新問題: 89

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スタッフが通常の営業時間内にオフィスに来て、SSH経由でデバイスにアクセスできないこの問題を解決するには、どの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 ([メッセージを残す](#))

説明

ACLにtcp101を許可する必要があります

最新問題: 90

展示を参照してください。この構成を適用した結果はどうなりますか？

```
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
```

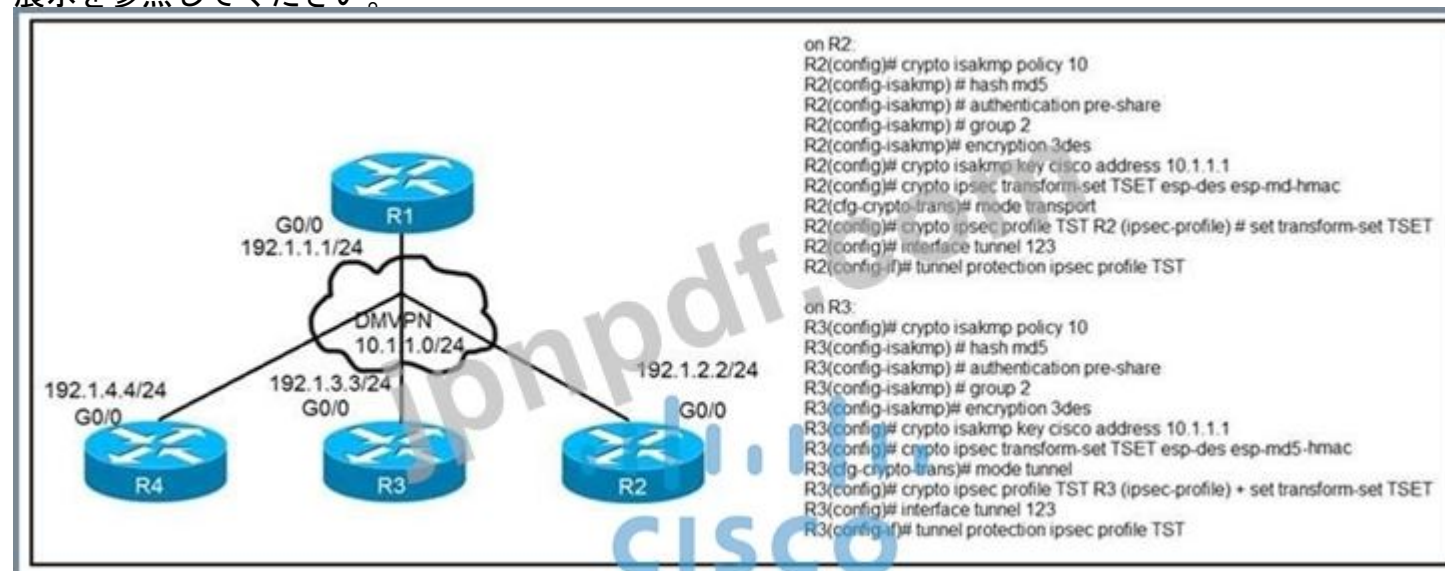
- A. ルーターは他のデバイスとBGPネイバーシップを形成できます。
- B. ルーターは他のデバイスとBGPネイバーシップを形成できません。
- C. ルーターは、次の名前のアクセスリストと一致するデバイスとBGPネイバーシップを形成できません。
BGP」。
- D. ルーターは、BGP」という名前のアクセスリストと一致する任意のデバイスとBGPネイバーシップを形成できます。

Answer: A ([メッセージを残す](#))

セクション :レイヤー3テクノロジー

最新問題: 91

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確認しました。問題を解決する2つのアクションはどれですか？ 2つ選択してください。)

- A. R2およびR3でcrypto isakmpkeyciscoアドレス192.1.1.1を設定します
- B. R2およびR3でcrypto isakmpkeyciscoアドレス0.0.0.0を設定します。
- C. R3でモードをモードトンネルからモードトランスポートに変更します
- D. モードをモードトランスポートからR2のモードトンネルに変更します。
- E. R2およびR3の暗号isakmpキーciscoアドレス10.1.1.1を削除します

Answer: ([解答を表示する](#))

※IPSecでDMVPNを使用する場合は、トンネルモードを使用する必要はありません。DMVPNはGREを使用するため、これは新しいIPヘッダーがGREによってすでに追加されていることを意味します。GREカプセル化は、暗号化プロセスが実行される前にトンネルインターフェイスで行われます。

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **92**

エンジニアは、会社のマルチエリアOSPF本社ルーターとサイトACiscoルーターをVRF liteで構成しました。各サイトルーターは、MPLSバックボーンのPEルーターに接続されています。

```
Head Office & Site A
ip cef
ip vrf abc
rd 101:101
!
interface FastEthernet0/0
ip vrf forwarding abc
ip address 172.16.16.X 255.255.255.252
!
router ospf 1 vrf abc
log-adjacency-changes
network 172.16.16.0 0.0.0.255 area 1
```

両方のサイトルーターの設定が完了した後、LSA 3,4、5、および7はいずれもサイトAルーターにインストールされていません。この問題を解決する構成はどれですか？

- A. routtr ospf 1vrfabcで本社とサイトAのルーターに接続されている両方のPEルーターで機能vrf-liteを構成します。
- B. ルーター ospf 1vrfabcで本社と接続されているPEルーターの機能vrf-liteを設定します
- C. サイトAの機能vrf-liteと、ルーター ospf 1vrfabcの下に接続されているPEルーターを構成します。
- D. ルーター ospf 1vrfabcの下の本社およびサイトAルーターで機能vrf-liteを設定します

Answer: A ([メッセージを残す](#))

最新問題: **93**

展示を参照してください。

```

Spoke# show dmvpn
Tunnel0, Type:Spoke, NHRP Peers:2,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
-----
1 172.18.16.2 192.168.1.1 UP 01:05:35 S
1 172.18.46.2 192.168.1.4 UP 00:00:25 D

```

エンジニアがスポークルータに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WANIPアドレスは何ですか？

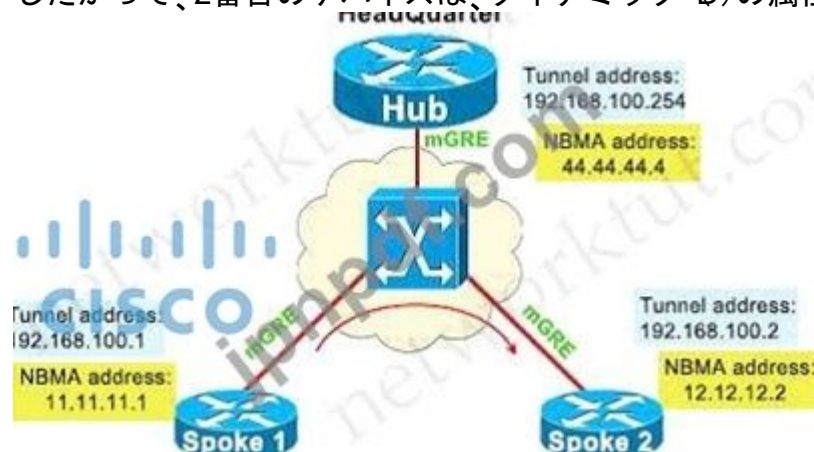
- A. 172.18.46.2
- B. 192.168.1.4
- C. 172.18.16.2
- D. 192.168.1.1

Answer: [\(解答を表示する\)](#)

出力から、2つのNHRPピアがあることがわかります。NBMAアドレスが

172.18.16.2と静的 (S)の「属性」Attrb)なので、ハブデバイスであると推測できます。

したがって、2番目のデバイスは、ダイナミック (D)の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-NAT、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->応答を期待しています、R->応答しています、W->待機中

UpDnTime->トンネルのUpまたはDownTime

インターフェイス :Tunnel1、IPv4NHRPの詳細

タイプ :スポーク、NHRPピア 2、

```

#Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb

```

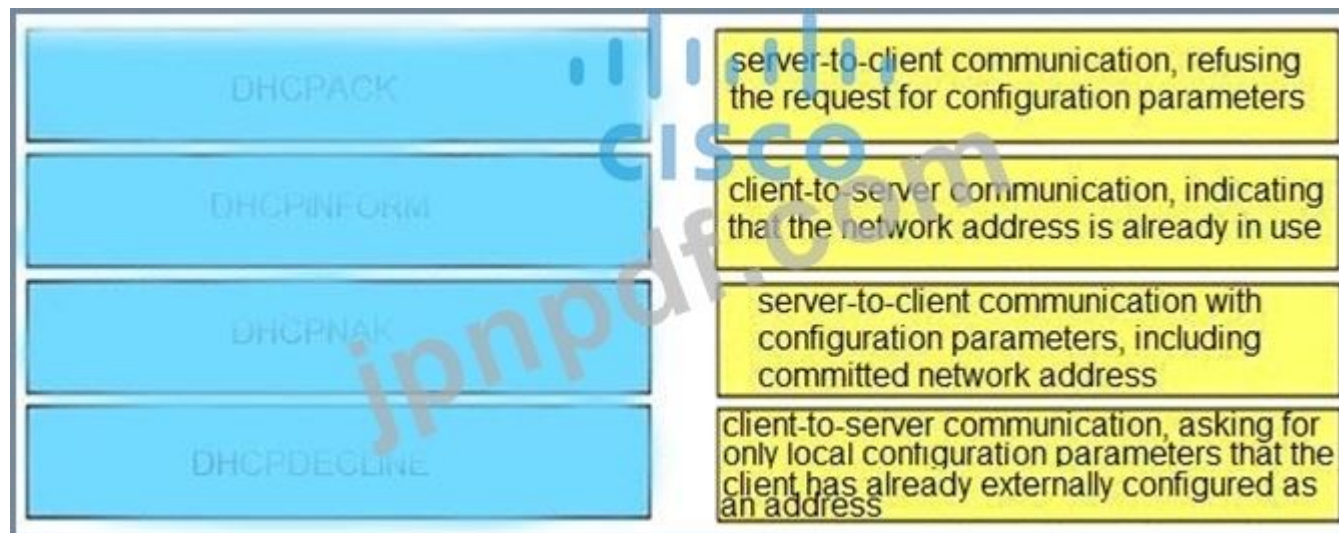
```

-----
1 44.44.44.4 192.168.100.254 UP 00:03:40 S
1 12.12.12.2 192.168.100.2 UP 00:03:20 D

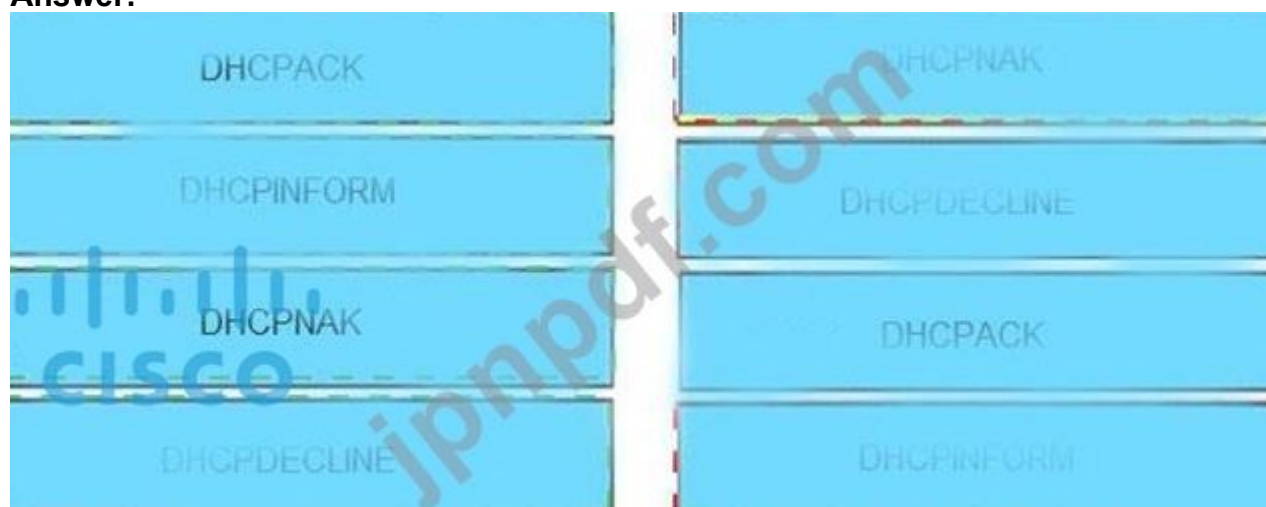
```

最新問題: 94

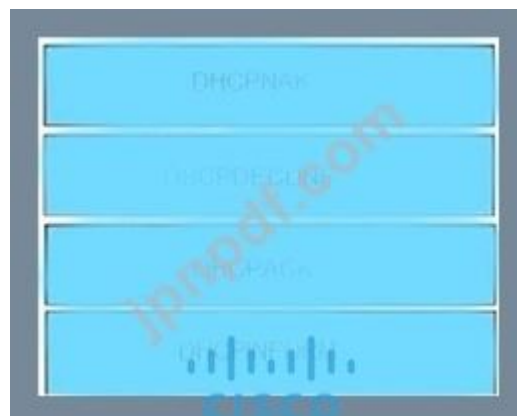
DHCPメッセージを左側から右側の正しい用途にドラッグアンドドロップします。



Answer:



説明



DHCPACK

コミットされたネットワークアドレスを含む構成パラメーターを使用したサーバーからクライアントへの通信。

DHCPINFORM

クライアントからサーバーへの通信。クライアントがすでに外部でアドレスとして構成しているローカル構成パラメーターのみを要求します。

DHCPNAK

サーバーからクライアントへの通信。構成パラメーターの要求を拒否します。

DHCPDECLINE

クライアントからサーバーへの通信。ネットワークアドレスがすでに使用されていることを示します

最新問題: 95

展示を参照してください。

```
snmp-server community ciscotest1
snmp-server host 192.168.1.128 ciscotest
snmp-server enable traps bgp
```

ネットワーク操作では、操作サブネットからこの構成を使用してデバイスの構成を読み書きできません。問題を解決する2つの構成はどれですか？ 2つ選択してください。)

- A. コミュニティ ciscotest1に加えてSNMPPrw権限を設定します。
- B. コミュニティ ciscotest1に加えてSNMPPrw権限を設定します。
- C. アクセスリスト1を変更し、アクセスリストで操作サブネットを許可します。
- D. アクセスリスト1を変更し、アクセスリストでSNMPを許可します。
- E. バージョン1に加えてSNMPPrw権限を構成します。

Answer: A,C (メッセージを残す)

最新問題: 96

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
```

SanFranciscoルーターとBostonルーターは、直接リンクがアップしているにもかかわらず、相互に到達するために低速のリンクを選択しています。どの構成で問題が解決しますか？

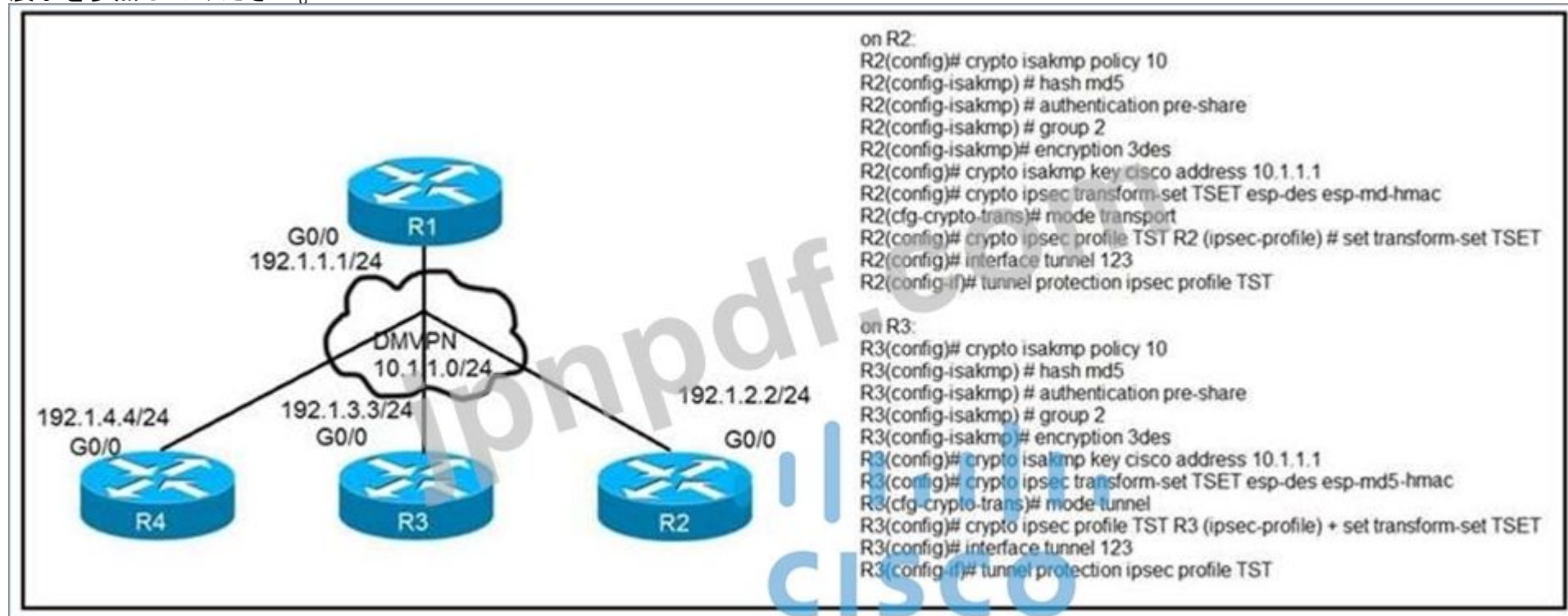
● Boston Router	router ospf 1 auto-cost reference-bandwidth 1000
● SanFrancisco Router	router ospf 1 auto-cost reference-bandwidth 1000
● All Routers	router ospf 1 auto-cost reference-bandwidth 100
● All Routers	router ospf 1 auto-cost reference-bandwidth 1000

- 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: A ([メッセージを残す](#))

最新問題: 97

展示を参照してください。

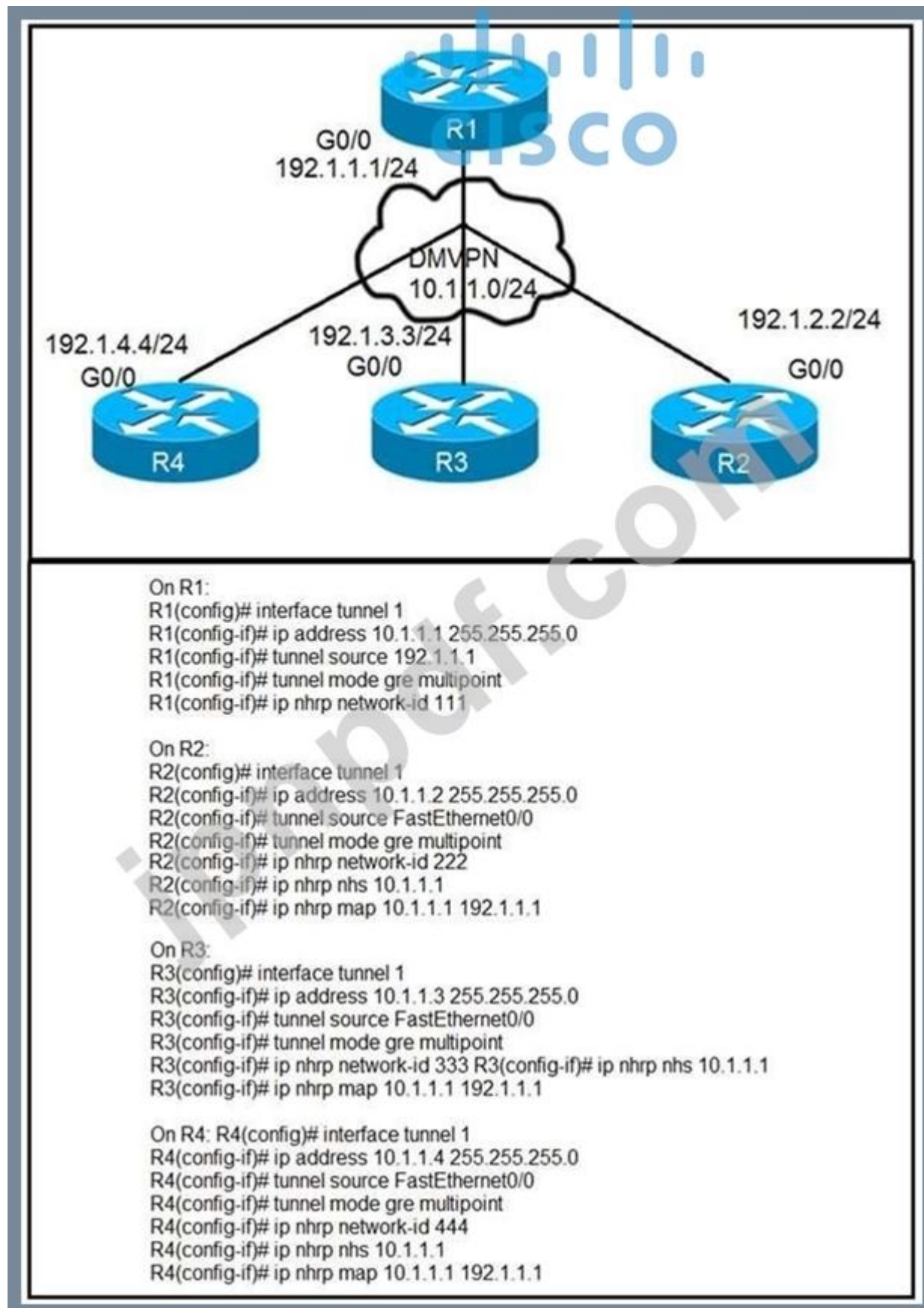


IPsecを適用した後、エンジニアはDMVPNトンネルがダウンし、スポークツースポークとハブの両方が確立されていないことを確認しました。問題を解決する2つのアクションはどれですか？ 2つ選択してください。）

- A. R2およびR3でcrypto isakmpkeyciscoアドレス192.1.1.1を設定します。
- B. R3でモードをモードトンネルからモードトランスポートに変更します。

- C. R2およびR3のcrypto isakmpkeyciscoアドレス10.1.1.1を削除します。
 - D. モードをモードトランスポートからR2のモードトンネルに変更します。
 - E. R2およびR3でcrypto isakmpkeyciscoアドレス0.0.0.0を設定します。
- Answer: B,E (メッセージを残す)**

最新問題: 98



展示品をご覧ください。DMVPNのスポークツースポーク間にフェーズ3トンネルを確立することはできません。

欠落している2つのコマンドはどれですか？ 2つ選択してください。)

- A. スポークルータにipnhrpredirectコマンドがありません。
- B. スポークルータにipnhrpショートカットコマンドがありません。

- C. ハブルータにipnhrpredirectコマンドがありません。
- D. ハブルータにipnhrpショートカットコマンドがありません。
- E. ハブルータにipnhrpmapコマンドがありません。

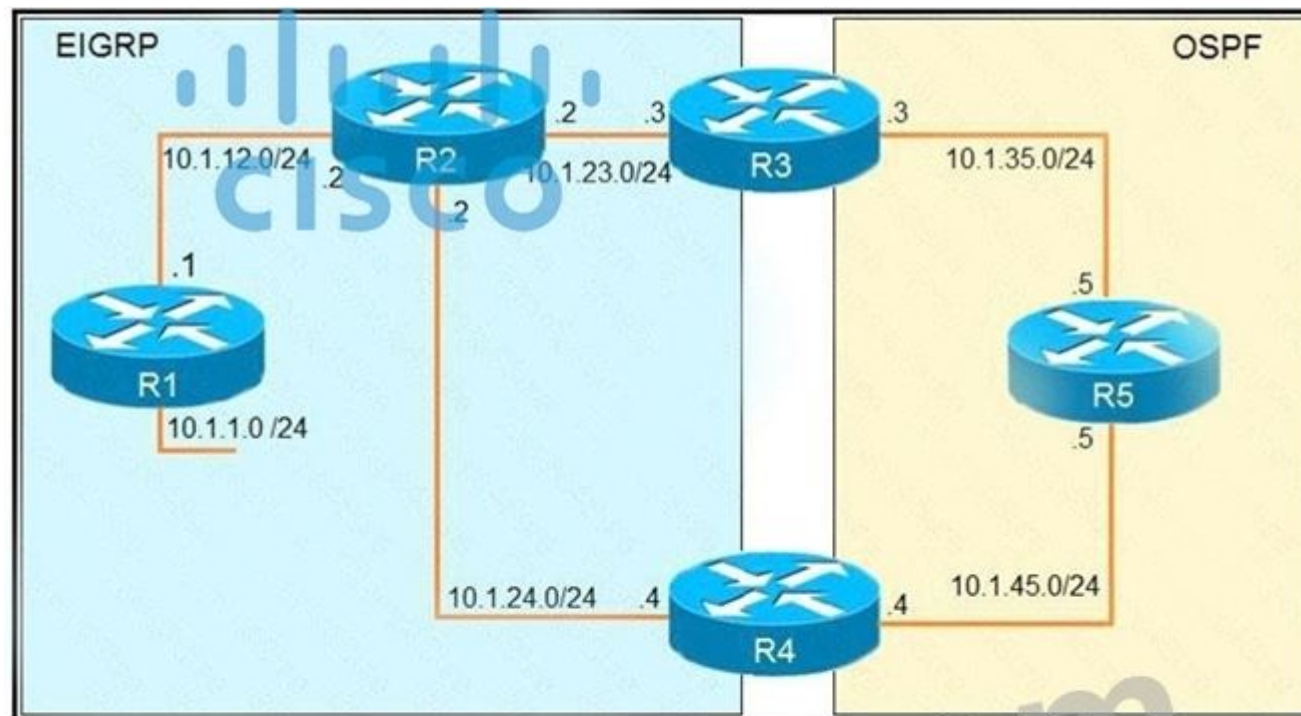
Answer: B,C (メッセージを残す)

セクション :VPNテクノロジー

説明/参照 :

最新問題: 99

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 truncated>
  
```

R5からのトレースルートの出力は、ネットワーク内のループを示しています。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)

```

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 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 ([メッセージを残す](#))

最新問題: 100

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
```

ユーザーから、DHCPサーバーからIPアドレスを取得できないとの報告がありました。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2時間を超えてアクティブになっているユーザーはいません。現在のリソース内の問題を修正するアクションはどれですか？

- A. サブネットマスクをDHCPプールのnetwork192.168.1.0255.255.254.0コマンドに変更します
- B. DHCPリース時間をより大きな値に設定します
- C. network192.168.2.0255.255.255.0コマンドをDHCPプールに追加します
- D. DHCPリース時間を小さい値に設定します

Answer: ([解答を表示する](#))

最新問題: 101

展示を参照してください。

```
R1#show policy-map control-plane
Control Plane
Service-policy input: CoPP
Class-map: PERMIT (match-all)
 50 packets, 3811 bytes
 5 minute offered rate 0000 bps
 Match: access-group 100
Class-map: ANY (match-all)
 210 packets, 19104 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: access-group 199
 drop
Class-map: class-default (match-any)
 348 packets, 48203 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: any

R1#show access-list 100
Extended IP access list 100
 10 permit udp any any eq 23 (100 matches)
 20 permit tcp any any eq telnet (5 matches)
 30 permit tcp any eq telnet any (10 matches)

R1#show access-list 199
Extended IP access list 199
 10 deny tcp any eq telnet any (50 matches)
 50 permit ip any any (1 match)

R1#show running-config | section line vty
line vty 0 4
 login
 transport input telnet ssh
 transport output telnet ssh
```

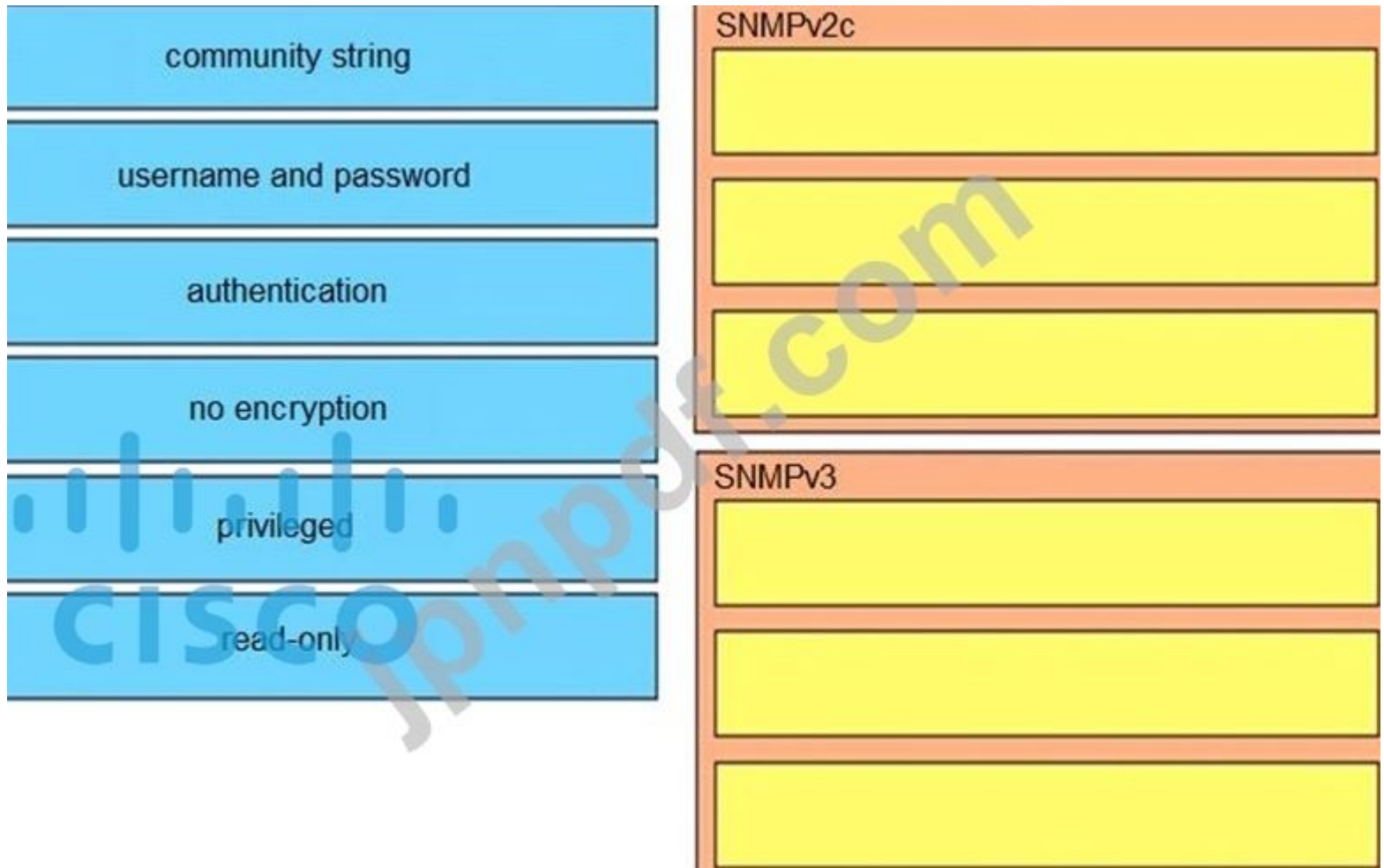
SSHによるルーターR1へのアクセスを制限する2つのアクションはどれですか？ (2つ選択してください。)

- A. 行vtyでトランスポート出力sshを設定し、アクセスリスト199からシーケンス10を削除します。
- B. service-policyCoPPからclass-mapANYを削除します
- C. 行vtyでトランスポート出力sshを設定し、アクセスリスト100からシーケンス20を削除します。
- D. 行vtyでトランスポート入力sshを設定し、アクセスリスト100からシーケンス30を削除します。
- E. アクセスリスト100からシーケンス10を削除し、シーケンス20を追加して、アクセスリスト199への任意のeqtelnetのtcpを拒否します。

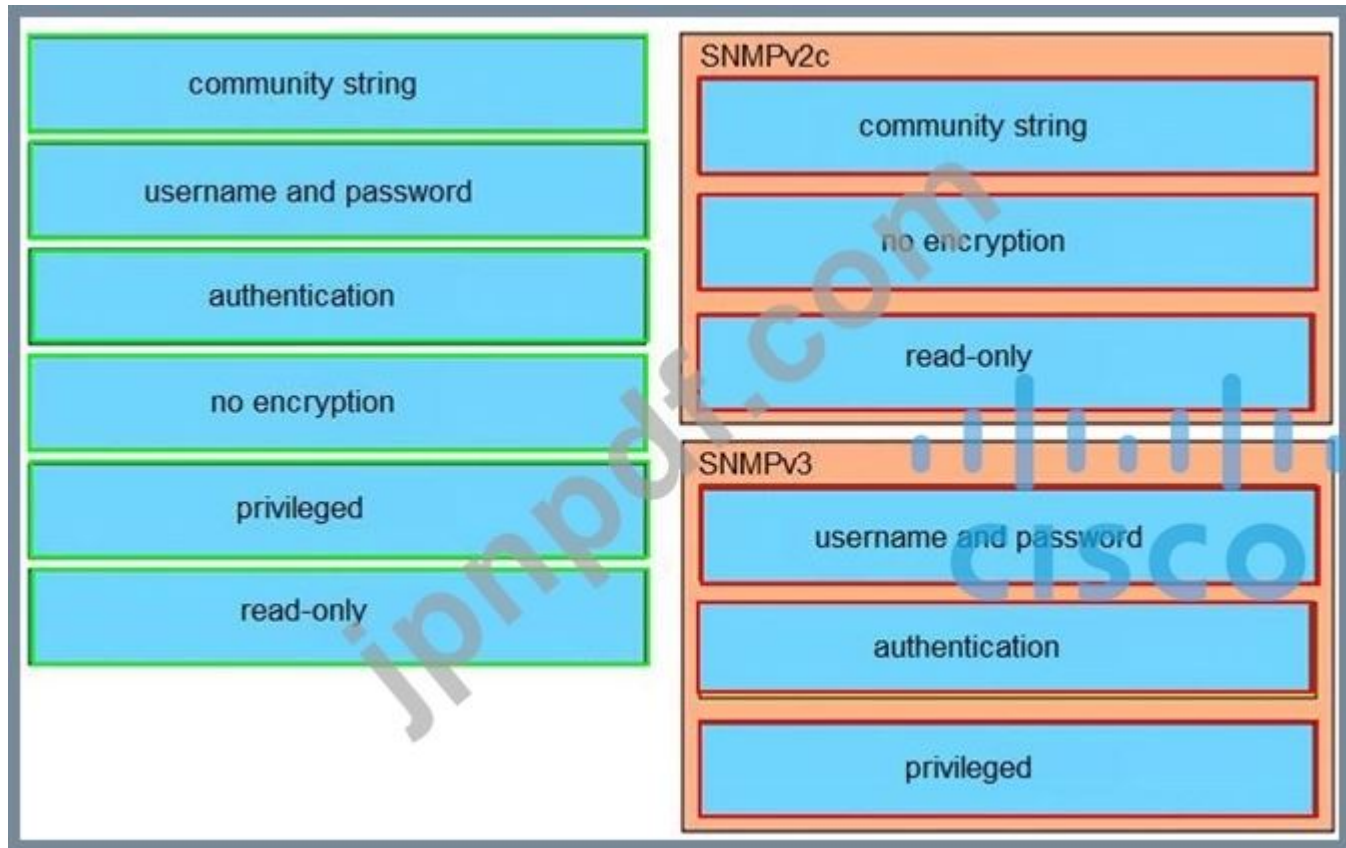
Answer: B,D (メッセージを残す)

最新問題: 102

Cisco IOSデバイスのSNMP属性を左側から、右側の正しいSNMPv2cまたはSNMPV3カテゴリにドラッグアンドドロップします。



Answer:



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

DHCPACK	server-to-client communication, refusing the request for configuration parameters
DHCPINFORM	client-to-server communication, indicating that the network address is already in use
DHCPNAK	server-to-client communication with configuration parameters, including committed network address
DHCPDECLINE	client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address

Answer:



最新問題: 104

IPv6ソースアドレスを転送する必要があるかどうかを判断するために、IPv6ソースガードは何を利用しますか？

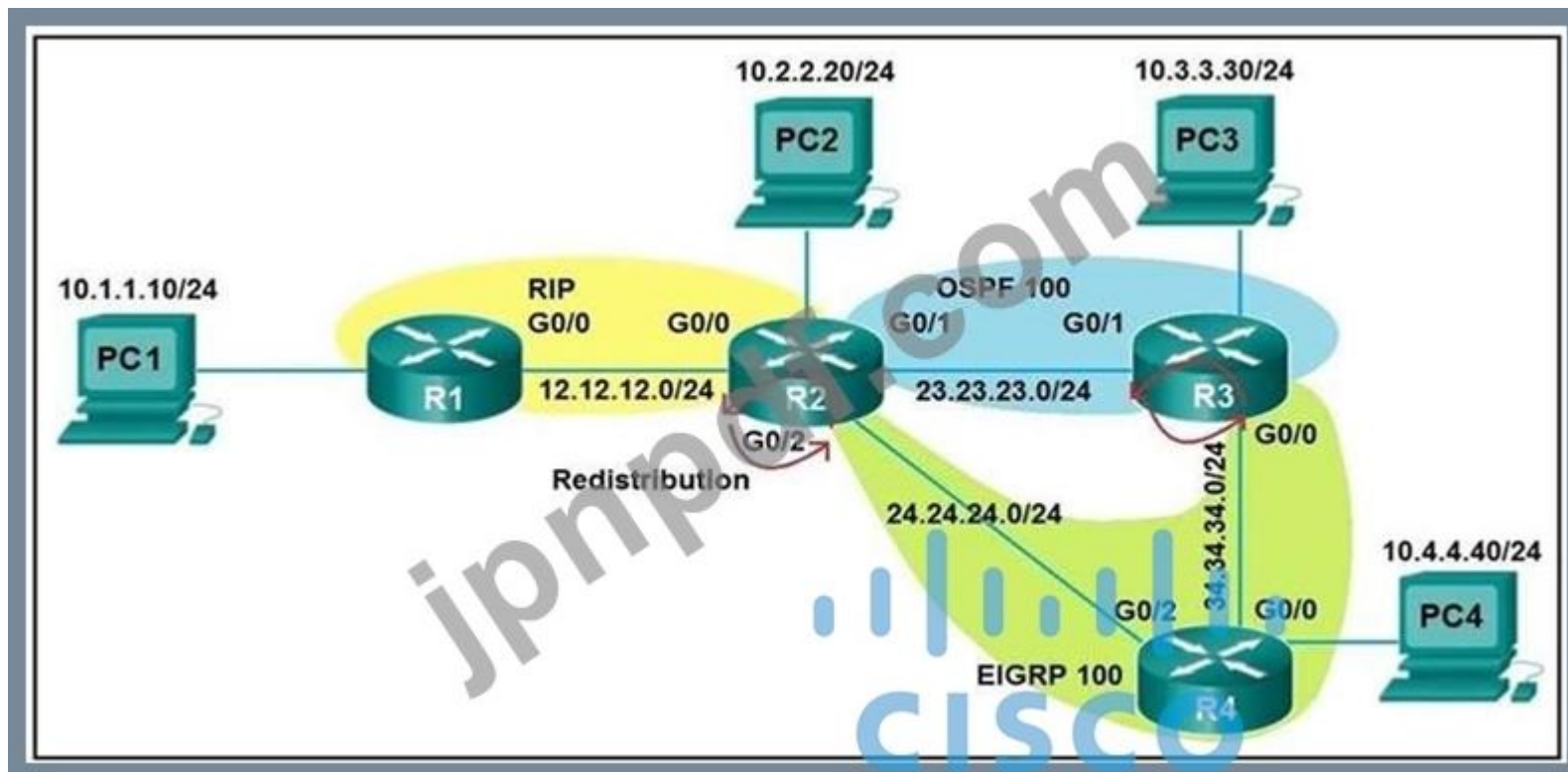
- A. ACE
- B. ACLS
- C. DHCP

D. バインディングテーブル

Answer: D (メッセージを残す)

IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets; rather, it works

最新問題: 105



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に到達できるように、エンジニアは問題を解決するためにどのアクションを実行できますか？

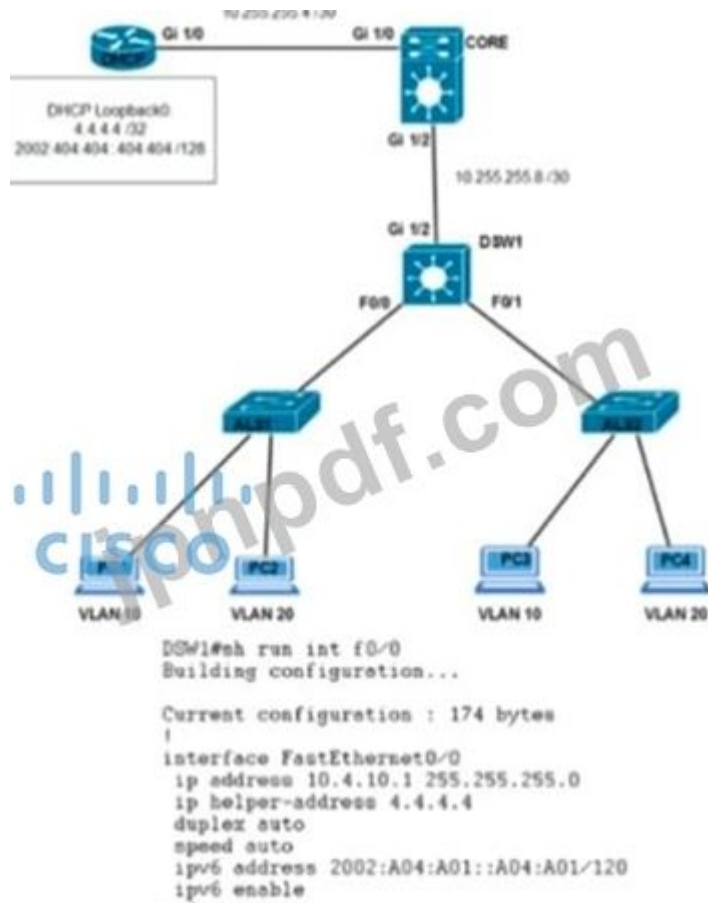
- A. R2のRIPプロセスで管理距離100を設定します。
- B. OSPFからEIGRPに再配布されるときに、プレフィックス10.1.1.0/24をフィルタリングします。
- C. RIPからEIGRPに再配布するとき、プレフィックス10.1.1.0/24をフィルタリングします。
- D. 直接接続されたインターフェースをR2に再配布します。

Answer: B (メッセージを残す)

セクション :レイヤー3テクノロジー

最新問題: 106

ALS2のクライアントはIPv4およびIPv6アドレスを受け取りますが、ALS1のクライアントはIPv4アドレスのみを受け取り、IPv6アドレスは受け取りません。DSW1のどのアクションにより、ALS1のクライアントがIPv6アドレスを受信できるようになりますか？



- Configure DSW1(dhcp-config)#default-router 2002:A04:A01::A04:A01
- Configure DSW1(config-if)#ipv6 dhcp relay destination 2002:404:404::404:404 GigabitEthernet1/2
- Configure DSW1(config)#ipv6 route 2002:404:404::404:404/128 FastEthernet1/0
- Configure DSW1(config-if)#ipv6 helper address 2002:404:404::404:404

- 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 (メッセージを残す)

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (80030%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 107

MPLSVPNデバイスタイプを左から右の定義にドラッグアンドドロップします。

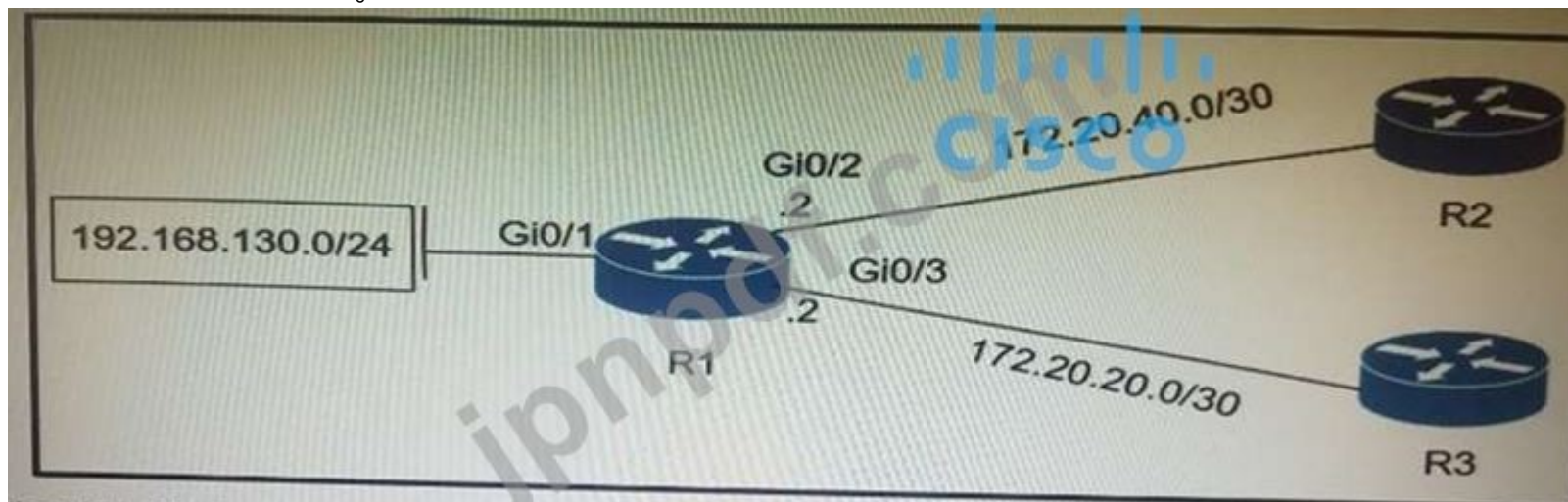
Customer (C) device	device in the core of the provider network that switches MPLS packets
CE device	device that attaches and detaches the VPN labels to the packets in the provider network
PE device	device in the enterprise network that connects to other customer devices
Provider (P) device	device at 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: 108

展示を参照してください。



どの構成がR1のポリシーを構成して、
192.168.130.0/24ネットワークから。

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)

```
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 172.20.20.1
```

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 172.20.40.2
```

D)

```
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
```

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

Answer: ([解答を表示する](#))

最新問題: 109

LDPはMPLSトポロジでどの機能を提供しますか？

- A. MPLSトポロジで複数のVPNをPルーターに接続できるようにします。
- B. LSRのMPLSトポロジでホップバイホップ転送を提供します。
- C. 異なるVRF間でMPLSVPNのルートを交換します。
- D. LSRがIPルートを交換するための手段を提供します。

Answer: **B** ([メッセージを残す](#))

LDPは、基盤となるInterior Gateway Protocol (IGP)ルーティングプロトコルによって選択されたルートにラベルを割り当てることにより、MPLSネットワークでのホップバイホップまたは動的ラベル配布の標準的な方法を提供します。結果として得られるラベル付きパスは、ラベルスイッチパス (LSP)と呼ばれ、ラベルトラフィックをMPLSバックボーンを介して特定の宛先に転送します。

参照：

12-4t-book.pdf

最新問題: 110

IPv6First-HopSecurity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。

IPv6 DHCPv6 Guard	Block a malicious host and permit the router from a legitimate route.
IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents.
IPv6 Source Guard	Create a binding table that is based on NS and NA messages.
IPv6 RA Guard	Filter inbound traffic on Layer 2 switch ports. It does not use the IPv6 binding table.
IPv6 ND Inspection	Create IPv6 neighbors connected to the device from information sources such as NDP snooping.

Answer:



説明

グラフィカルユーザーインターフェイス、チャート説明が自動的に生成されます



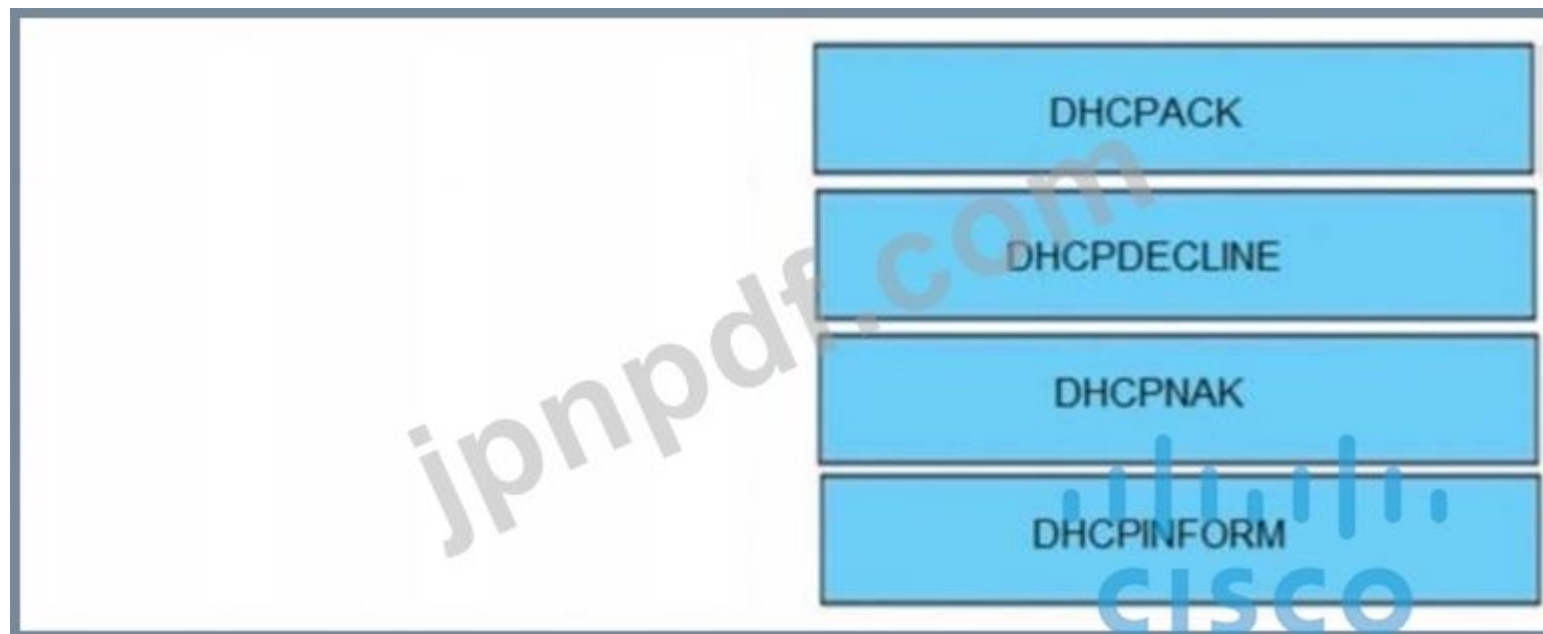
最新問題: 111

ドラッグアンドドロップの質問

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

DHCPACK	server-to-client communication, refusing the request for configuration parameters
DHCPINFORM	client-to-server communication, indicating that the network address is already in use
DHCPNAK	server-to-client communication with configuration parameters, including committed network address
DHCPDECLINE	client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address

Answer:



最新問題: 112

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引き続き存在します。どのアクションがルートをブロックしますか？

- A. 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-DLdeny20。
- 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. route-mapコマンドのシーケンス10をpermitからdenyに変更します。
- D. 標準の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 ([メッセージを残す](#))

最新問題: 113

展示を参照してください。

```

TAC+: TCP/IP open to 171.68.118.101/49 failed
Destination unreachable; gateway or host down
AAA/AUTHEN (2546660185): status = ERROR
AAA/AUTHEN/START (2546660185): Method=LOCAL
AAA/AUTHEN (2546660185): status = FAIL
As1 CHAP: Unable to validate Response. Username chapuser: Authentication failure

```

ユーザー認証が拒否されるのはなぜですか？

- A. ユーザーがCHAP用に設定されているため、TACACS+サーバーはユーザーを拒否します。
- B. TACACS +サーバーがダウンしており、ユーザーはローカルデータベースにありません。
- C. TACACS +サーバーは「ユーザー」を想定していますが、NTクライアントは「ドメイン/ユーザー」を送信します。
- D. TACACS +サーバーがダウンしており、ユーザーはローカルデータベースにいます。

Answer: B ([メッセージを残す](#))

最新問題: 114

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。

Init	Each router compares the DBD packets that were received from the other router.
2-way	Routers exchange information with other routers in the multiaccess network.
Down	The neighboring router requests the other routers to send missing entries.
Exchange	The network has already elected a DR and a backup BDR.
ExStart	The OSPF router ID of the receiving router was not contained in the hello message.
Loading	No hellos have been received from a neighbor router.

Answer:

Init	Exchange
2-way	ExStart
Down	Loading
Exchange	2-way
ExStart	Init
Loading	Down

Explanation:

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) が受信されていないことを意味しますが、この状態でもhelloパケットをネイバーに送信できます。

完全に隣接するネイバー状態の間に、ルータがルータデッドインターバル時間内にネイバーからhelloパケットを受信しない場合 デフォルト

ではRouterDeadInterval = 4 * HelloInterval)、または手動で設定されたネイバーが設定から削除されている場合、ネイバーは状態がFullからDownに変わります。

試み

この状態は、NBMA環境で手動で設定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。ネイバーからは、デッドインターバル内にhelloが受信されていません。

初期化

この状態は、ルータがネイバーからhelloパケットを受信したが、受信側ルータのIDがhelloパケットに含まれていなかったことを示します。ルータがネイバーからhelloパケットを受信すると、有効なhelloパケットを受信したことの確認応答として、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たことを示します。双方向とは、各ルーターが他のルーターのhelloパケットを認識したことを意味します。この状態は、helloパケットを受信するルータが、受信したhelloパケットのネイバーフィールド内に自身のルータIDを確認したときに達成されます。この状態で、ルータはこのネイバーに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)でのみいっぱいになります。他のすべてのネイバーとの双方向状態のままです。ポイントツーポイントおよびポイントツーマルチポイントネットワークでは、ルーターは接続されているすべてのルーターでいっぱいになります。

この段階の終わりに、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が選出されます。DR選挙プロセスの詳細については、DR選挙を参照してください。

注 init状態のネイバーからDatabase Descriptor (DBD)パケットを受信すると、双方向状態に移行します。

Exstart

DRとBDRが選択されると、リンク状態情報を交換する実際のプロセスは、ルータとそのDRおよびBDRの間で開始できます。(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、隣接関係を形成するための初期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になり、交換を開始します。そのため、シーケンス番号をインクリメントできる唯一のルーターです。このマスター/スレーブ関係のプロセス中に、ルーターIDが最も大きいDR/BDRがマスターになると論理的に結論付け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、ルーターに構成された優先度が高いため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、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、スレーブによって明示的に確認されたマスターによってのみインクリメントできるシーケンス番号があります。ルータは、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アップデートパケット (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ている情報と比較され、新しいまたはより新しいリンクステート情報がネイバーで利用可能かどうかチェックされます。

読み込み中

この状態では、リンク状態情報の実際の交換が行われます。DBDによって提供された情報に基づいて、ルータ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アップデートパケットで提供します。隣接中に、ルータが古いまたは欠落しているLSAを受信すると、リンクステート要求パケットを送信して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されます。

満杯

この状態では、ルータは互いに完全に隣接しています。すべてのルータとネットワークのLSAが交換され、ルータのデータベースが完全に同期されます。

Fullは、OSPFルータの通常の状態です。ルータ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。これに対する唯一の例外は、ブロードキャストネットワークでは通常の双方向状態です。ルータは、NBMA/ブロードキャストメディアのDRと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の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でFULL状態を達成するDRおよびBDRは、DRまたはBDRのいずれかでshow ip ospf neighborコマンドを入力すると、FULL/DROTHERを表示します。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のいずれかであるため、これはネイバーをFULL/DROTHERとして表示します。

参照 :

<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html> OSPF隣接関係が形成されると、ルータはいくつかの状態変化を経験します隣接するものと完全に隣接する前に。状態は、Down-> Attempt (オプション)-> Init-> 2-Way-> Exstart-> Exchange->Loading->Fullです。これらの状態に関する簡単な説明を以下に示します。

ダウン :このネイバーから情報 (hello)を受信していません。

試行 :NBMA環境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。ネイバーからは、デッドインターバル内にhelloが受信されていません。

Init :ルータがネイバーからhelloパケットを受信したが、受信側ルータのIDがhelloパケットに含まれていなかったことを指定します

2-Way :2つのルータ間で双方向通信が確立されたことを示します。

Exstart :DRとBDRが選出されると、リンク状態情報を交換する実際のプロセスは、ルータとそのDRおよびBDRの間で開始できます。

交換 :OSPFルータはデータベース記述子 (DBD)パケットを交換および比較します。読み込み中 :この状態では、リンク状態情報の実際の交換が行われます。古くなった、または欠落しているエントリも再送する必要があります。

フル :ルータは互いに完全に隣接しています

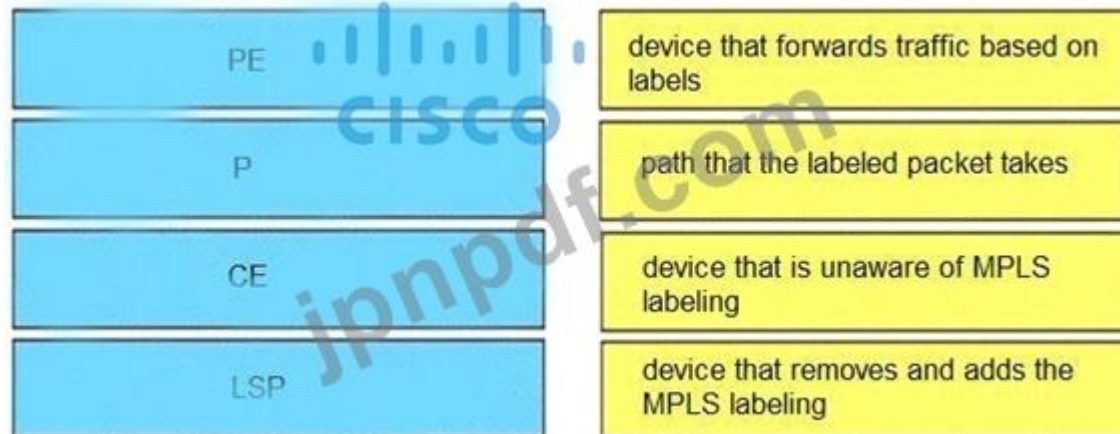
(参照 :

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml)

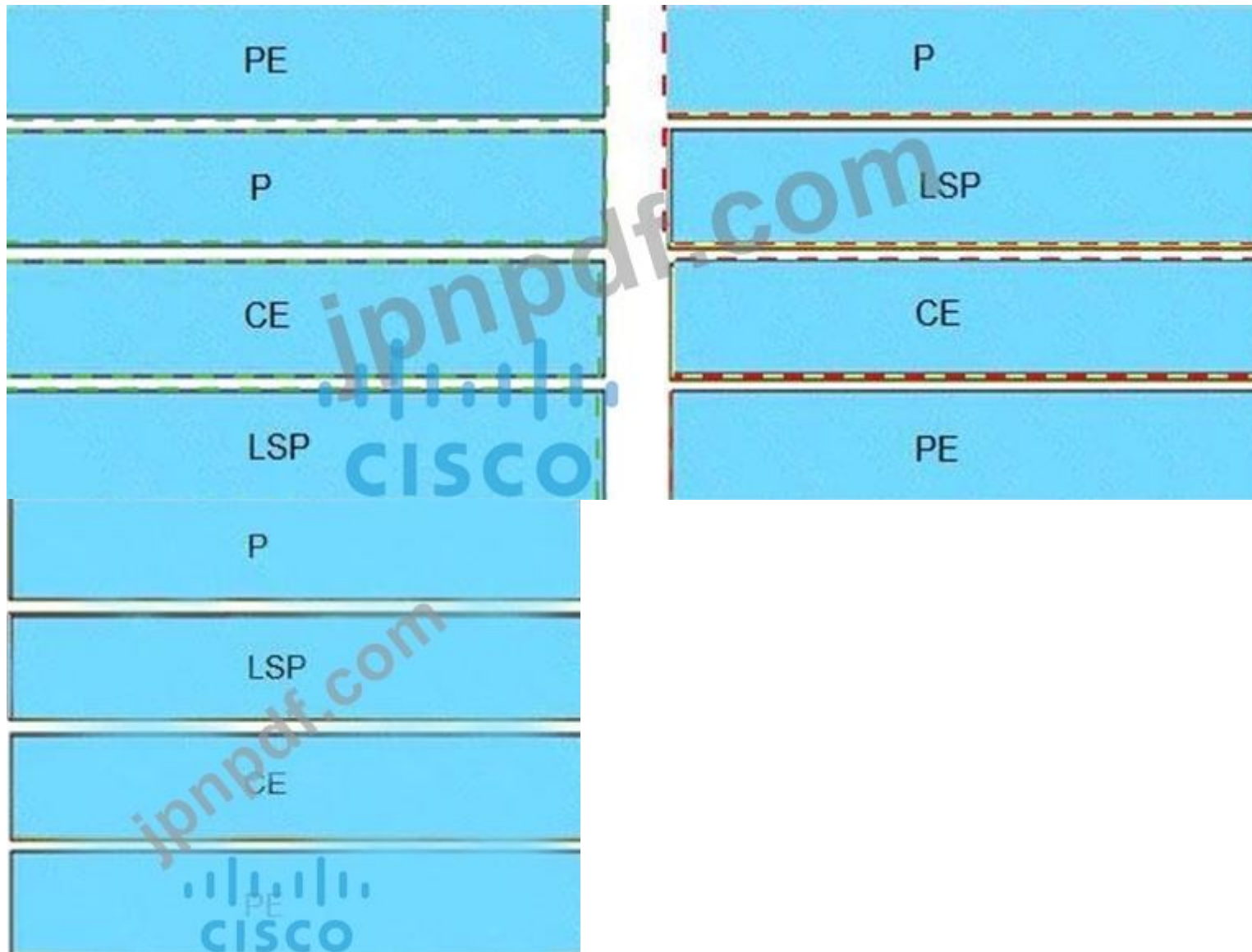
<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html>

最新問題: 115

MPLS用語を左側から右側の正しい定義にドラッグアンドドロップします。

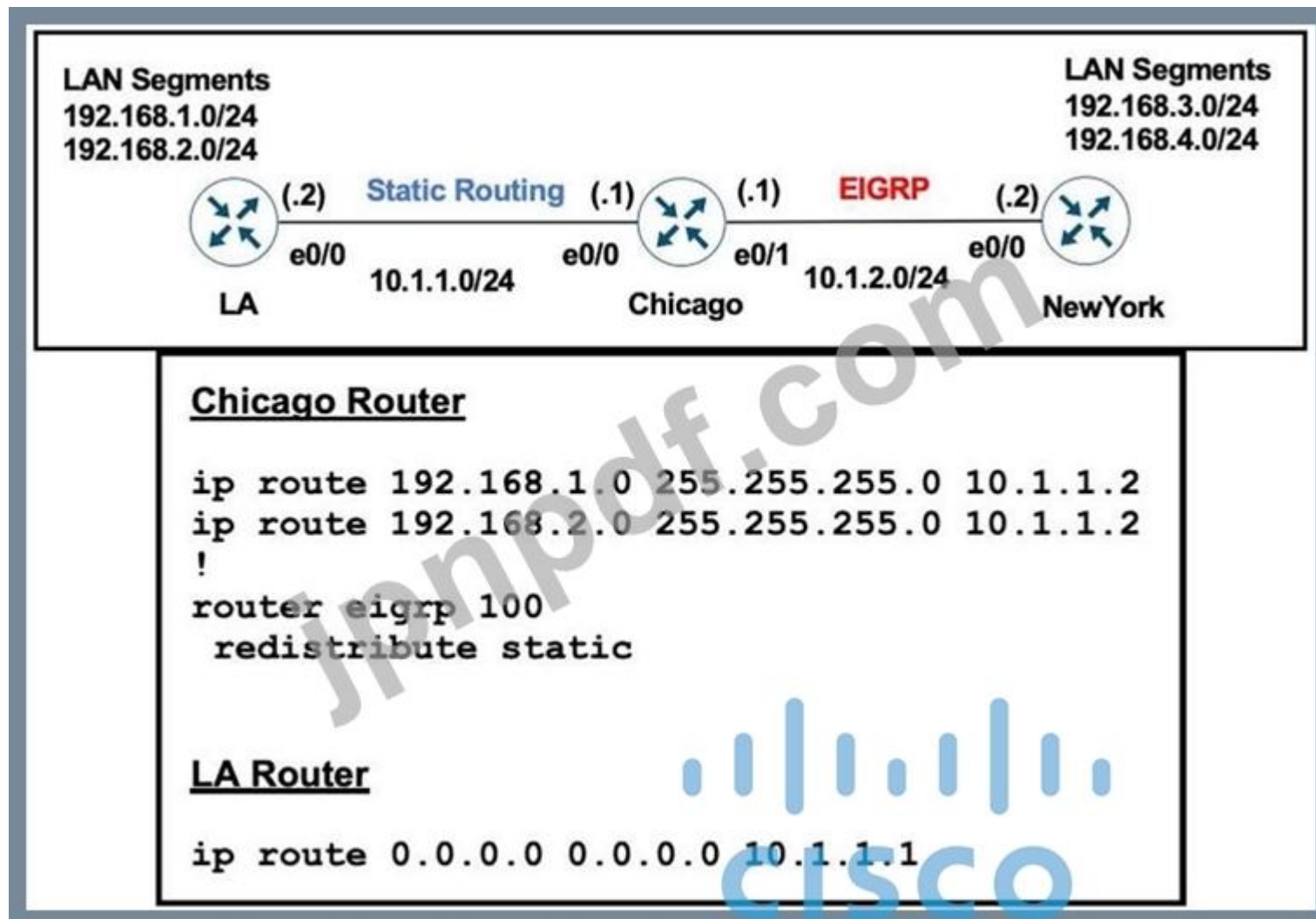


Answer:



最新問題: 116

展示品をご覧ください。



192.168.1.0/24ネットワーク上のユーザーは192.168.3.1に正常にpingを実行できますが、管理者はLAルーターから192.168.3.1にpingを実行できません。問題を解決する構成のセットはどれですか？

A)

Chicago Router

```
router eigrp 100
 redistribute static metric 10 10 10 10 10
```

B)

Chicago Router

```
router eigrp 100
 redistribute connected
```

C)

Chicago Router

```
ip route 192.168.3.0 255.255.255.0 10.1.2.2
ip route 192.168.4.0 255.255.255.0 10.1.2.2
```

D)

LA Router

```
ip route 192.168.3.0 255.255.255.0 10.1.1.1
ip route 192.168.4.0 255.255.255.0 10.1.1.1
```

A. オプションA

B. オプションC

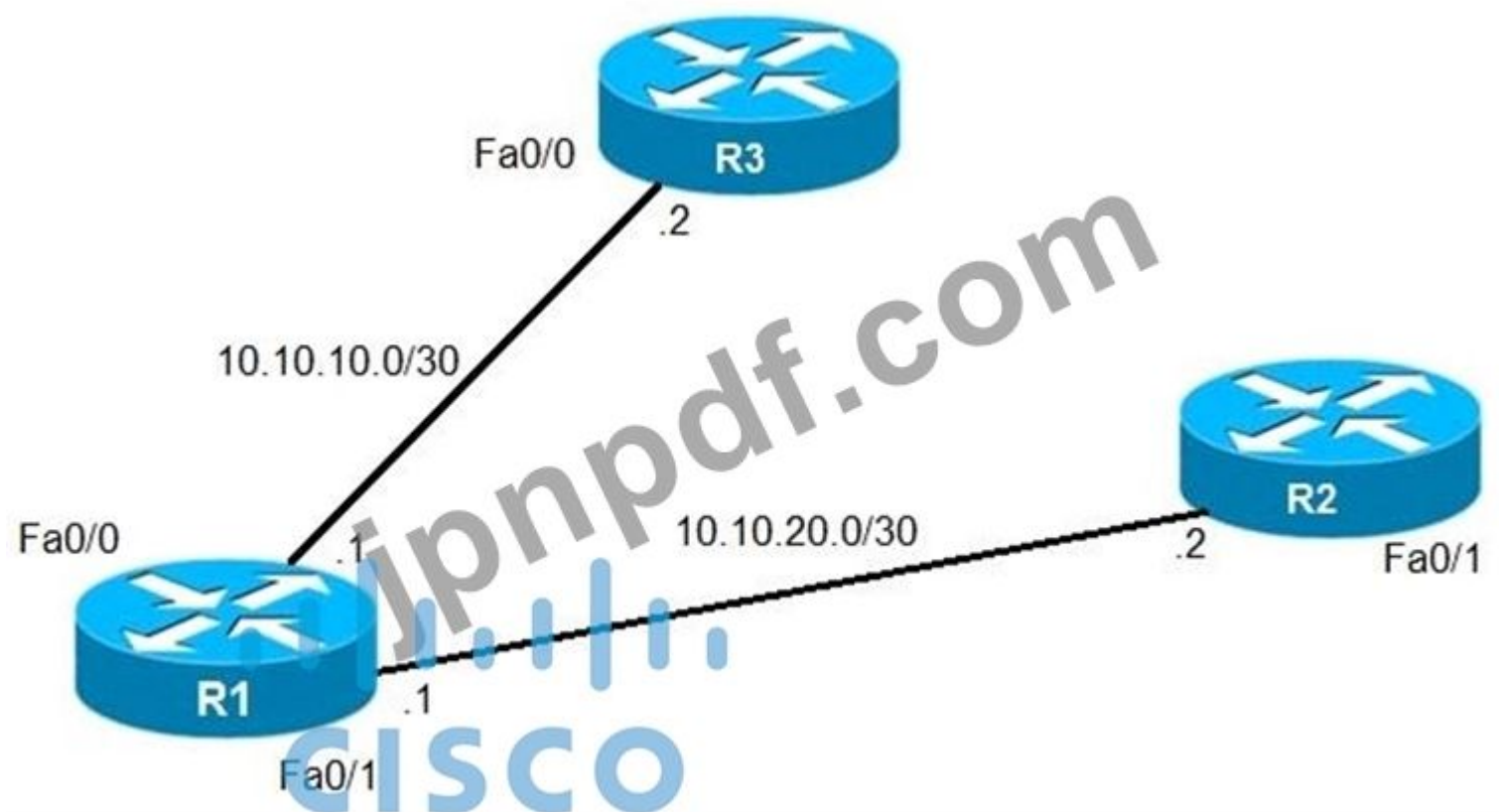
C. オプションB

D. オプションD

Answer: A (メッセージを残す)

最新問題: 117

展示を参照してください。



IP SLAがルータR1に設定され、Fa0/0がルータR3Fa0/0インターフェイスとの到達可能性を失った場合にデフォルトルートを変更できるようになりました。ルートがルータR2を通過するように変更されました。この問題のトラブルシューティングに使用されるデバッグコマンドはどれですか？

A. デバッグIPフロー

B. debug ip sla error

C. デバッグIPルーティング

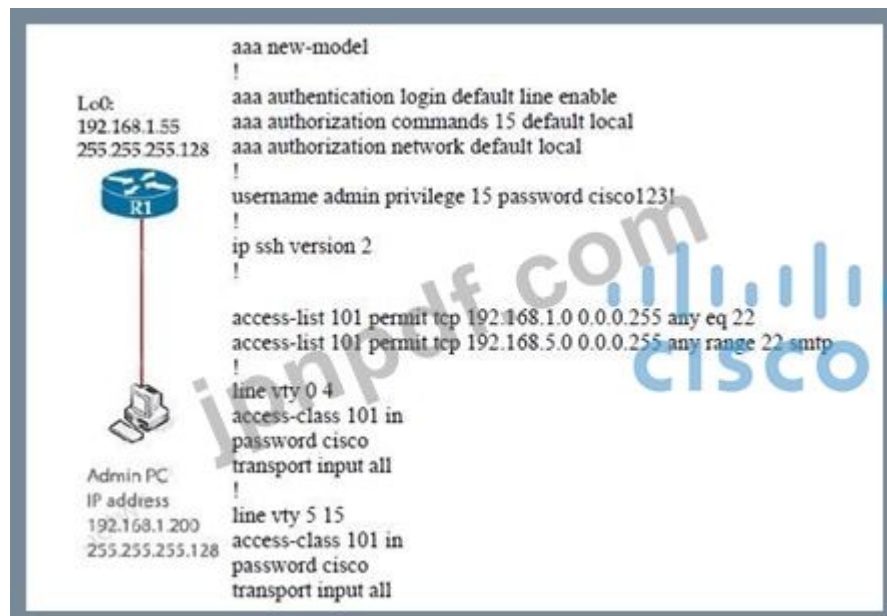
D. ipパケットをデバッグします

Answer: C (メッセージを残す)

debug ip routingこのコマンドは、ルーティングテーブルに関連するメッセージのデバッグを有効にします。

最新問題: 118

展示を参照してください。



管理者はR1に正常にログインしますが、特権モードコマンドにアクセスできません。問題を解決するには何を構成する必要がありますか？

- A. aaaauthorizationリバースアクセス
- B. シークレットまたはパスワードコマンドを有効にして特権モードに入る
- C. 秘密のcisco123！パスワードcisco123の代わりにusernameコマンドの最後に！
- D. vty回線のパスワードをcisco123と一致させます！

Answer: ([解答を表示する](#))

最新問題: 119

展示を参照してください。R2はルータリフレクターであり、R1とR3はルータリフレクタークライアントです。ルータリフレクターは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。

ルータがアドバタイズ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はプレフィックスを他のクライアントにアドバタイズしません。
- B. ルートリフレクターのセットアップには、ルーター間に完全な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設定では、プレフィックスはクライアント間でアドバタイズされません。

Answer: A ([メッセージを残す](#))

セクション :レイヤー3テクノロジー

最新問題: 120

展示を参照してください。エンジニアが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。デバイスはTACACS+を使用して認証しようとしています。

どのアクションが目的の構成を生成しますか？

```
R1#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login Console local
R1#show running-config | section line
line con 0
 logging synchronous
R1#
```

- A. グローバル設定にaaa authentication login default none コマンドを追加します。
- B. aaa authentication login Console local コマンドで、大文字の C を小文字の c に置き換えます。
- C. グローバル設定にaaa authentication login default group tacacs+ local-case コマンドを追加します。
- D. login authentication Console コマンドを回線構成に追加します

Answer: D ([メッセージを残す](#))

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: 121

展示を参照してください。

```
Router# show tag-switching tdp bindings
(...)
tib entry: 10.10.10.1/32, rev 31
  local binding: tag: 18
  remote binding: tsr: 10.10.10.1:0, tag: imp-null
  remote binding: tsr: 10.10.10.2:0, tag: 18
  remote binding: tsr: 10.10.10.6:0, tag: 21
tib entry: 10.10.10.2/32, rev 22
  local binding: tag: 17
  remote binding: tsr: 10.10.10.2:0, tag: imp-null
  remote binding: tsr: 10.10.10.1:0, tag: 19
  remote binding: tsr: 10.10.10.6:0, tag: 22
```

MPLS VPNクラウドでimp-nullタグは何を表していますか？

- A. ラベルをポップします
- B. ラベルを付ける
- C. EXPビットを含める
- D. EXPビットを除外する

Answer: A ([メッセージを残す](#))

説明

imp-null (implicit null) タグは、パケットを転送する前に、タグエントリをタグスタックからポップするようにアップストリームルータに指示します。

注 : ポップとは、上部のMPLSラベルを削除することを意味します

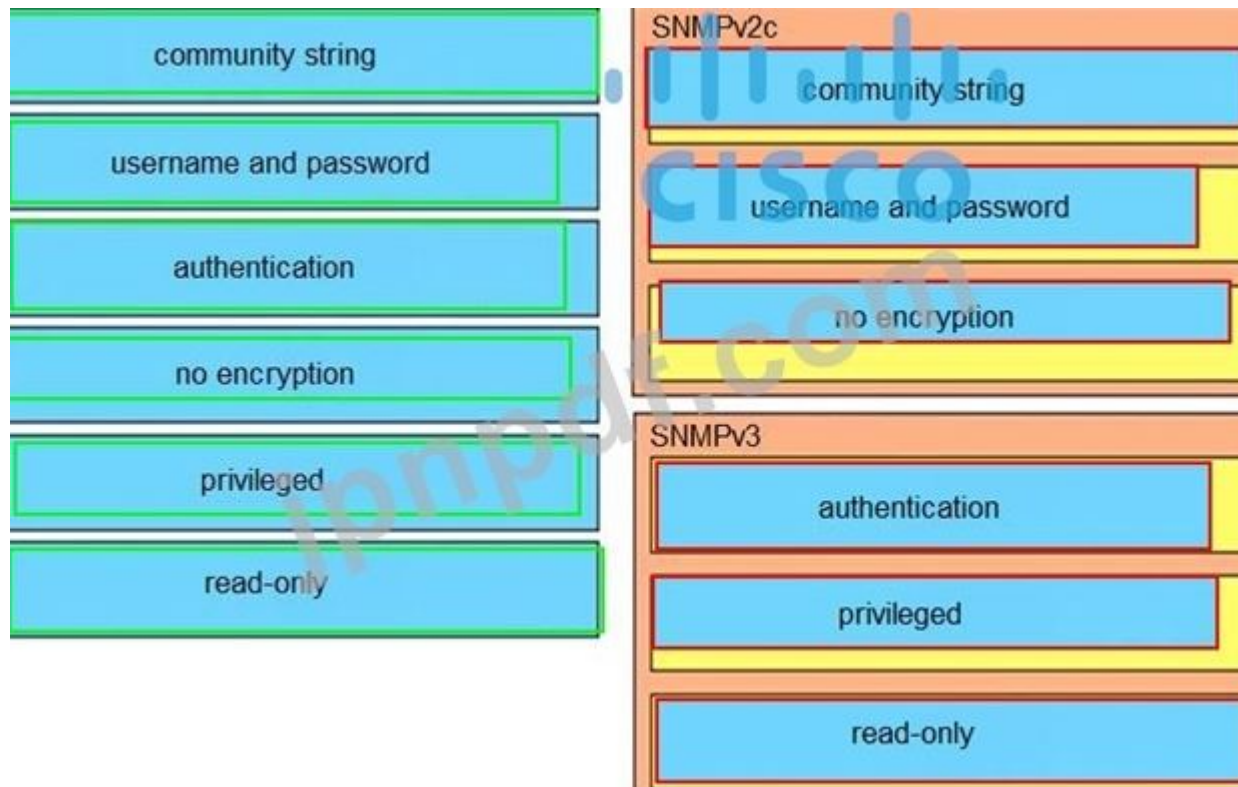
有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 122

Cisco IOSデバイスのSNMP属性を左側から、右側の正しいSNMPv2cまたはSNMPV3カテゴリにドラッグアンドドロップします。

community string	SNMPv2c
username and password	
authentication	
no encryption	
privileged	SNMPv3
read-only	

Answer:



最新問題: 123

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
  
```

ユーザーから、DHCPサーバーからIPアドレスを取得できないと報告されました。DHCPサーバーは次のように構成されています。このDHCPサーバーを使用している非同時ユーザーは合計で約300人ですが、1日2時間以上アクティブになっているユーザーはいません。現在のリソース」

- A. DHCPリース時間をより大きな値に設定します
- B. network192.168.2.0255.255.255.0コマンドをDHCPプールに追加します
- C. サブネットマスクをDHCPプールのnetwork192.168.1.0255.255.254.0コマンドに変更します
- D. DHCPリース時間を小さい値に設定します

Answer: A (メッセージを残す)

最新問題: 124

展示を参照してください。

```
R1(config)#route-map ADD permit 20
R1(config-route-map)#set tag 1

R1(config)#router ospf
R1(config-router)#redistribute rip subnets route-map ADD
```

R1について正しい説明はどれですか。

- A. OSPFは、タグが1の場合にのみRIPルートを再配布します。
- B. RIPルートは変更なしでOSPFに再配布されます。
- C. R1は、OSPFに再配布する前に、RIPで学習したルートのメトリックに1を追加します。
- D. RIPで学習したルートは、タグ値1でOSPFに配布されます。

Answer: [\(解答を表示する\)](#)

最新問題: 125

展示を参照してください。

```
Sending 5, 100-byte ICMP Echos to AB01:2011:7:100::3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

エンジニアがルータR1とR3の間にBGPを設定しました。BGPピアは、ルートを交換できるようにネイバー隣接関係を確立できません。この問題を解決する構成はどれですか？

A. R3

ルータ-bgp6502

ネイバーAB01 2011 :7 :100 :: 1 ebgp-multihop 255

B. R1

router bgp 6501 neighbor AB01 2011 :7 :100 :: 3 ebgp-multihop 255

C. R3

ルータ-bgp6502

アドレスファミリー ipv6

隣人 AB01 2011 :7 :100 :: 1 アクティブ

D. R1

ルータ-bgp6501

アドレスファミリー ipv6

ネイバー AB01 2011 :7 :100; 3 アクティブ化

Answer: C ([メッセージを残す](#))

最新問題: 126

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つ選択してください。)

- A. showsnmpv3ユーザー
- B. debug snmpv3 engine-id
- C. snmpパケットをデバッグします
- D. SNMPユーザーを表示
- E. debug snmp engine-id

Answer: ([解答を表示する](#))

最新問題: 127

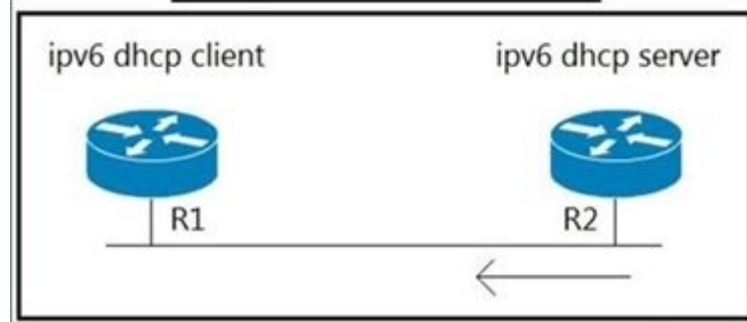
展示を参照してください。

ipv6 dhcp server:

```
ipv6 unicast-routing
!  
int e0/1  
ipv6 enable  
ipv6 add 2001:11::1/64  
ipv6 nd other-config-flag  
no shut  
ipv6 dhcp server IPv6Pool  
!  
ipv6 dhcp pool IPv6Pool  
dns-server 2002:555::1  
domain-name my.net
```

ipv6 dhcp client:

```
interface Ethernet0/1  
no ip address  
ipv6 address dhcp  
ipv6 enable  
no shut
```



ネットワーク管理者は、サーバーからIPv6アドレスを取得していないDHCPクライアントのIPv6アドレス割り当てのトラブルシューティングを行っています。

DHCPサーバーからクライアントIPv6アドレスを取得する構成はどれですか？

- A. DHCPサーバーでのipv6dhcpserver自動コマンド
- B. インターフェイスのipv6addressautoconfigコマンド
- C. DHCPサーバーでのservicedhcpコマンド
- D. インターフェイスでのipv6dhcprelay-agentコマンド

Answer: ([解答を表示する](#))

別紙を参照してください。

```
router ospf 10
  router-id 192.168.1.1
  log-adjacency-changes
  redistribute bgp 1 subnets route-map BGP-TO-OSPF
!
route-map BGP-TO-OSPF deny 10
  match ip address 50
route-map BGP-TO-OSPF permit 20
!
access-list 50 permit 172.16.1.0 0.0.0.255
```

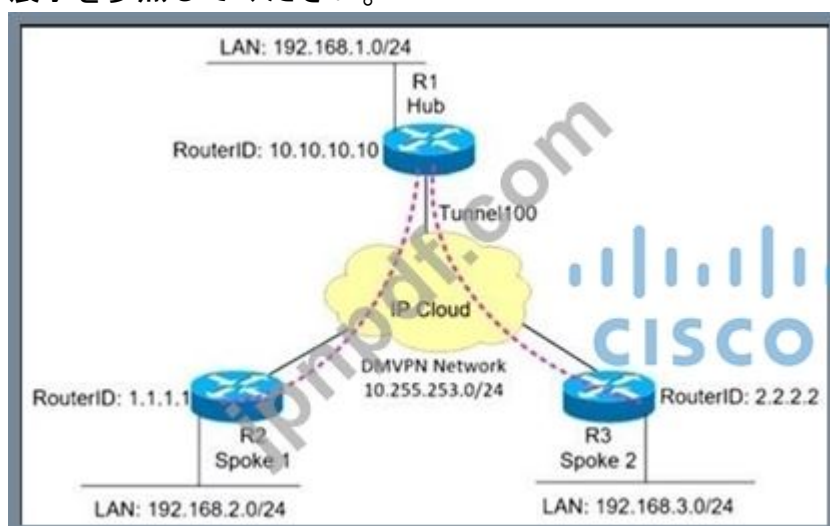
BGPからOSPFプロセス10への再配布について正しい説明はどれですか。

- A. ネットワーク172.16.1.0/24は、管理距離1で再配布されます。
- B. ネットワーク10.10.10.0/24は、管理距離20で再配布されます。
- C. ネットワーク10.10.10.0 / 24はOSPFに再配布されません
- D. ネットワーク172.16.1.0/24はOSPFに再配布されません。

Answer: [\(解答を表示する\)](#)

最新問題: 129

展示を参照してください。



```

Mar 1 17:19:04.051: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Tunnel100 from LOADING to FULL, Loading Done
Mar 1 17:19:06.375: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Tunnel100 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset
Mar 1 17:19:06.627: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Tunnel100 from LOADING to FULL, Loading Done
Mar 1 17:19:10.123: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Tunnel100 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset
Mar 1 17:19:14.499: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.10.10 on Tunnel100 from LOADING to FULL, Loading Done
Mar 1 17:19:19.139: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.10.10 on Tunnel100 from EXSTART to DOWN, Neighbor Down: Interface
down or detached
Mar 1 17:01:51.975: %OSPF-4-NONEIGHBOR: Received database description from unknown neighbor 192.168.1.1
Mar 1 17:01:57.783: OSPF: Rcv LS UPD from 192.168.1.1 on Tunnel100 length 88 LSA count 1
Mar 1 17:01:57.155: OSPF: Send LSP to 192.168.1.1 on Tunnel100 length 100 LSA count 2

```

ネットワーク管理者は、ハブルーター上のDMVPNネットワーク用にOSPFルーティングプロトコルを設定します。複数のスポークでDMVPNトンネルを確立するために必要な構成はどれですか？

- A. ワンスポークルーター上のip ospf network point-to-multipoint
- B. ハブルーター上のipospfnetworkポイントツーポイント
- C. 両方のスポークルーターでのip ospf networkpoint-to-multipoint
- D. 両方のスポークルーターのipospfnetworkポイントツーポイント

Answer: C (メッセージを残す)

最新問題: 130

アドレスを左側から右側の正しいIPv6フィルター目的にドラッグアンドドロップします。

permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443	Permit NTP from this source 2001:0D8B:0800:200c::1f
permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514	Permit syslog from this source 2001:0D88:0800:200c::1c
permit ip 2001:d8b:800:200c::800/117 2001:0DBB:800:2010::/64 eq 80	Permit HTTP from this source 2001:0D8B:0800:200c::0ff
permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123	Permit HTTPS from this source 2001:0D8B:0800:200c::07ff

Answer:

permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443	permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123
permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514	permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514
permit ip 2001:d8b:800:200c::800/117 2001:0DBB:800:2010::/64 eq 80	permit ip 2001:d8b:800:200c::800/117 2001:0DBB:800:2010::/64 eq 80
permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 23	permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443

説明

同じ回答はすでに以下で更新されています：



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

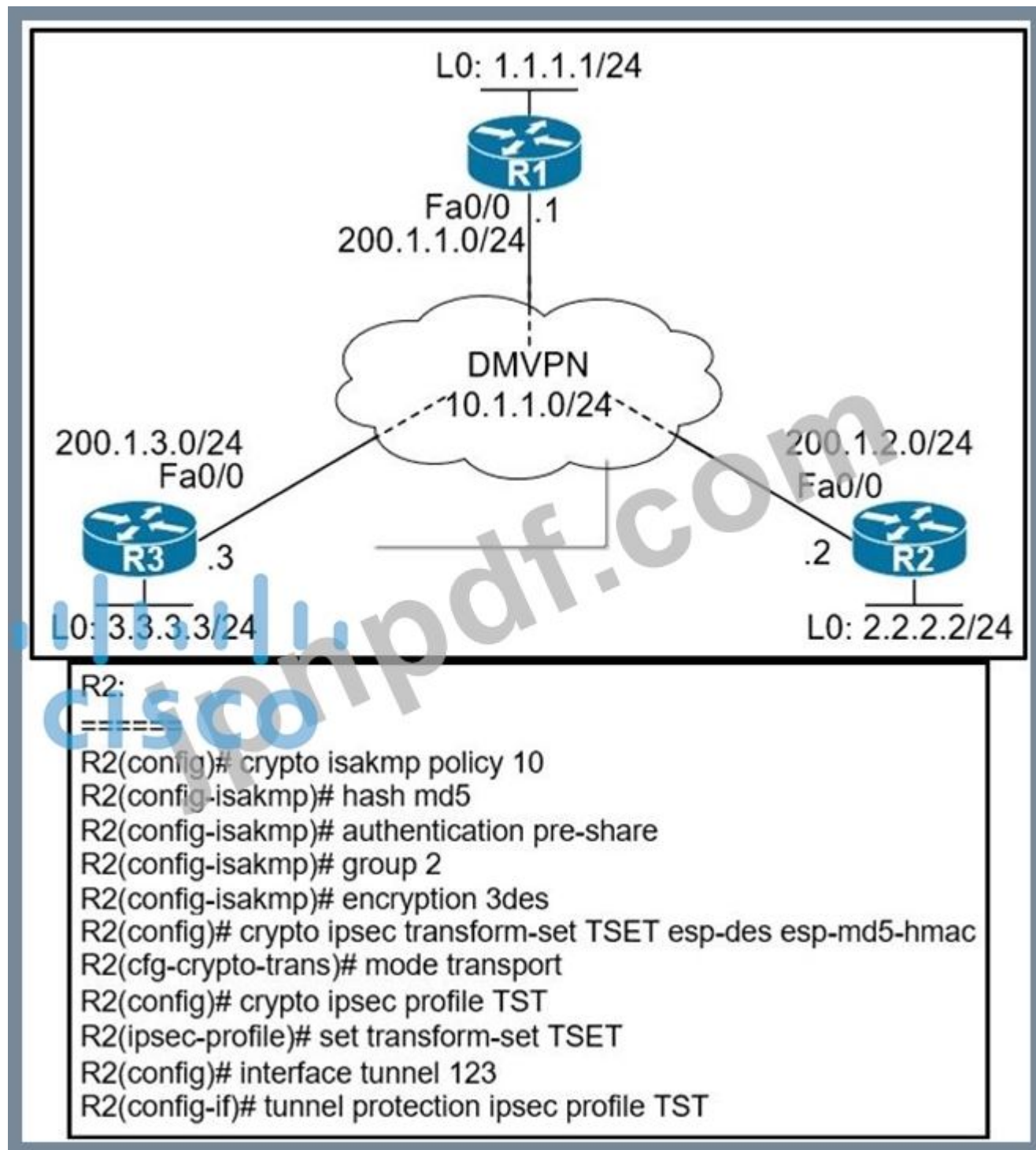
SyslogはUDPポート514で実行され、NTPはUDPポート123で実行されるため、それらを覚えていれば、一致する答えを簡単に見つけることができます。しかし、2001:d88:800:200c::c/126は2001:d88:800:200c:0:0:0:c (合誦つのホスト)の範囲であるため、この質問にはいくつかのタイプミスがあるかもしれません。ホスト2001:0D88:0800:200c::1fは対象外です。についても同じです。

2001:d88:800:200c:0:0:0:cから2001:d88:800:200c:0:0:0:fであり、ホスト2001:0D88:0800:200c::1cをカバーしていません

。

最新問題: 131

展示品をご覧ください。



DMVPNが構成されている場合、トンネルソースとしてループバックを使用するスポークツースポーク通信を許可する構成はどれですか。

- A. ハブでcrypto isakmpkeyciscoアドレス0.0.0.0を設定します。
- B. ハブでcryptoisakmpキーCiscoアドレス200.1.0.0255.255.0.0を設定します。
- C. スポークにcrypto isakmpkeyciscoアドレス200.1.0.0255.255.0.0を設定します。
- D. スポークにcrypto isakmpkeyciscoアドレス0.0.0.0を設定します。

Answer: A (メッセージを残す)

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

最新問題: 132

展示を参照してください。

```

Router#show ip route
<output omitted>
Gateway of last resort is not set

    192.168.1.0/32 is subnetted, 1 subnets
O       192.168.1.1 [110/11] via 192.168.12.1, 16:56:40, Ethernet0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Loopback0
L       192.168.2.2/32 is directly connected, Loopback0
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, Ethernet0/1
L       192.168.3.1/32 is directly connected, Ethernet0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/24 is directly connected, Ethernet0/0
L       192.168.12.2/32 is directly connected, Ethernet0/0
Router#show running-config | section ospf
router ospf 1
  summary-address 10.0.0.0 255.0.0.0
  redistribute static subnets
  network 192.168.3.0 0.0.0.255 area 0
  network 192.168.12.0 0.0.0.255 area 0
Router#

```

エンジニアがネットワーク10.0.0.0/8のOSPFでサマリールートを生成しようとしています。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。サマリー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データベースにのみ表示され、ルーティングテーブルには表示されません。
- C. 10.0.0.0/8内にサブネットのルートがないため、サマリー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には表示されませんが、同じエリア内の他のOSPFルーターには表示されます。

Answer: C (メッセージを残す)

-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のみ、ASBRで使用する必要があります。ただし、要約されたルートを作成するための要件は次のとおりです。

-ASBRは、サマリールートのアドレス範囲を、そのASBR上のOSPFに再配布されたすべてのルートと比較して、従属サブネット (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つの従属サブネットが存在する場合、ASBRはサマリールートをアドバタイズします。

最新問題: 133

IPv6ソースアドレスを転送する必要があるかどうかを判断するために、IPv6ソースガードは何を利用しますか？

- A. ACE

- B. ACLS
- C. DHCP
- D. バインディングテーブル

Answer: ([解答を表示する](#))

IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets; rather, it works

最新問題: 134

次のコマンドの出力は何ですか。

show ip vrf

- A. VRFに関連付けられたショーのルーティングプロトコル情報。
- B. VRFに関連付けられたIPルーティングテーブル情報を表示します
- C. ショーのデフォルトのRD値
- D. 指定されたVRFのARPテーブル（静的および動的エントリ）を表示します

Answer: C ([メッセージを残す](#))

最新問題: 135

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。

Init	Each router compares the DBD packets that were received from the other router.
2-way	Routers exchange information with other routers in the multiaccess network.
Down	The neighboring router requests the other routers to send missing entries.
Exchange	The network has already elected a DR and a backup BDR.
ExStart	The OSPF router ID of the receiving router was not contained in the hello message.
Loading	No hellos have been received from a neighbor router.

Answer:



説明

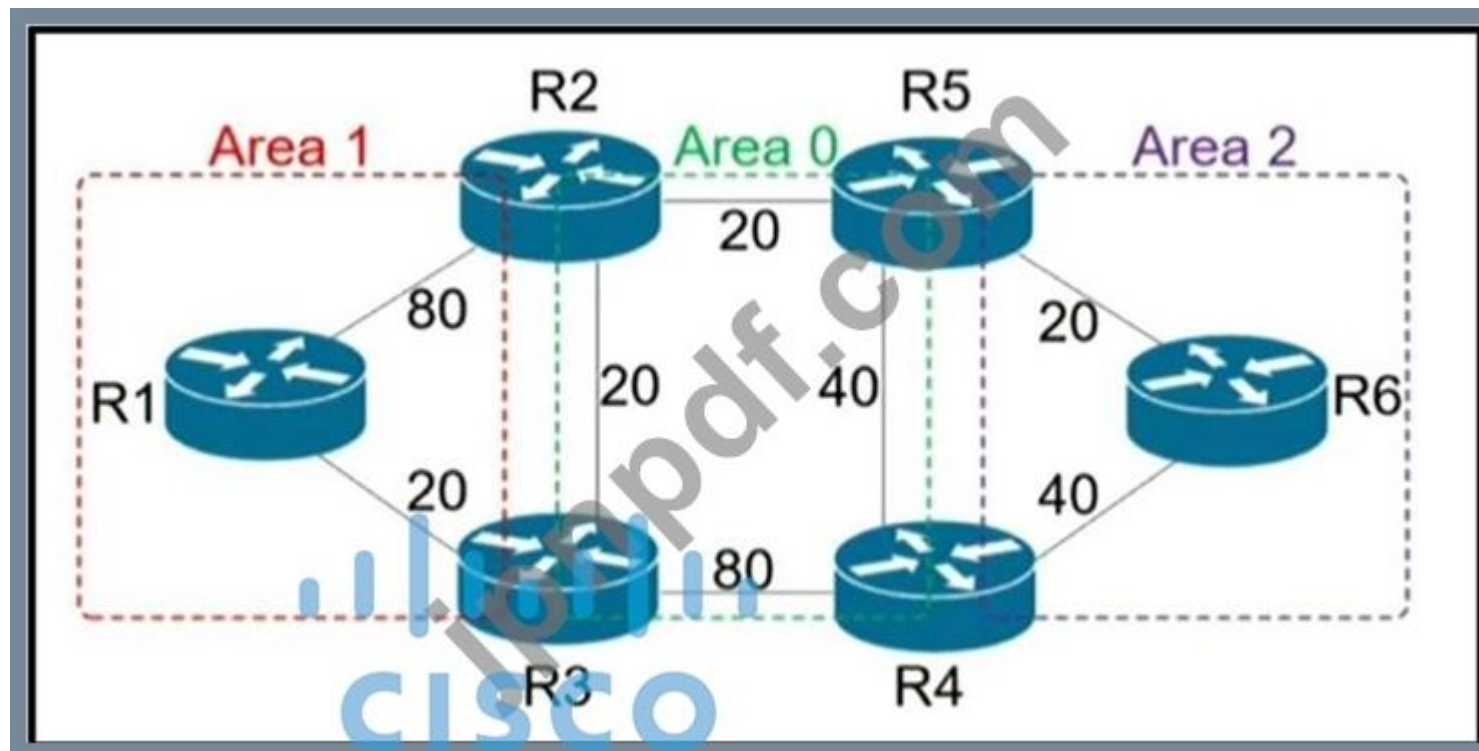


自動的に生成されたテーブルの説明

(参照http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml)

最新問題: 136

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。問題を解決するアクションはどれですか？

- A. R2とR3の間のコストを61に増やします
- 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に増やします
- D. R2とR1の間のコストを41に減らします

Answer: A (メッセージを残す)

有効な 300-410 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の 300-410 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (80030%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 137

MPLSレイヤ3VPN設定でトラフィックのロードバランシングを許可するコマンドはどれですか。

- A. マルチパス eibgp 2
- B. マルチパス 2
- C. 最大パス 2
- D. 最大パス ibgp 2

Answer: D (メッセージを残す)

最新問題: 138

MPLSラベルの内容を定義するリストはどれですか。

- A. 20ビットラベル; 3ビットトラフィッククラス。1ビットのボトムスタック。8ビットTTL

- B. 32ビットラベル; 3ビットトラフィッククラス。1ビットのボトムスタック。8ビットTTL
- C. 20ビットラベル; 3ビットフローラベル; 1ビットのボトムスタック。8ビットホップ制限
- D. 32ビットラベル; 3ビットフローラベル; 1ビットのボトムスタック。8ビットホップ制限

Answer: ([解答を表示する](#))

セクション :VPNテクノロジー

説明/参照 :<https://tools.ietf.org/html/rfc5462>

最新問題: 139

```
router# show ip route
.....
D 192.168.32.0/19 [90/25789217] via 10.1.1.1
R 192.168.32.0/24 [120/4] via 10.1.1.2
O 192.168.32.0/26 [110/229840] via 10.1.1.3
```

展示を参照してください。エンジニアが192.168.32.100を10.1.1.1経由で転送しようとしていますが、10.1.1.2経由で転送されました。10.1.1.1を介してパケットを転送するアクションは何ですか？

- A. より低いメトリックで192.168.32.0ルートを受信するようにEIGRPを設定します。
- B. プレフィックスが/24以上の192.168.32.0ルートを受信するようにEIGRPを設定します。
- C. 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。
- D. /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。

Answer: ([解答を表示する](#))

最新問題: 140

エンジニアは、デフォルトの属性を持つBGPを使用して、2つの異なるサービスプロバイダーに接続された2つのルーターを構成しました。リンクの1つが高遅延を示しているため、ネットワークの速度が低下しています。2番目のISPリンクが稼働している場合に、高遅延ISPリンクの使用を回避するためにエンジニアが構成する必要があるBGP属性はどれですか。

- A. 重量
- B. LOCAL_PREF
- C. MED
- D. AS-PATH

Answer: A ([メッセージを残す](#))

最新問題: 141

展示を参照してください。

```
R2#show policy-map control-plane
Control Plane
Service-policy input: CoPP
Class-map: SSH (match-all)
 29 packets, 2215 bytes
 5 minute offered rate 0000 bps
 Match: access-group 100

Class-map: ANY (match-all)
 46 packets, 3878 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: access-group 199
 drop

Class-map: class-default (match-any)
 41 packets, 5687 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: any

R2#show access-list 100
Extended IP access list 100
 10 deny tcp any any eq 22 (14 matches)
 20 permit tcp host 192.168.12.1 any eq 22 (29 matches)
R2#show access-list 199
Extended IP access list 199
 10 permit ip any any (51 matches)
```

展示を参照してください。192.168.12.1からR2へのアクセスを制限するアクションはどれですか？

- A. シーケンス10を変更して、アクセスリスト100へのtcp any eq22anyを拒否します。
- B. シーケンス20を変更して、tcp host 192.168.12.1 eq22anyがアクセスリスト100にアクセスできるようにします。
- C. アクセスリスト100のシーケンス10をシーケンス20と交換します。
- D. アクセスリスト100のシーケンス20をシーケンス10と交換します

Answer: ([解答を表示する](#))

最新問題: 142

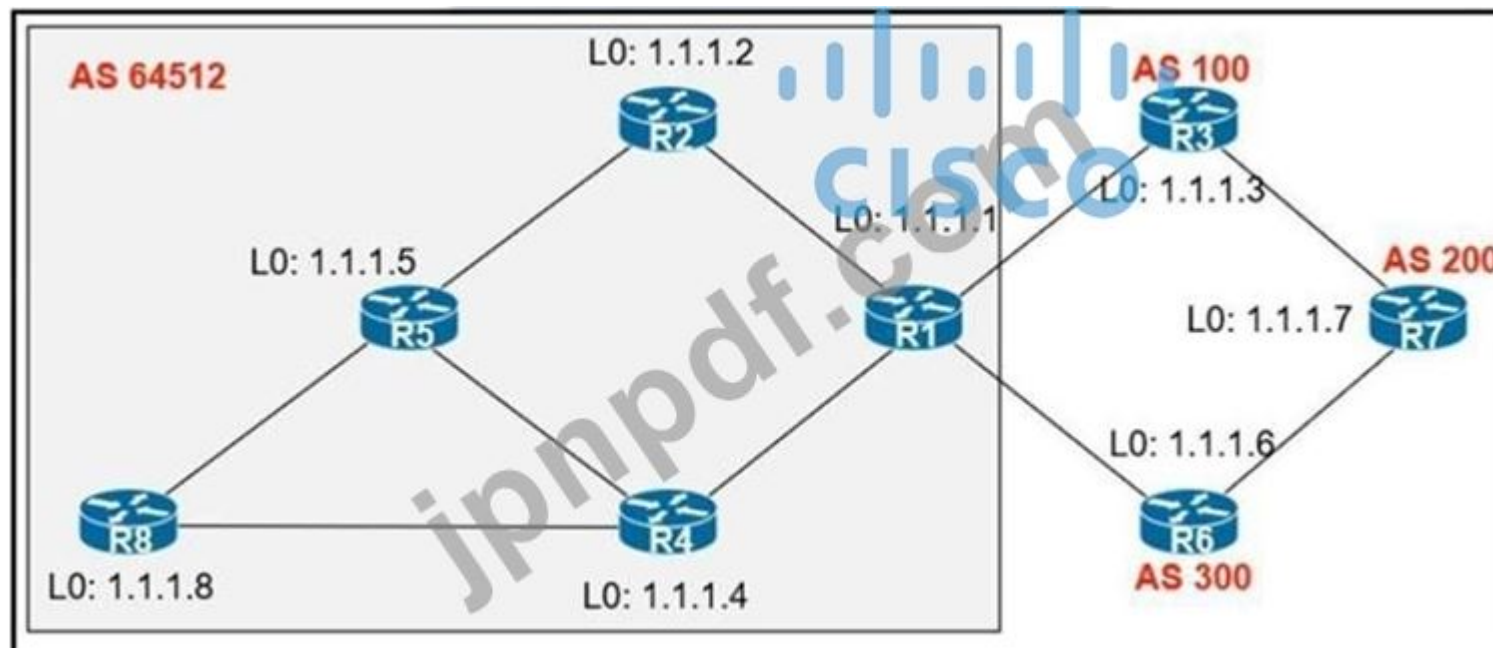
BFDの機能は何ですか？

- A. ルーティングプロトコルとメディアタイプに依存する障害検出
- B. ルーティングプロトコルやメディアタイプに依存しない障害検出
- C. レイヤ2隣接障害後のピアリカバリ
- D. レイヤ3プロトコル隣接障害後のピアリカバリ

Answer: A ([メッセージを残す](#))

最新問題: 143

示す :



エンジニアは、R2とR5をルートリフレクターとして設定し、eBGPピアにアドバタイズするためにすべてのルートがR1に送信されるわけではないことに気づきました。すべてのネットワークで到達可能性を復元するためにすべてのルートをアドバタイズするために、どのiBGPルーターをルートリフレクターとして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 (メッセージを残す)

説明

R2とR5がルートリフレクター (RR) の場合、R4と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はそれらを削除します。したがって、eBGPピアにアドバタイズするための一部のルートがR1にありません。

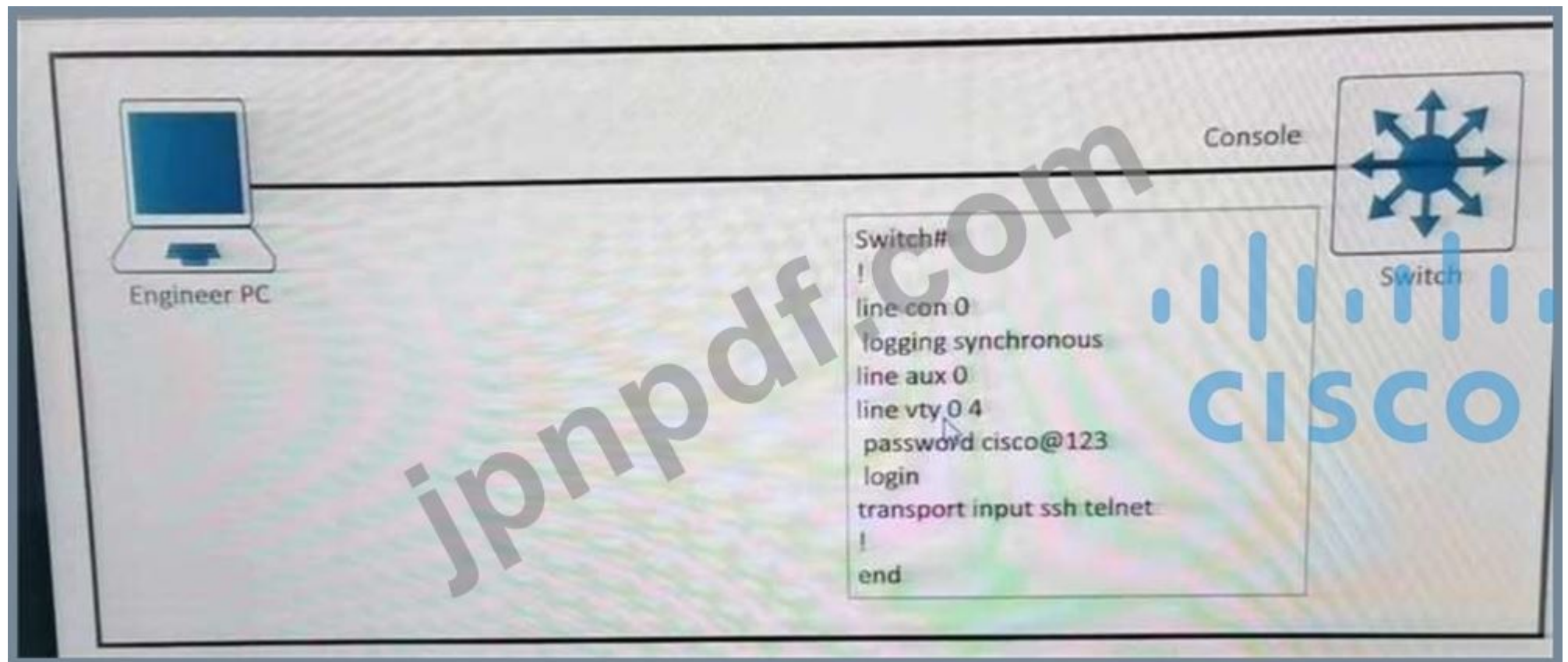
良い参考資料：

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/TECRST-2310.pdf> ルートリフレクター (RR) は完全にiBGPメッシュである必要があるため、R1とR1の両方でRRを構成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: 144

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の高床式はコンソールポートを介して接続できます。コンソールポートのどの構成で問題が解決しますか？

- A. exec 0.0
- B. ログインとパスワード
- C. 幹部なし
- D. トランスポート入力telnet

Answer: C (メッセージを残す)

最新問題: 145

展示を参照してください。

Router Configuration:

```
ip vrf customer_a
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
interface FastEthernet0.1
 encapsulation dot1q 2
 ip vrf forwarding customer_a
 ip address 192.168.4.1 255.255.255.0
!
router ospf 1
 log-adjacency-changes
!
router ospf 2 vrf customer_a
 log-adjacency-changes
 network 192.168.4.0 0.0.0.255 area 0
!
end
```

ネットワーク管理者は、顧客A用にVRF liteを構成しました。
リモートサイトの技術者がルータのVRFを誤って設定しました。
customer_aの両方のサイトの接続を解決する構成はどれですか？

- ip vrf customer_a
 rd 1:1
 route-target export 1:2
 route-target import 1:2
- ip vrf customer_a
 rd 1:1
 route-target import 1:1
 route-target export 1:2
- ip vrf customer_a
 rd 1:2
 route-target both 1:2
- ip vrf customer_a
 rd 1:2
 route-target both 1:1

- 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: D (メッセージを残す)

展示から、私たちは次のことを学びました。

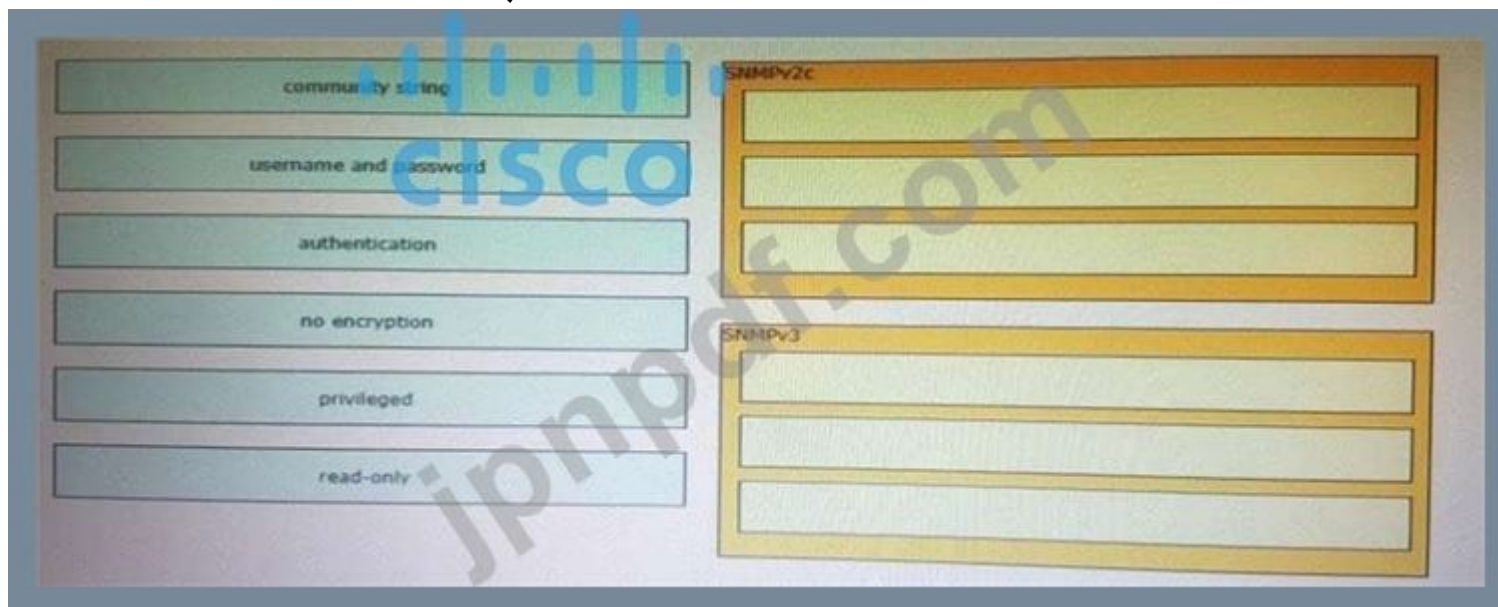
+ VRF customer_aは1:1のルートターゲット (RT) でエクスポートされたため、リモートサイトでは同じRT 1:1でインポートする必要があります。

+ VRF customer_aは1 :1のルートターゲット (RT)でインポートされたため、リモートサイトでは同じRT 1 :1でエクスポートする必要があります。

したがって、リモートサイトでは、コマンド foute-target both 1 :1」を設定する必要があります。これは、foute-target import1 :1」と foute-targetexport1 :1」の2つのコマンドに相当します。

最新問題: 146

Cisco IOSデバイスのSNMP属性を、右側の正しいSNMPv2cまたはSNMPv3カテゴリにドラッグアンドドロップします。



Answer:



説明

SNMPv2c :

コミュニティ文字列

ユーザー名とパスワード

暗号化なし

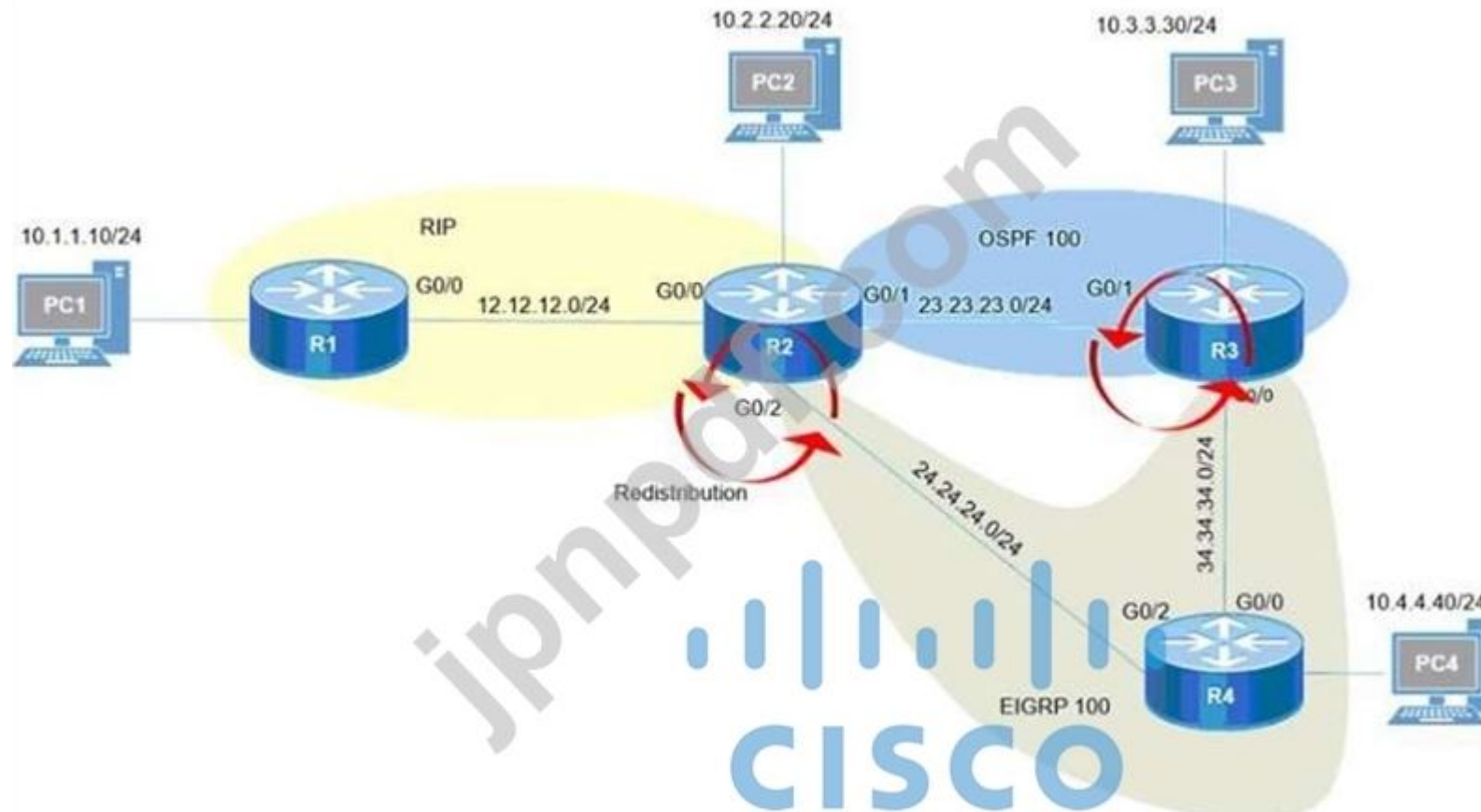
SNMPv3 :

認証

読み取り専用
特権

最新問題: 147

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り、PC2 PC3になり、PC4はPC1に到達できなくなります。問題を解決するための2つの解決策は何ですか？ 2つ選択してください。)

- A. R2でRIPに再配布するときに、RIPルートをRIPにフィルターで戻す
- B. R2のRIPに再配布するときに、OSPFルートをRIPFROMEIGRPにフィルタリングします。
- C. R2で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でOSPFに再配布するときに、EIGRPからOSPFに戻るRIPおよびOSPFルートをフィルタリングします
- E. R3で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 (メッセージを残す)

説明

PC2でさえPC1に到達できないため、R2でのRIPの再配布に問題があります。RIPはOSPFおよびEIGRPよりも管理距離 (AD) 値が高いため、相互再配布を行うときにループされます。

最新問題: 148

展示を参照してください。

```
*17:40:07.826: AAA/BIND(00000055): Bind i/f
*17:40:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*17:40:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*17:40:07.826: TPLUS: TPLUS(00000055) login timer started 1020 sec timeout
*17:40:07.826: TPLUS: processing authentication start request id 85
*17:40:07.826: TPLUS: Authentication start packet created for 850
*17:40:07.826: Using server 10.106.60.182
*17:40:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*17:40:07.830: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.830: TPLUS(00000055)/0/READ: Would block while reading
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*17:40:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*17:40:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*17:40:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

エンジニアがTACACSの問題のトラブルシューティングを行っています。

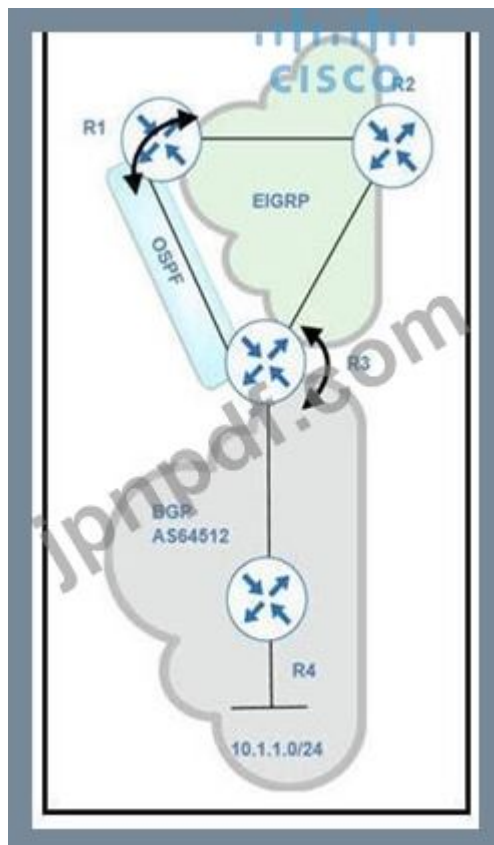
問題を解決するアクションはどれですか？

- A. 設定されたAAAプロファイルをVTYに適用します。
- B. 一致するTACACSサーバーIPを構成します。
- C. 一致する事前共有キーを構成します。
- D. 相対ソースインターフェースから認証を生成します。

Answer: C (メッセージを残す)

最新問題: 149

展示を参照してください。



BGPとEIGRPはR3で相互に再配布され、EIGRPとOSPFはR1で相互に再配布されます。

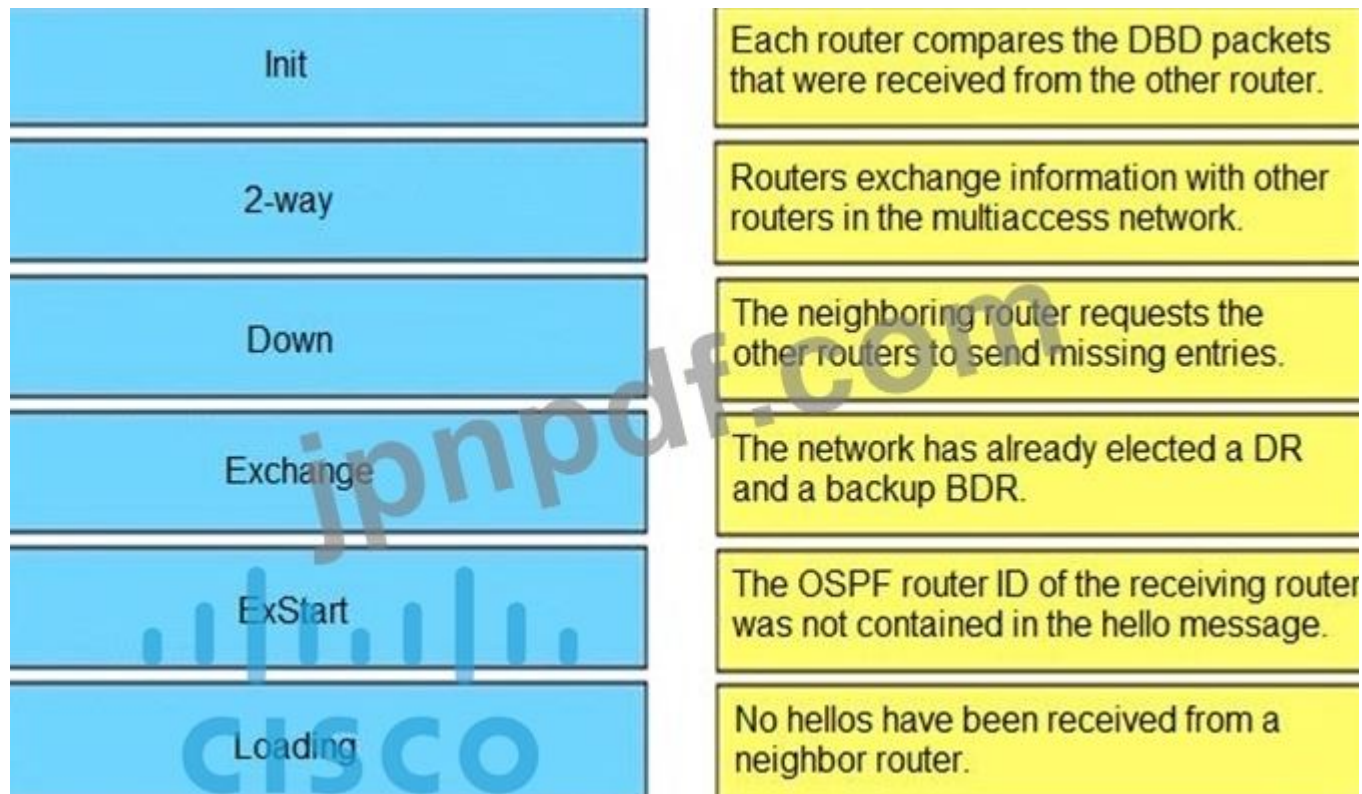
ユーザーは、10.1.1.0/24プレフィックスでホストされているアプリケーションにパケット損失とサービスの中断を報告します。エンジニアは、パケット損失がない状態でR3からR4へのリンクをテストしましたが、debugiprouteコマンドを実行するとR3で頻りにルーティングが変更されることに気がきました。どのアクションがサービスを安定させますか？

- A. OSPF配布リストをR3にアウトバウンドして、10.1.10/24プレフィックスがR3にアドバタイズされないようにします。
- B. R3を通過するトラフィックで高いCPUとパケット損失を引き起こすR3での頻りにOSPFSPF計算を減らします。
- C. ローカル10.1.1.0/24プレフィックスでICMP pingを使用してR4からテストを繰り返し、サブネットのホスト側またはスイッチ側でレイヤー2エラーを修正します。
- D. 10.1.1.0/24プレフィックスにタグを付け、プレフィックスがR1のOSPFに再配布されないようにします。

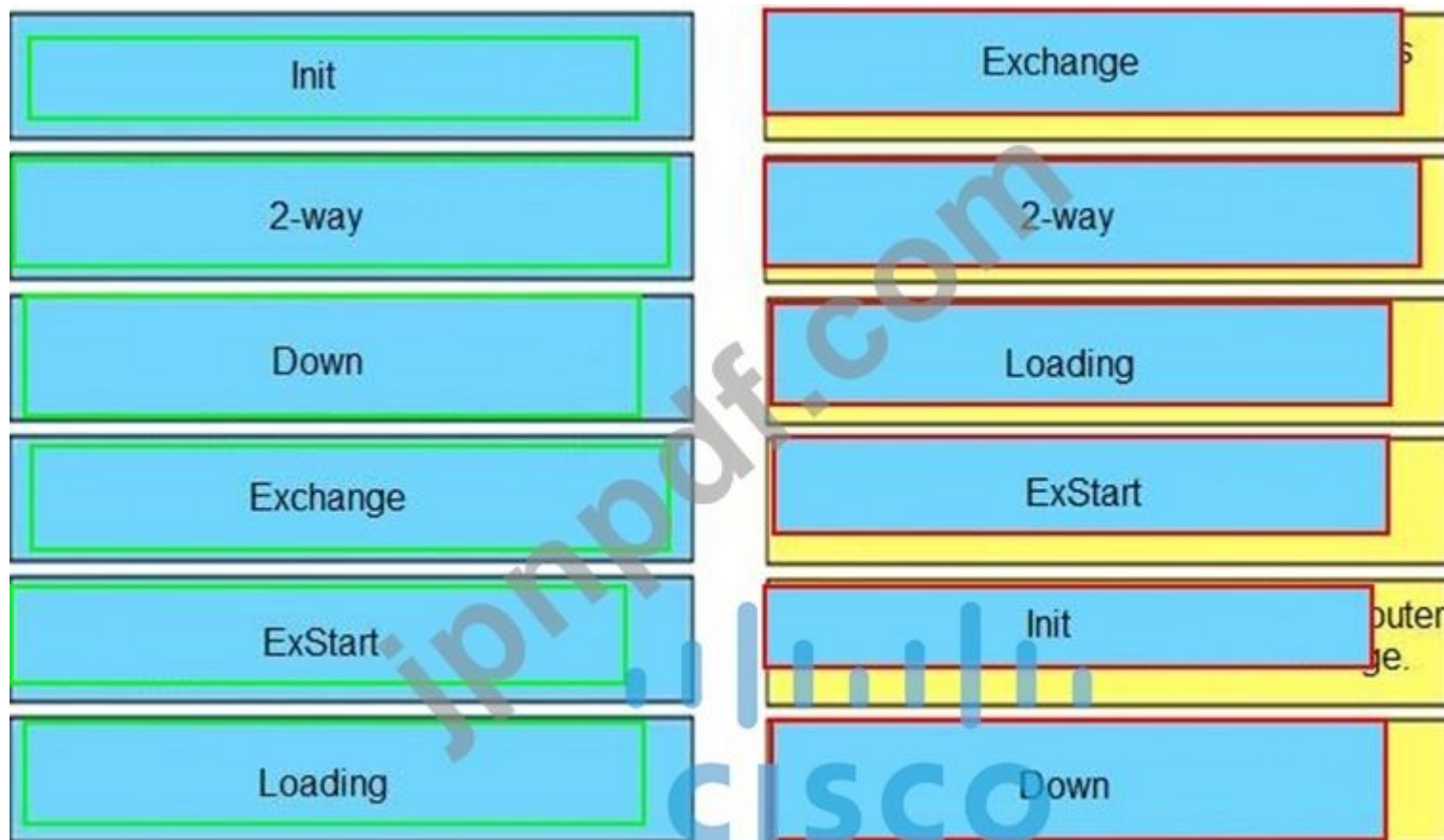
Answer: D (メッセージを残す)

最新問題: 150

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:



(参照http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml)

最新問題: 151

ラベルエッジルータによって実行されるラベル操作はどれですか。

A. スワップとポップ

B. スワップとプッシュ

C. PUSHとPHP

D. プッシュとポップ

Answer: ([解答を表示する](#))

説明

ラベルエッジルーター (LER、MPLSネットワークのエッジで動作し、ネットワークの入口と出口のポイントとして機能します。LERはMPLSラベルを着信パケットにプッシュし、発信パケットからポップします。

有効な 300-410 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の 300-410 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (80030%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 152

展示を参照してください。

```
Router#sh ip route ospf
<output omitted>
Gateway is last resort is not set

    10.0.0.0/24 is subnetted, 1 subnets
    o E2   10.0.0.0 [110/20] via 192.168.12.2, 00:00:10, Ethernet0/0
    o     192.168.3.0/24 [110/20] via 192.168.12.2, 00:00:50, Ethernet0/0
Router#
Router#show ip bgp
<output omitted>
   Network        Next Hop        Metric      LocPrf        Weight        Path
>*  192.168.1.1/32  0.0.0.0         0           32768         ?
>*  192.168.3.0    192.168.12.2   20          32768         ?
>*  192.168.12.0   0.0.0.0         0           32768         ?
Router#show running-config | section router bgp
router bgp 65000
  bgp log-neighbor-changes
  redistribute ospf 1
Router#
```

エンジニアがOSPFをBGPに再配布しようとしていますが、すべてのルートが再配布されているわけではありません。

この問題の理由は何ですか？

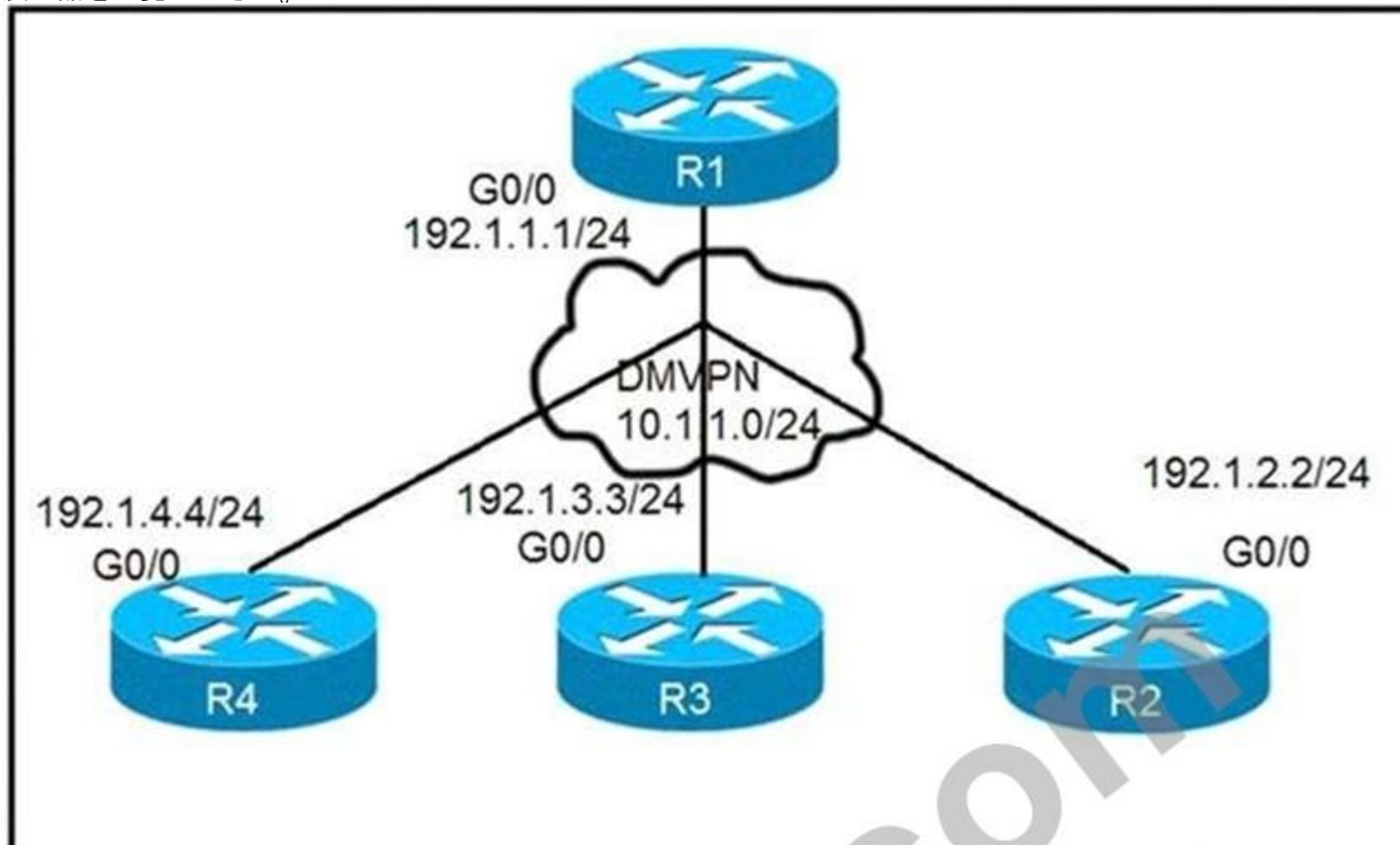
A. デフォルトでは、内部ルーターと外部タイプ1ルートのみがBGPに再配布されます。

- B. BGPコンバージェンスが遅いため、ルートは最終的にBGPテーブルに存在します。
- C. クラスフルネットワークのみがOSPFからBGPに再配布されます。
- D. デフォルトでは、内部OSPFルートのみがBGPに再配布されます

Answer: [\(解答を表示する\)](#)

最新問題: 153

展示品をご覧ください。



```
On R1:  
R1(config)# interface tunnel 1  
R1(config-if)# ip address 10.1.1.1 255.255.255.0  
R1(config-if)# tunnel source 192.1.1.1  
R1(config-if)# tunnel mode gre multipoint  
R1(config-if)# ip nhrp network-id 111
```

```
On R2:  
R2(config)# interface tunnel 1  
R2(config-if)# ip address 10.1.1.2 255.255.255.0  
R2(config-if)# tunnel source FastEthernet0/0  
R2(config-if)# tunnel mode gre multipoint  
R2(config-if)# ip nhrp network-id 222  
R2(config-if)# ip nhrp nhs 10.1.1.1  
R2(config-if)# ip nhrp map 10.1.1.1 192.1.1.1
```



```
On R3:  
R3(config)# interface tunnel 1  
R3(config-if)# ip address 10.1.1.3 255.255.255.0  
R3(config-if)# tunnel source FastEthernet0/0  
R3(config-if)# tunnel mode gre multipoint  
R3(config-if)# ip nhrp network-id 333 R3(config-if)# ip nhrp nhs 10.1.1.1  
R3(config-if)# ip nhrp map 10.1.1.1 192.1.1.1
```

```
On R4: R4(config)# interface tunnel 1  
R4(config-if)# ip address 10.1.1.4 255.255.255.0  
R4(config-if)# tunnel source FastEthernet0/0  
R4(config-if)# tunnel mode gre multipoint  
R4(config-if)# ip nhrp network-id 444  
R4(config-if)# ip nhrp nhs 10.1.1.1  
R4(config-if)# ip nhrp map 10.1.1.1 192.1.1.1
```

DMVPNのスポークツースポーク間にフェーズ3トンネルを確立することはできません。欠落している2つのコマンドはどれですか？ 2つ選択してください。）

- A. スポークルータにipnhrpredirectコマンドがありません。
- B. ハブルータにipnhrpredirectコマンドがありません。
- C. ハブルータにipnhrpショートカットコマンドがありません。
- D. ハブルータにipnhrpmapコマンドがありません。
- E. スポークルータにipnhrpショートカットコマンドがありません。

Answer: B,D (メッセージを残す)

最新問題: 154

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. 10.1.4.0/26
- D. 10.2.2.0/24

Answer: D (メッセージを残す)

最新問題: 155

展示を参照してください。

```

R200#show ip bgp summary
BGP router identifier 10.1.1.1, local AS number 65000
BGP table version is 26, main routing table version 26
1 network entries using 132 bytes of memory
1 path entries using 52 bytes of memory
2/1 BGP path/bestpath attribute entries using 296 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 28 bytes of memory
BGP using 508 total bytes of memory
BGP activity 24/23 prefixes, 24/23 paths, scan interval 60 secs
Neighbor      V    AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.0.2.2     4 65100 20335   20329    0 0    0 00:02:04 Idle (PfxCt)
R200#

```

どのような状況でBGPネイバーはアイドル状態のままになりますか？

- A. プレフィックスがBGPピアから受信されない場合
- B. インバウンド方向にプレフィックスリストが適用されている場合
- C. プレフィックスが上限に達した場合
- D. プレフィックスが上限を超えた場合

Answer: ([解答を表示する](#))

最新問題: 156

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引き続き存在します。どのアクションがルートをブロックしますか？

- A. 標準の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。
- 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. route-mapコマンドのシーケンス10をpermitからdenyに変更します。
- D. 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-DL deny20。

Answer: C ([メッセージを残す](#))

最新問題: 157

IPv6First-HopSecurity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。

IPv6 DHCPv6 Guard	Block a malicious host and permit the router from a legitimate route.
IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents.
IPv6 Source Guard	Create a binding table that is based on NS and NA messages.
IPv6 RA Guard	Filter inbound traffic on Layer 2 switch ports that are not in the IPv6 binding table.
IPv6 ND Inspection	Create IPv6 neighbors connected to the device from information sources such as NDP snooping.

Answer:

IPv6 DHCPv6 Guard	IPv6 RA Guard
IPv6 Binding Table	IPv6 DHCPv6 Guard
IPv6 Source Guard	IPv6 ND Inspection
IPv6 RA Guard	IPv6 Source Guard
IPv6 ND Inspection	IPv6 Binding Table

最新問題: 158

展示を参照してください。

```

Ipv6 unicast-routing
!
Router ospfv3 4
  Router-id 192.168.1.1
!
Interface E 0/0
  Ipv6 enable
  Ip address 10.1.1.1 255.255.255.0
  Ospfv3 4 area 0 ipv4
  No shut
!
Interface Loopback0
  Ipv6 enable
  Ipv4 172.16.1.1 255.255.255.0
  Ospfv3 4 area 0 ipv4

```

ネットワーク管理者は、E 0/0インターフェイスでIPv6用にブランチルーターを構成しました。隣接ルーターは要件を満たすように完全に構

成されていますが、隣接関係が確立されていません。IPv6ネイバーを起動するために、ブランチルータの問題を修正するアクションはどれですか。

A. address-family ipv4 unicastコマンドを使用して、E0/0インターフェイスでIPv4アドレスファミリーを有効にします。

B. no ipv6 enableコマンドを使用して、E0/0インターフェイスでIPv6を無効にします

C. address-family ipv4 unicastコマンドを使用して、ルータospfv34プロセスでIPv4アドレスファミリーを有効にします。

D. E0/0インターフェイスでnoospfv3 4 area 0 ipv4コマンドを使用して、IPv4のOSPFを無効にします。

Answer: C (メッセージを残す)

もう一度、シスコはOSPFv3設定に必要なIOS設定コマンドを変更しました。新しいOSPFv3設定では、以前の「ipv6routerospf」ルーティングプロセスコマンドおよび「ipv6ospf」インターフェイスコマンドの代わりに「ospfv3」キーワードが使用されます。

Open Shortest Path Firstバージョン3 (OSPFv3) アドレスファミリー機能により、IPv4とIPv6の両方のユニキャストトラフィックをサポートできます。この機能を使用すると、ユーザーはインターフェイスごとに2つのプロセスを持つことができますが、アドレスファミリー (AF) ごとに1つのプロセスしかありません。

最新問題: 159

展示を参照してください。

```
service timestamps debug datetime msec
service timestamps log datetime
clock timezone MST -7 0
clock summer-time MST recurring
ntp authentication-key 1 md5 00101A0B0152181206224747071E 7
ntp server 10.10.10.10

R1#show clock
*06:13:44.045 MST Sun Dec 30 2018

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#logging host 10.10.10.20
R1(config)#end
R1#
*Dec 30 13:15:28: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Dec 30 13:15:28: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.10.10.20 port 514
started - CLI initiated
```

管理者は、R1で変更が行われた後、システムログのタイムスタンプが時計と一致しなかったことに気づきました。このエラーの理由は何ですか？

A. システム時計が夏時間に正しく設定されていません。

B. NTPサーバーでの認証エラーにより、タイムスタンプが正しくありません。

- C. キーワードlocaltimeがtimestampserviceコマンドで定義されていません。
- D. NTPサーバーは別のタイムゾーンにあります。

Answer: B ([メッセージを残す](#))

最新問題: 160

BFDを使用する利点は何ですか？

- A. レイヤ1でローカルリンク障害を検出し、ルーティングテーブルを更新します。
- B. レイヤ3でローカルリンク障害を検出し、ルーティングプロトコルを更新します。
- C. レイヤ1およびレイヤ3の問題に対して1秒未満の障害検出があります。
- D. レイヤ1およびレイヤ2の問題に対して1秒未満の障害検出があります。

Answer: (解答を表示する)

セクション: 混合質問

最新問題: 161

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
```

ユーザーから、DHCPサーバーからIPアドレスを取得できないとの報告がありました。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2時間を超えてアクティブになっているユーザーはいません。現在のリソース内の問題を修正するアクションはどれですか？

- A. DHCPリース時間を小さい値に設定します
- B. network192.168.2.0255.255.255.0コマンドをDHCPプールに追加します
- C. DHCPリース時間をより大きな値に設定します
- D. サブネットマスクをDHCPプールのnetwork192.168.1.0255.255.254.0コマンドに変更します

Answer: A ([メッセージを残す](#))

最新問題: 162

MPLSレイヤ3VPNの2つの機能は何ですか。(2つ選択してください。)

- A. LDPとBGPは疑似配線シグナリングに使用できます。
- B. 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。
- C. BGPは、PEノード間のカスタマーVPNv4ルートのシグナリングに使用されます。
- D. ノードセグメントIDの packets は、宛先への最短パスとともに転送されます。
- E. MPLSネットワークで転送される場合、カスタマートラフィックはVPNラベルにカプセル化されます。

Answer: (解答を表示する)

MPLS Layer-3 VPNは、CEサイト間のIP接続を提供します* MPLS VPNは、フルメッシュ、ハブアンドスポーク、およびハイブリッドIP接続を可能にします* CEサイトは、PE-CEリンクを介したIPピアリングを介してMPLSネットワークに接続します* MPLS Layer-3 VPNは、PEエッジノードのVRFを介して実装されます*顧客ルーティングと転送セグメンテーションを提供するVRF * PEノード間の顧客VPN (VPNv4) ルートのシグナリングに使用されるBGP *トラフィックの分離を確実にするために、顧客トラフィックはMPLSで転送されるときに追加のVPNラベルにカプセル化されますネットワーク*主要なアプリケーションは、レイヤー3ビジネスVPNサービス、エンタープライズネットワークセグメンテーション、およびセグメント化されたレイヤー3データセンターアクセスです。

最新問題: 163

パケットタイプ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。

data plane packets	user-generated packets that are always forwarded by network devices to other end-station devices
control plane packets	network device generated or received packets that are used for the creation of the network itself
management plane packets	network device generated or received packets; packets that are used to operate the network
services plane packets	user-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than the normal traffic by the network devices

Answer:

data plane packets	data plane packets
control plane packets	control plane packets
management plane packets	management plane packets
services plane packets	services plane packets

最新問題: 164

展示を参照してください。

```

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

```

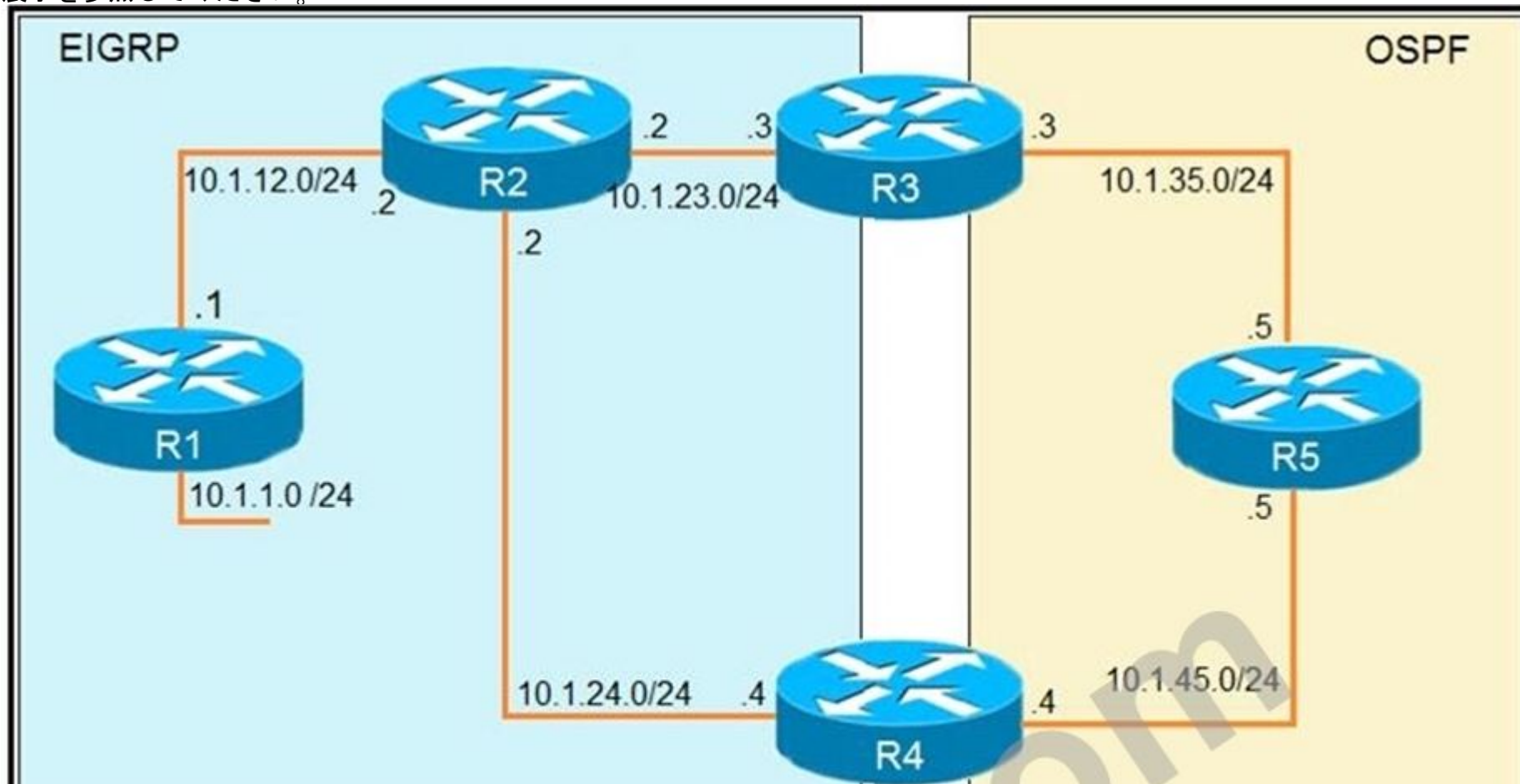
この構成を適用した結果はどうなりますか？

- A. ルータは、BGP」という名前のアクセスリストと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。
- B. ルータは他のデバイスとBGPネイバーシップを形成できません。
- C. ルーターは他のデバイスとBGPネイバーシップを形成できます。
- D. ルーターは、BGP」という名前のアクセスリストと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: ([解答を表示する](#))

最新問題: 165

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
 0 10.1.23.2 108 msec 76 msec 80 msec
 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 truncated>
```

R5からのトレースルートの出力は、ネットワーク内のループを示しています。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)

```
R2
outer ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG

oute-map SET-TAG permit 10
 set tag 1

R4
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: ([解答を表示する](#))

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、OSPF再配布ステートメントでは、BWメトリックの値が高く、遅延の値が1であるためです。したがって、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、ループを引き起こします。これで、R5はR3から10.1.1.0/24を学習し、R4がEIGRPに再配布するのと同じルートがR4にアドバタイズされます。R3がOSPFでEIGRPを再配布するときにタグ1を設定し、R4が再配布中にタグ1ですべてのOSPFルートを拒否した場合、R3は10.1.1.0/24を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: 166

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
```

FastEthernet0 / 1がダウンすると、192.168.253.2を介した172.29.0.0/16へのルートがRIBにインストールされません。問題を解決するアクションはどれですか？

- A. 報告された距離よりも大きい実行可能距離を構成します
- B. 後続の実行可能距離よりも大きい実行可能距離を構成します。
- C. 報告された距離を後継者の実行可能な距離よりも大きく設定します。
- D. 実行可能距離よりも大きい報告距離を構成します

Answer: A ([メッセージを残す](#))

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 167

展示品をご覧ください。

```
R3#show policy-map control-plane
Control Plane

Service-policy output: R3_CoPP

Class-map: mgmt (match-all)
 361 packets, 73858 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: access-group 120
 police:
  cir 8000 bps, bc 1500 bytes, be 1500 bytes
  conformed 8 packets, 1506 bytes; actions:
  transmit
  exceeded 353 packets, 72352 bytes; actions:
  drop
  violated 0 packets, 0 bytes; actions:
  drop
  conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map: class-default (match-any)
 124 packets, 10635 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: any
R3#show access-lists 120
Extended IP access list 120
 10 permit udp any any eq snmptrap (361 matches)
```

SNMPトラップパケットで観察された断続的な接続を解決するアクションはどれですか？

- A. TCPトラフィックに一致する新しいクラスマップを追加します
- B. 管理クラスマップのCIRを増やします
- C. ACL 120に新しいエントリを1つ追加して、UDPポート161を許可します。
- D. 管理クラスマップのコミットされたバーストサイズを減らします

Answer: C ([メッセージを残す](#))

最新問題: 168

展示を参照してください。

```

R1#show policy-map control-plane
Control Plane

Service-policy output: CoPP

Class-map: SNMP-Out (match-all)
 124 packets, 3693 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name SNMP
police:
  cir 8000 bps, bc 1500 bytes
  conformed 0 packets, 0 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    drop
  conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
 10 packets, 1003 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any

R1#show ip access-list SNMP
Extended IP access list SNMP
 10 permit udp any eq snmp any

```

R1はSNMPを使用して監視されており、監視デバイスは部分的な情報のみを取得しています。この問題を解決するには、どのようなアクションを取る必要がありますか？

- A. CoPPポリシーを変更して、SNMPに構成されているCIR制限を増やします。
- B. CoPPポリシーを変更して、SNMPの構成済み超過制限を増やします。
- C. snmptrapを含めるようにアクセスリストを変更します。
- D. アクセスリストを変更して2行目を追加し、udp any anyeqsnmpを許可します

Answer: ([解答を表示する](#))

最新問題: 169

エンジニアは、ルートに影響を与えるポリシーでアクセスリストNON-CISCOを設定しました

```

route-map PBR, deny, sequence 5
Match clauses:
 ip address (access-list): NON-CISCO
Set clauses:
Policy routing matches: 0 packets, 0 bytes
route-map PBR, permit, sequence 10
Match clauses:
Set clauses:
 ip next-hop 192.168.1.5
Policy routing matches: 388213827 packets, 222009685077 bytes

```

このルートマップ設定の2つの効果は何ですか？ (2つ選択してください。)

- 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ルックアップ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 (メッセージを残す)

<https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds-ce.html>

最新問題: 170

展示を参照してください。

```
access-list 100 deny tcp any any eq 465
access-list 100 deny tcp any eq 465 any
access-list 100 permit tcp any any eq 80
access-list 100 permit tcp any eq 80 any
access-list 100 permit udp any any eq 443
access-list 100 permit udp any eq 443 any
```

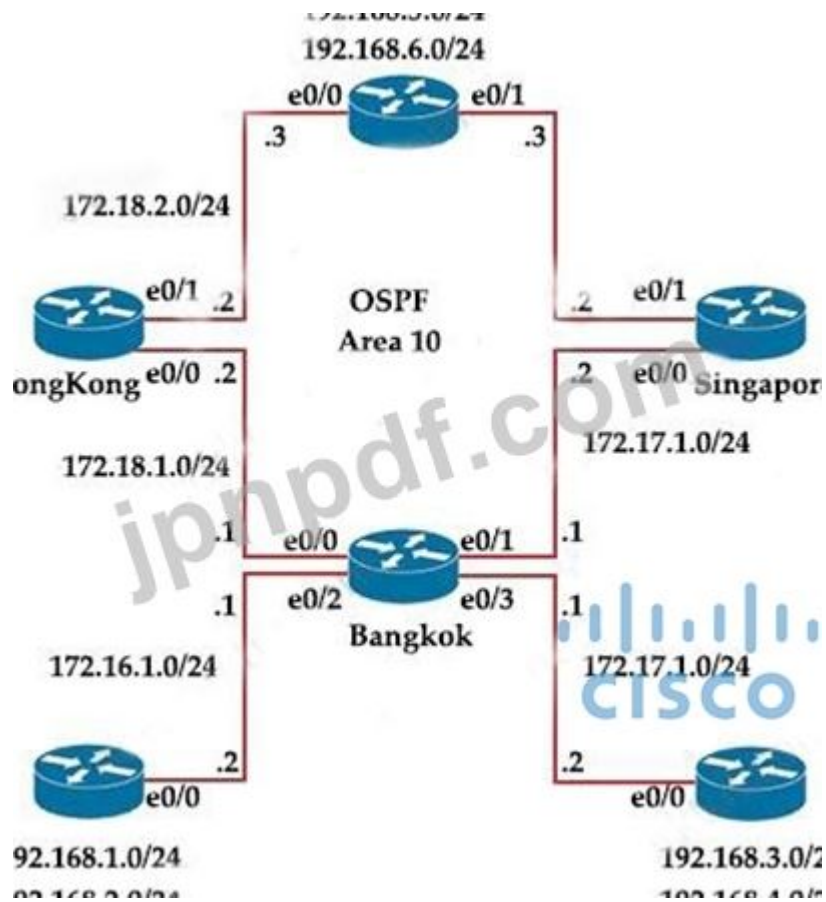
トラブルシューティング中に、安全なWebブラウザを使用してデバイスにアクセスできないことが判明しました。問題を解決するには何が必要ですか？

- A. tcpポート443を許可する
- B. udpポート465を許可する
- C. tcpポート22を許可する
- D. tcpポート465を許可する

Answer: A (メッセージを残す)

最新問題: 171

示す：



バンコクはECMPを使用して192.168.5.0/24ネットワークに到達しています。管理者は、192.168.3.0/24および192.168.4.0/24ネットワークからのTelnetトラフィックが香港ルーターを優先ルーターとして使用するようにバンコクを構成する必要があります。このタスクを実行する構成のセットはどれですか？

A. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255

!

ルートマップPBR1許可10

IPアドレス101に一致

set ip next-hop 172.18.1.2

インターフェイスEthernet0/3

ip policy route-map PBR1

B. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23 access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23

!

ルートマップPBR1許可10

IPアドレス101に一致

set ip next-hop 172.18.1.2

インターフェイスEthernet0/1

ip policy route-map PBR1

C. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23 access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23

!

ルートマップPBR1許可10

IPアドレス101に一致

```
set ip next-hop 172.18.1.2
```

！

インターフェイスEthernet0/3

```
ip policy route-map PBR1
```

```
D. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
```

！

ルートマップPBR1許可10

IPアドレス101に一致

```
set ip next-hop 172.18.1.2
```

！

インターフェイスEthernet0/1

```
ip policy route-map PBR1
```

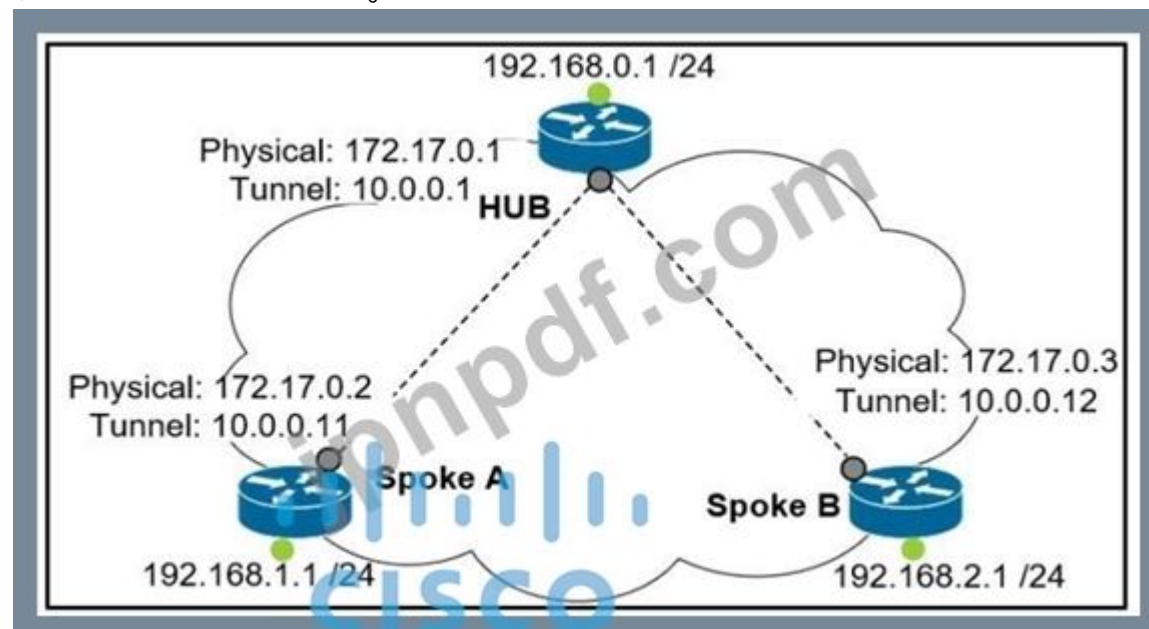
Answer: C (メッセージを残す)

ここバンコクのルーターでポリシーベースルーティング (PBR) を使用して、192.168.3.0 /24と192.168.4.0/24からのトラフィックを照合し、「set ipnext-hop」を香港のルーター (この場合は172.18.1.2) に送信する必要があります。

注 :192.168.3.0 /24および192.168.4.0/24からのトラフィックを受信するには、着信インターフェイスe0/3にPBRを適用する必要があることに注意してください。

最新問題: 172

展示を参照してください。



スポークBルーターとのダイナミックDMVPNトンネルを有効にするには、スポークAルーター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。

interface Tunnel0
description mGRE – DMVPN Tunnel
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel destination FastEthernet 0/0
tunnel mode gre multipoint

interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source FastEthernet 0/0
tunnel mode gre multipoint
ip nhrp nhs 10.0.0.1
in nhrn map 10 0 0 1 172 17 0 1

C. interface Tunnel0
ip address 10.1.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source 1.1.1.10
ip nhrp map 10.0.0.11 172.17.0.2
tunnel mode gre

D. interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast static
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode gre multipoint

A. オプションA

B. オプションB

C. オプションC

D. オプションD

Answer: ([解答を表示する](#))

最新問題: 173

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、ISP2に切り替えるのではなく、2つのISP間で接続がフラッピングしていることに気づきました。問題を解決するアクションはどれですか？

- 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を経由するデフォルトルートで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ルートの管理距離に一致するようにしきい値を変更します。

Answer: A (メッセージを残す)

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

最新問題: 174

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, deny, 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#

```

サーバーにアクセスするには、どの2つのアクションを実行する必要がありますか？ (2つ選択してください。)

- A. ルートマップにシーケンス20を追加して、アクセスリスト1を許可します。

- B. アクセスリストを変更して、192.168.2.2へのルートを拒否します。
- C. 管理距離がOSPFよりも大きい192.168.2.2に到達するためのフローティング静的ルートを追加します
- D. アクセスリストを変更して、permit ip anyの2行目を追加します
- E. 192.168.2.2へのルートを許可するように配布リストseq10を変更します。

Answer: B,C (メッセージを残す)

最新問題: 175

MPLSVPN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。

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

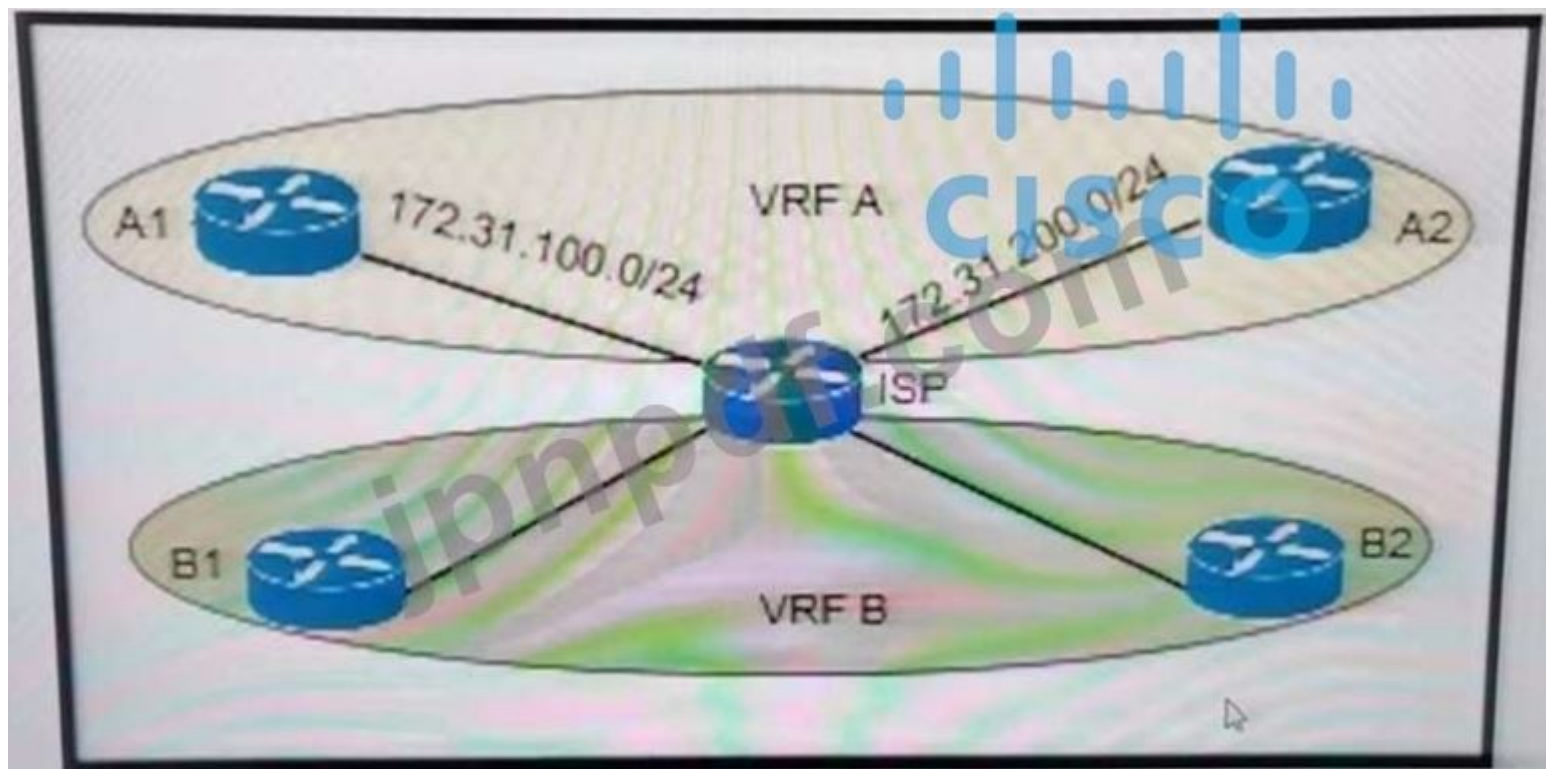
Answer:

Customer (C) device	Customer (C) device that switches MPLS packets
CE device	Provider (P) device
PE device	PE device
Provider (P) device	CE device

最新問題: 176

展示を参照してください。

ISPルーターは、VRF-Lite機能を使用して、カスタマーAとカスタマーB用に完全に構成されています。カスタマー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

インターフェイスfa0/0

説明To->ISP

```
ip add 172.31.100.1 255.255.255.0
```

シャットなし

!

```
router ospf 100
```

```
ネット172.31.100.10.0.0.255エリア0
```

A2

インターフェイスfa0/0

説明To->ISP

```
ip add 172.31.200.1 255.255.255.0
```

シャットなし

!

```
router ospf 100
```

```
ネット172.31.200.10.0.0.255エリア0
```

B. A1

インターフェイスfa0/0

説明To->ISP

ipvrf転送A

```
ip add 172.31.100.1 255.255.255.0
```

シャットなし

!

```
router ospf 100
```

```
ネット172.31.100.10.0.0.255エリア0
```

A2

インターフェイスfa0/0

説明To->ISP

ipvrfr転送A

ip add 172.31.200.1 255.255.255.0

シャットなし

!

router ospf 100

ネット172.31.200.10.0.0.255エリア0

C. A1

インターフェイスfa0/0

説明To->ISP

ip add 172.31.200.1 255.255.255.0

シャットなし

!

router ospf 100

ネット172.31.200.10.0.0.255エリア0

A2

インターフェイスfa0/0

説明To->ISP

ip add 172.31.100.1 255.255.255.0

シャットなし

!

router ospf 100

ネット172.31.100.10.0.0.255エリア0

D. A1

インターフェイスfa0/0

説明To->ISP

ipvrfr転送A

ip add 172.31.100.1 255.255.255.0

シャットなし

!

router ospf 100 vrf A

ネット172.31.200.10.0.0.255エリア0

A2

インターフェイスfa0/0

説明To->ISP

ipvrfr転送A

ip add 172.31.100.1 255.255.255.0

シャットなし

!

```
router ospf 100 vrf A
```

```
ネット172.31.200.10.0.0.255エリア0
```

Answer: ([解答を表示する](#))

説明

A1およびA2ルーターは、それらがVRFAに属していることを認識していません。

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、次のように構成する必要があります (一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 :

```
インターフェイスg0/0
```

```
説明ISP->To_CustomerA
```

```
ip vrf 転送A
```

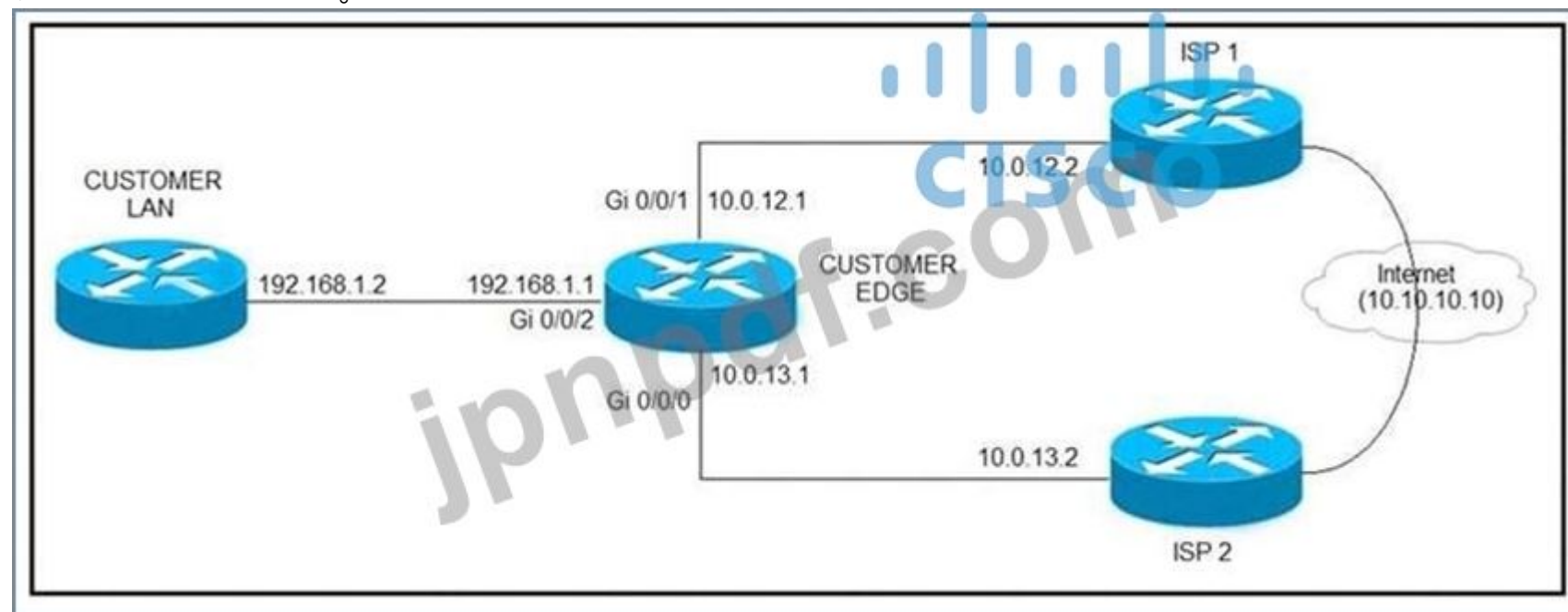
```
IPアドレス172.31.100.2255.255.255.0
```

```
router ospf 100 vrf A
```

```
ネットワーク172.31.200.20.0.0.255エリア0
```

最新問題: 177

展示を参照してください。



ISP1とISP2はインターネットに直接接続します。顧客は冗長性を実現するために両方のISPリンクを追跡しており、ルータコンソールにCisco IOSIPSLA追跡出力を表示できません。IP SLA設定に欠落しているコマンドはどれですか？

- A. 今すぐ開始時間
- B. すぐに開始時刻
- C. 開始時刻00:00
- D. 開始時刻0

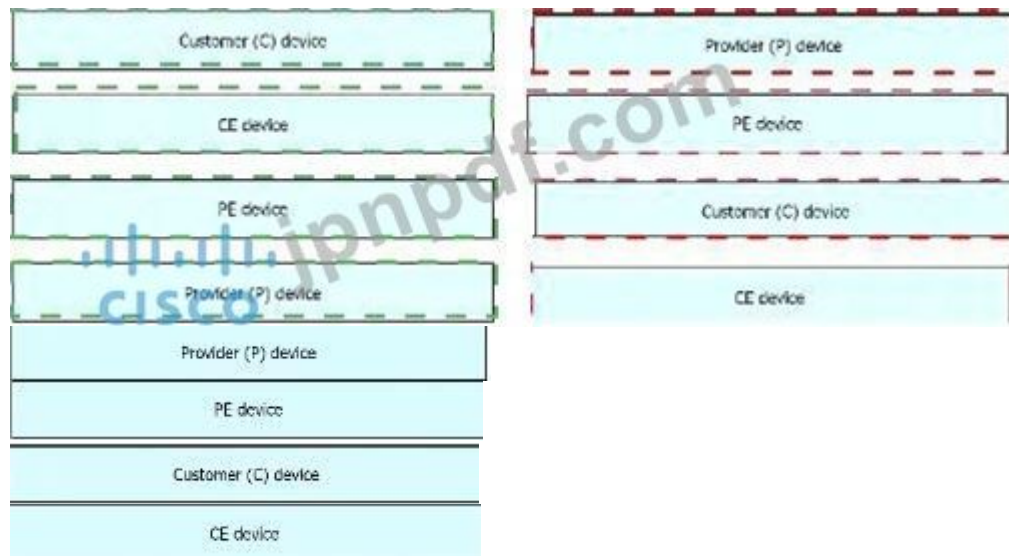
Answer: ([解答を表示する](#))

最新問題: 178

MPLSVPNデバイスタイプを左から右の定義にドラッグアンドドロップします。

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:



最新問題: 179

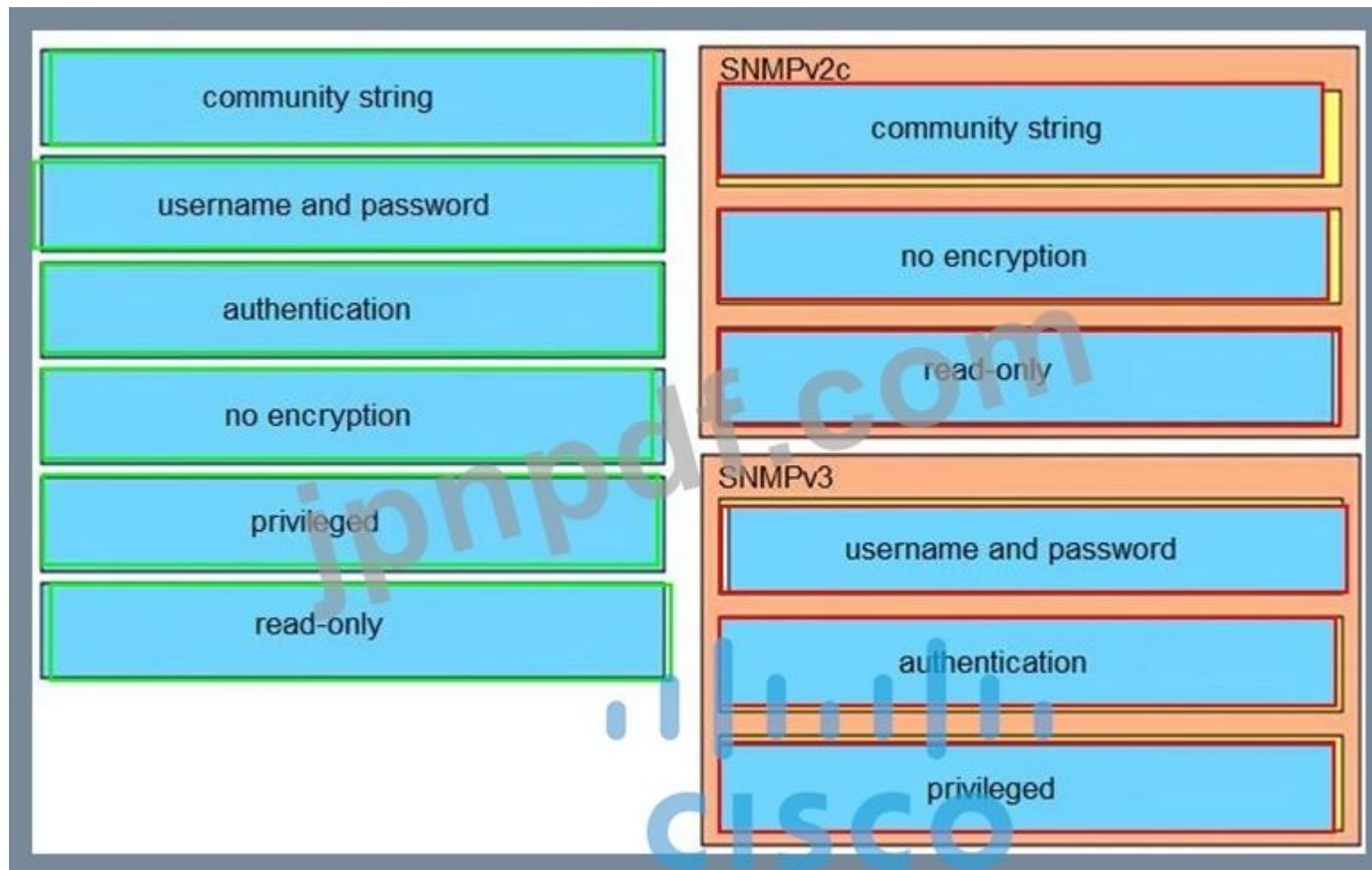
Cisco IOSデバイスのSNMP属性を左側から、右側の正しいSNMPv2cまたはSNMPV3カテゴリにドラッグアンドドロップします。

community string
username and password
authentication
no encryption
privileged
read-only

SNMPv2c

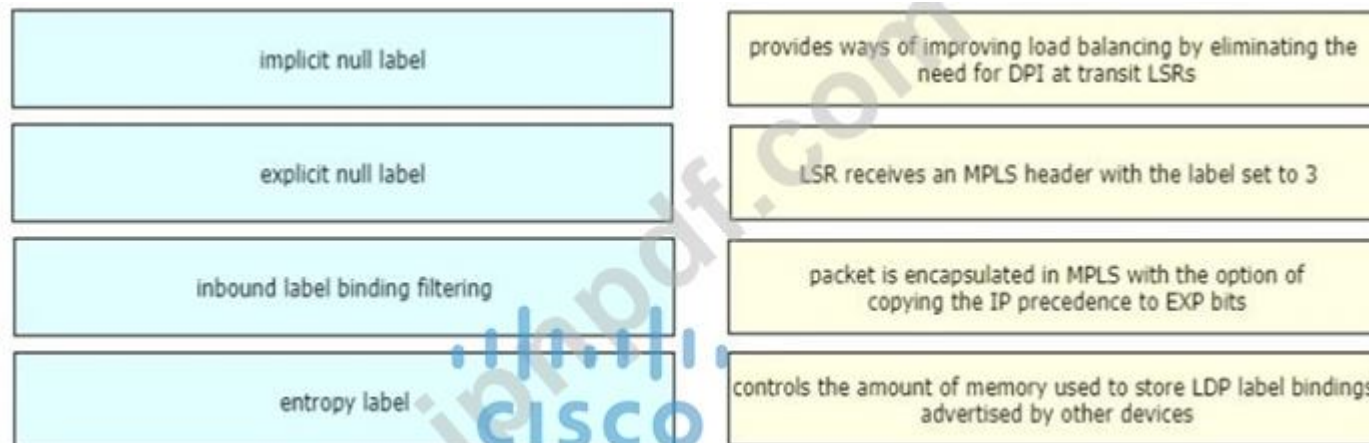
SNMPv3

Answer:



最新問題: 180

LDP機能を左から右の説明にドラッグアンドドロップします



Answer:



最新問題: 181

展示を参照してください。

R200#show ip bgp summary

BGP router identifier 10.1.1.1, local AS number 65000

BGP table version is 26, main routing table version 26

1 network entries using 132 bytes of memory

1 path entries using 52 bytes of memory

2/1 BGP path/bestpath attribute entries using 296 bytes of memory

0 BGP route-map cache entries using 0 bytes of memory

0 BGP filter-list cache entries using 0 bytes of memory

Bitfield cache entries: current 1 (at peak 2) using 28 bytes of memory

BGP using 508 total bytes of memory

BGP activity 24/23 prefixes, 24/23 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.0.2.2	4	65100	20335	20329	0	0	0	00:02:04	Idle (PfxCt)

R200#

どのような状況でBGPネイバーはアイドル状態のままになりますか？

- A. インバウンド方向にプレフィックスリストが適用されている場合
- B. プレフィックスが上限を超えた場合
- C. プレフィックスがBGPピアから受信されない場合
- D. プレフィックスが上限に達した場合

Answer: B (メッセージを残す)

有効な 300-410 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の 300-410 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (80030%OFF問題集溶と正解付きで 30%w特別割引コード:

Freepdfdumps)

最新問題: 182

MPLSネットワークのルート識別子に関する説明のうち正しいものはどれですか。

- A. ルート識別子を使用すると、ルーティングテーブルの複数のインスタンスをエッジルーター内に共存させることができます。
- B. ルート識別子はラベルのバインドに使用されます。
- C. ルート識別子は、MPLSネットワーク全体で一意的なVPNv4アドレスを作成します。
- D. ルート識別子は、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プレフィックスを定義します。

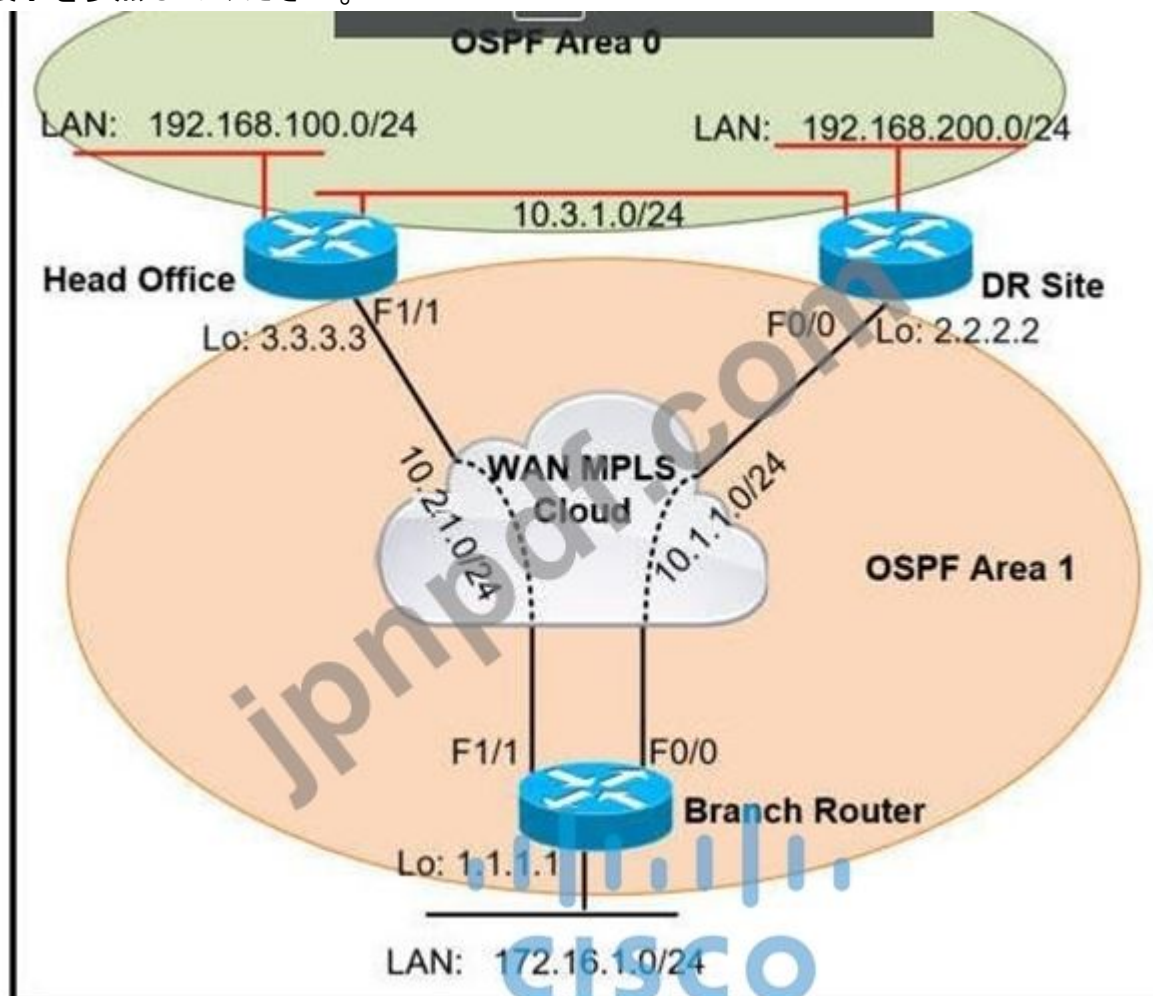
Answer: C ([メッセージを残す](#))

セクション :VPNテクノロジー

説明/参照 :

最新問題: 183

展示を参照してください。



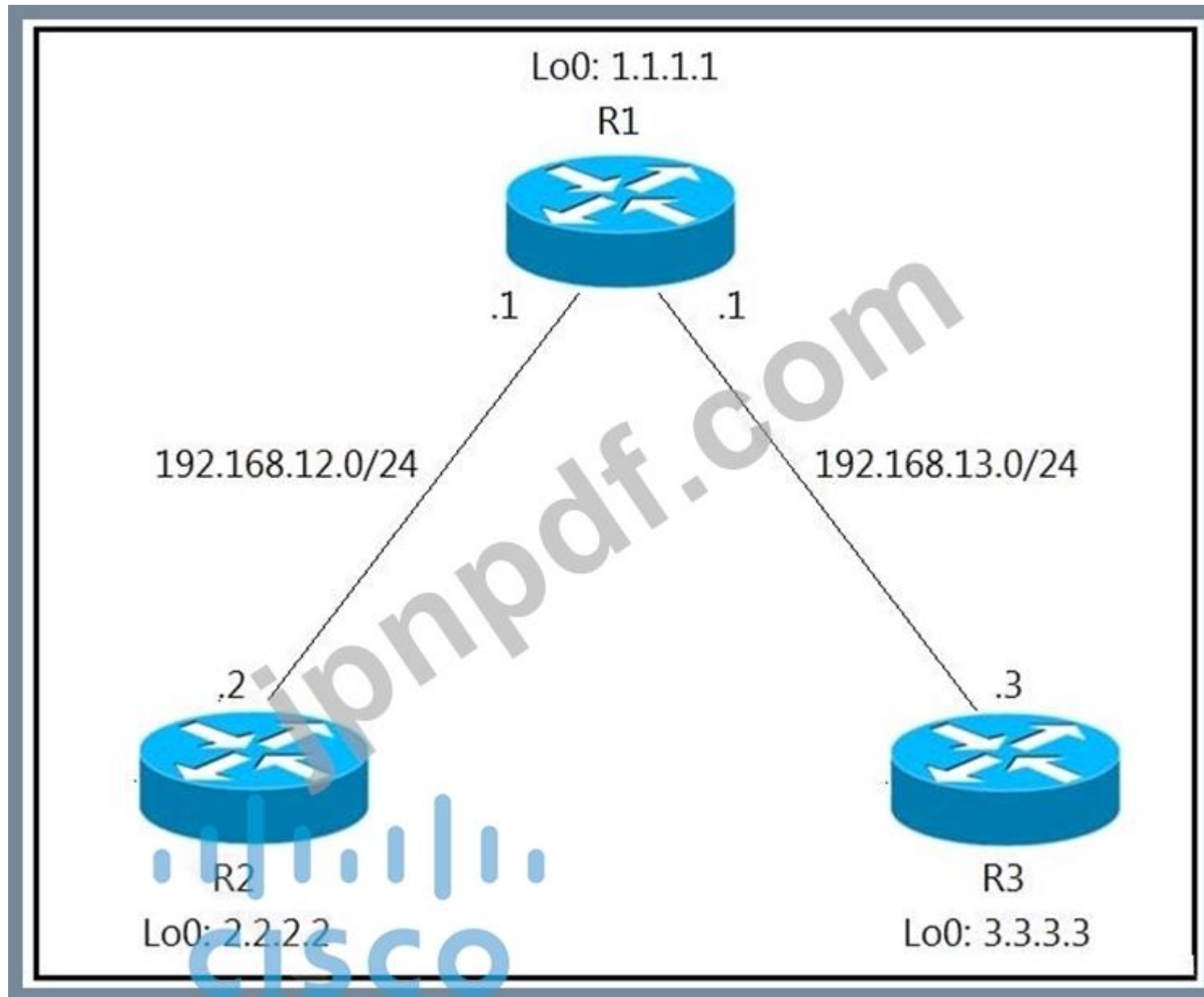
ネットワーク管理者は、ブランチルータのコンソールログを確認して、DRルータとのOSPF隣接関係の問題のトラブルシューティングを行います。この問題を解決するアクションはどれですか？

- A. DRサイトのサブネットに一致するブランチWANインターフェースをアドバタイズします。
- B. DRサイトのフラッピングリンクを安定させて、OSPF隣接関係を確立します。
- C. サイト間で一致するhello間隔とdead間隔を構成します。
- D. 関連するOSPFエリアのDRサイトのWANインターフェースを設定します。

Answer: ([解答を表示する](#)**)**

最新問題: 184

展示を参照してください。



エンジニアが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. R1にR2ループバックアドレスの静的ルートを追加し、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R1のリークマップを使用し、それを配布リストコマンドでR3に適用します。
- C. 必要なプレフィックスと一致するR3のリークマップを使用し、EIGRPスタブ機能を適用します。
- D. R1にR2ループバックアドレスの静的なルートを追加し、それを再配布してR3にアドバタイズします。

Answer: B (メッセージを残す)

EIGRPスタブ機能は、不要なEIGRPクエリを防止し、アドバタイズする一部のルートをフィルタリングするのに役立ちます。ルータをスタブルータとして構成したいが、アドバタイズする一部のルートに例外を設けたい場合はどうなりますか？これは、リークマップ機能で可能です。この質問でリークマップを設定する方法は次のとおりです。

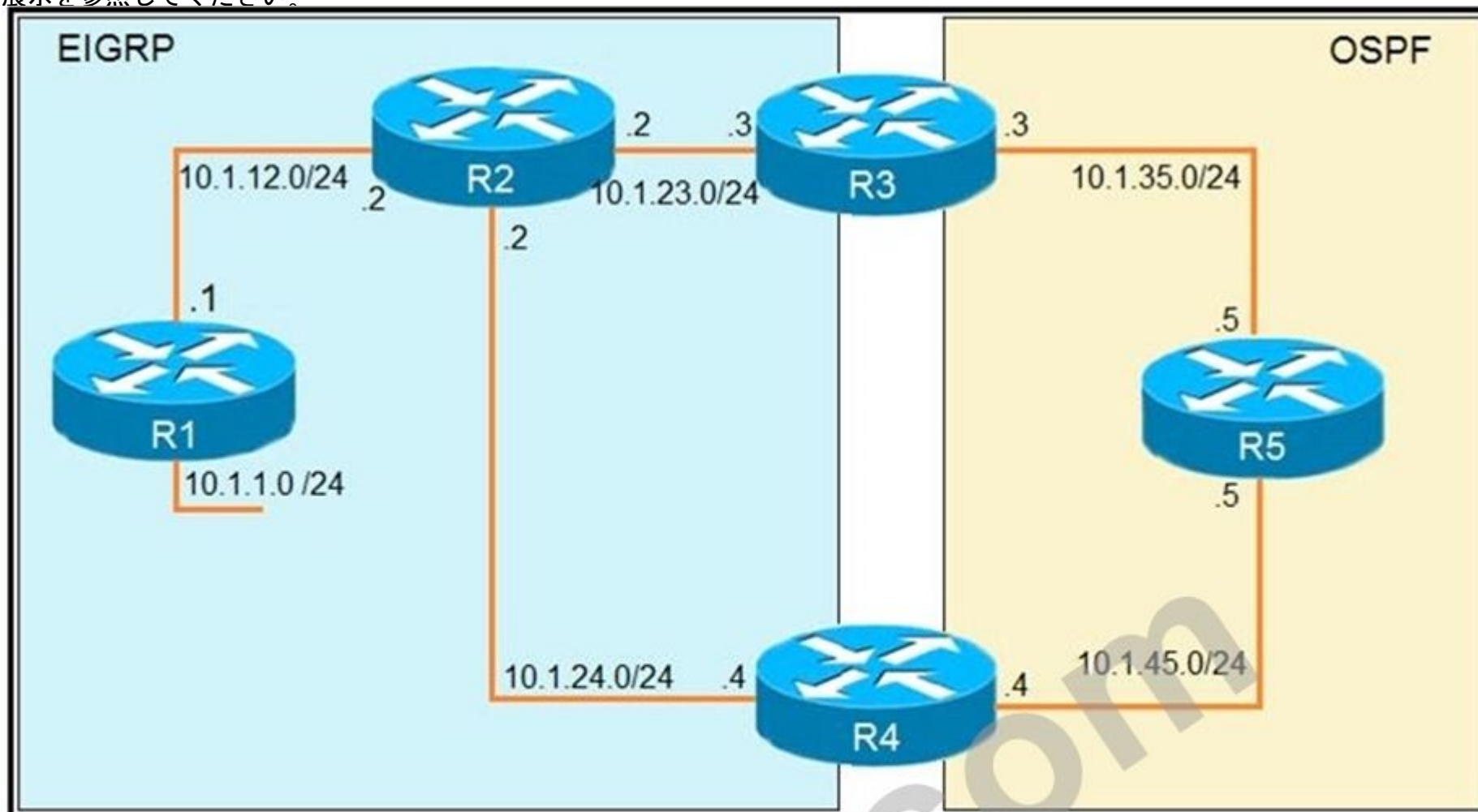
```
R1
R1 (config-std-nacl)#permit host 2.2.2.2
R1 (config)#ip access-list standard R2_L0
R1 (config)#route-map R2_L0_LEAK
R2 (config-route-map)#match ip address R2_L0
```

R1 (config)#router eigrp 1

R1 (config-router)#eigrpスタブリークマップR2_L0_LEAK

最新問題: 185

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 truncated>
```

R5からのトレースルートの出力は、ネットワーク内のループを示しています。このループを防ぐ構成はどれですか？

A)

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

```
route-map SET-TAG permit 10
 set tag 1
```

B)

```
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)

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

oute-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

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D
- B. オプションA
- C. オプションB
- D. オプションC

Answer: ([解答を表示する](#))

最新問題: 186

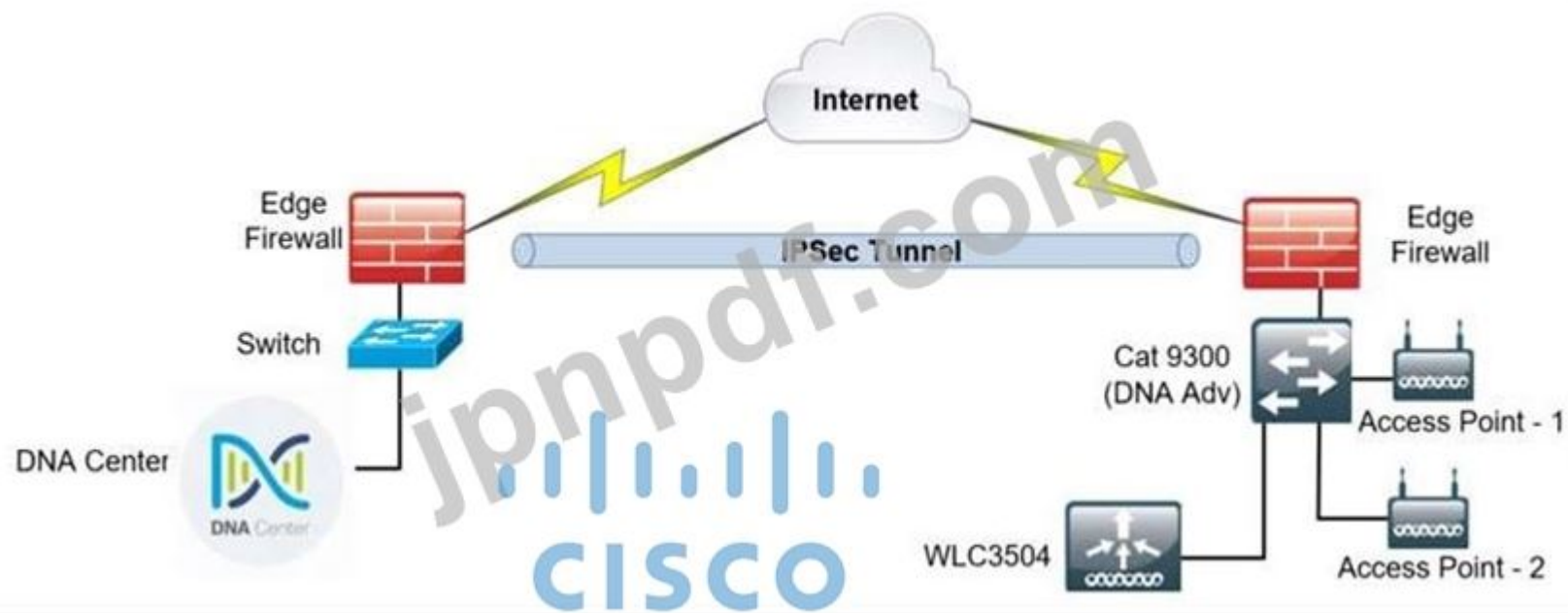
VRFインスタンスの2つの特徴は何ですか？ (2つ選択してください。)

- A. Pデバイスに接続されたカスタマーサイトのVPNメンバーシップによって定義されます。
- B. 各VRFには、異なるルーティングテーブルとCEFテーブルのセットがあります
- C. 顧客サイトをさまざまなVRFに関連付けることができます
- D. インターフェイスは1つのVRFに関連付けられている必要があります。
- E. すべてのVRFは、顧客のルーティングテーブルとCEFテーブルを共有します。

Answer: ([解答を表示する](#))

最新問題: 187

展示を参照してください。



ネットワーク管理者は、CiscoDNACenterでCiscoCatalyst9300とCiscoWLC3504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、WLCに[エラー"uncontactable"が表示されます。Cisco DNACenter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、WLC3504にアップロードします。
- B. Cisco DNACenterからWLC3504を削除し、CiscoDNACenterに再度追加します。
- C. Catalyst9300に接続されたデバイスの階層の下にWLC3504を追加します。
- D. USB上のCisco DNA Centerから.pernファイルをコピーし、WLC3504にアップロードします。

Answer: ([解答を表示する](#))

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html#anc12>

最新問題: 188

IPv6 ND検査について正しい説明はどれですか？

- A. レイヤー3ネイバーテーブル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て保護します。
- B. レイヤ2ネイバーテーブルのステートレス自動設定アドレスのバインディングを学習して保護します。
- C. レイヤ3ネイバーテーブルのステートフル自動設定アドレスのバインディングを学習して保護します。
- D. レイヤ2ネイバーテーブルのステートフル自動設定アドレスのバインディングを学習して保護します。

Answer: ([解答を表示する](#))

IPv6 NDインスペクションは、レイヤー2ネイバーテーブル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て保護します。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-to-MACマッピングが検証可能である場合、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、近隣キャッシュへの攻撃など、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: 189

展示を参照してください。

```
interface loopback0
ip address 4.4.4.4 255.255.255.0
|
interface FastEthernet1/0
Description **** WAN link ****
ip address 10.0.0.1 255.255.255.0
|
interface FastEthernet1/1
Description **** LAN Network ****
ip address 192.168.1.1 255.255.255.0
|
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
network 4.4.4.0 0.0.0.0 area 0
network 10.0.0.1 0.0.0.0 area 0
network 192.168.1.1 0.0.0.0 area 10
|
```

到達可能性をloopback0に復元するコマンドのセットはどれですか？

A)

```
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network point-to-point
```

B)

```
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network broadcast
```

C)

```
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf interface area 10
interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf interface type network
```

A. オプションA

B. オプションC

C. オプションD

D. オプションB

Answer: A (メッセージを残す)

最新問題: 190

ラボシミュレーション

これらの目標を達成するために、トポロジに従って顧客ごとに個別のVRFを構成します。



R1

```
R1 R2 SW1 SW2 SW3 SW4
R1>
R1> CHINESEDUMPS
R1> 通过测试
R1>
R1>
R1>en
R1#sh run
Building configuration...

Current configuration : 1357 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
CHINESEDUMPS
no aaa new-model
通过测试
!
```

```
R1 R2 SW1 SW2 SW3 SW4
CHINESEDUMPS
通过测试

!
ip vrf cu-green
rd 65000:200
!
ip vrf cu-red
rd 65000:10
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
CHINESEDUMPS
通过测试
CISCO
```

R1

R2

SW1

SW2

SW3

SW4

CHINESEDUMPS

通过测试

```
interface Loopback0
 ip address 10.10.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.1.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.20.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 duplex auto
!
interface Ethernet0/2.100
 encapsulation dot1Q 100
 ip address 10.10.10.1 255.255.255.255
!
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.1 255.255.255.255
```



jpnpdf.com

CHINESEDUMPS

通过测试



CISCO

```
R1 R2 SW1 SW2 SW3 SW4
interface Ethernet0/2.200
encapsulation dot1q 200
ip address 10.10.20.1 255.255.255.252
!
interface Ethernet0/3
no ip address
shutdown
duplex auto
!
router bgp 65000
bgp log-neighbor-changes
no bgp default ipv4-unicast
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
control-plane
!
```

R2

R1

R2

SW1

SW2

SW3

SW4

R2>en

R2#Show run

Building configuration...

Current configuration : 1353 bytes

version 15.8

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

!

!

no aaa new-model

!

!

!

clock timezone PST -8 0

mmi polling-interval 60

no mmi auto-configure

R1

R2

SW1

SW2

SW3

SW4

CHINESEDUMPS

通过测试



```
ip vrf cu-green
rd 65000:200
```

```
ip vrf cu-red
rd 65000:100
```

```
no ip domain lookup
```

```
ip cef
```

```
no ipv6 cef
```

```
!
multilink bundle-name authenticated
```

CHINESEDUMPS

通过测试

jpnpdf.com

R1 R2 SW1 SW2 SW3 SW4

```
! CHINESEDUMPS
! interface Loopback0
! ip address 10.10.2.2 255.255.255.255
!
! interface Ethernet0/0
! ip address 192.168.2.254 255.255.255.0
! duplex auto
!
! interface Ethernet0/1
! ip address 192.168.2.254 255.255.255.0
! duplex auto
!
! interface Ethernet0/2
! no ip address
! duplex auto
!
! interface Ethernet0/2.100
! encapsulation dot1Q 100
! ip address 10.10.10.2 255.255.255.252
!
! CHINESEDUMPS
! interface Ethernet0/2.200
! encapsulation dot1Q 200
! ip address 10.10.20.2 255.255.255.252
```

```
R1  R2  SW1  SW2  SW3  SW4
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.2 255.255.255.252
 !
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
 !
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 !
ip forward-protocol nd
 !
 !
no ip http server
no ip http secure-server
 !
ipv6 ioam timestamp
 !
control-plane
 !
 !
```

SW1

```
R1 R2 SW1 SW2 SW3 SW4
SW1>en
SW1#sh run
Building configuration...

Current configuration : 942 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
!
CHINESEDUMPS
no aaa new-model
clock timezone PST -8 0
!
```

```
R1 R2 SW1 SW2 SW3 SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
!
interface Ethernet0/0
no switchport
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
```


R1 R2 SW1 SW2 SW3 SW4

```
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Ethernet0/0
!
interface Ethernet0/1
no switchport
ip address 192.168.22.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
```

通过测试

通过测试

通过测试

```
R1  R2  SW1  SW2  SW3  SW4
!
interface Ethernet0/1
no switchport
ip address 192.168.22.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.22.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
CHINESEDUMPS
!
control-plane
!
```

SW3

R1 R2 SW1 SW2 SW3 SW4

```
SW3>
SW3>en
SW3#show run
Building configuration...

Current configuration : 942 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
clock timezone PST -8 0
```



CHINESEDUMPS
通过测试
jppnpdf.com

```
R1  R2  SW1  SW2  SW3  SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Ethernet0/0
no switchport
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
```

```
R1  R2  SW1  SW2  SW3  SW4
no switchport
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward protocol nd
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
control-plane
!
```

```
R1  R2  SW1  SW2  SW3  SW4
SW4>en
SW4#show run
Building configuration...

Current configuration : 944 bytes
!
! Last configuration change at 04:13:09 ST Sat May 7 2022
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW4
!
boot-start-marker
boot-end-marker
!
!
CHINESEDUMPS
no add new-model
clock timezone PST -8 0
!
```

```
R1  R2  SW1  SW2  SW3  SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Ethernet0/0
!
interface Ethernet0/1
no switchport
ip address 192.168.20.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
```


インターフェイスEthernet0/0

ip vrf forwardingcu-red

IPアドレス192.168.1.254255.255.255.0

SW1への到達可能性を確認します。

R1#ping vrf cu-red 192.168.1.1

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.2.1に送信し、タイムアウトは2秒です。

!!!!

成功率は100% 5/5)、往復の最小/平均/最大= 1/1/1 ms

R2の場合：

インターフェイスEthernet0/0

ip vrf forwardingcu-red

IPアドレス192.168.2.254255.255.255.0

SW3への到達可能性を確認します。

R2#ping vrf cu-red 192.168.2.1

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.1.1に送信し、タイムアウトは2秒です。

!!!!

SW2とSW4にはvrfcu-greenを使用します。

R1の場合：

インターフェイスEthernet0/1

ip vrf forwardingcu-green

IPアドレス192.168.20.254255.255.255.0

SW2への到達可能性をテストします。

R1#ping vrf cu-green 192.168.20.1

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.22.1に送信し、タイムアウトは2秒です。

!!!!

成功率は100% 5/5)、往復の最小/平均/最大= 1/1/1 ms

R2の場合：

インターフェイスEthernet0/1

ip vrf forwardingcu-green

IPアドレス192.168.22.254255.255.255.0

SW4への到達可能性をテストします。

R2#ping vrf cu-green 192.168.22.1

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.20.1に送信し、タイムアウトは2秒です。

!!!!

成功率は100% 5/5)、往復の最小/平均/最大= 1/1/1 ms

R1の場合：

インターフェイスEthernet0/2.100

mpls ip

!

インターフェイスEthernet0/2.200

mpls ip

!

BGPの構成 :

ルーターbgp65000

ネイバー10.10.10.2リモート-65000として

ネイバー10.10.20.2リモート-65000として

!

アドレスファミリvpngv4

ネイバー10.10.10.2アクティベート

ネイバー10.10.20.2アクティベート

exit-address-family

!

アドレスファミリipv4vrfcu-green

接続された再配布

exit-address-family

!

アドレスファミリipv4vrfcu-red

接続された再配布

exit-address-family

!

R1 (config)#ip vrf cu-red

R1 (config-vrf) #oute-target both 65000 :100

!

R1 (config)#ip vrf cu-green

R1 (config-vrf) #oute-target both 65000 :200

R2の場合 :

インターフェイスEthernet0/2.100

mpls ip

!

インターフェイスEthernet0/2.200

mpls ip

!

ルーターbgp65000

ネイバー10.10.10.1リモート-65000として

ネイバー10.10.20.1リモート-65000として

!

アドレスファミリvpngv4

ネイバー10.10.10.1アクティベート

ネイバー10.10.20.1アクティベート

exit-address-family

!

アドレスファミリipv4vrfcu-green

接続された再配布

exit-address-family

!

アドレスファミリipv4vrfcu-red

接続された再配布

exit-address-family

R2 (config)#ip vrf cu-red

R2 (config-vrf) #oute-target both 65000 :100

!

R2 (config)#ip vrf cu-green

R2 (config-vrf) #oute-target both 65000 :200

検証:

SW1からSW3へ:

SW1#ping 192.168.1.1

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.1.1に送信し、タイムアウトは2秒です。

!!!!

成功率は100% (5/5)、往復の最小/平均/最大= 1/1/1 ms

ただし、VRFcu-greenでSW2またはSW4に到達することはできません。

SW1#ping 192.168.22.1

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.22.1に送信し、タイムアウトは2秒です。

U.UU

成功率は0% (0/5)

SW1#ping 192.168.20.1

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.20.1に送信し、タイムアウトは2秒です。

U.UU

成功率は0% (0/5)

SW2の同じテスト:

SW2からSW4へ:

SW2#ping 192.168.20.1

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.20.1に送信し、タイムアウトは2秒です。

!!!!

成功率は100% (5/5)、往復の最小/平均/最大= 1/1/1 ms

ただし、VRFcu-redでSW3またはSW1に到達することはできません。

```
SW2#ping 192.168.1.1
```

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.1.1に送信し、タイムアウトは2秒です。

```
U.UU
```

成功率は0% (0/5)

```
SW2#ping 192.168.2.1
```

中止するにはエスケープシーケンスを入力します。

5、100バイトのICMPエコーを192.168.2.1に送信し、タイムアウトは2秒です。

```
U.UU
```

成功率は0% (0/5)

R1とR2の両方に、VRFcu-redとcu-green用に別々のテーブルがあります。

最新問題: 191

PEルータはIPv4プレフィックスをMPLSVPN内で何に変換しますか？

- A. VPN-IPv4プレフィックスと64ビットルート識別子の組み合わせ
- B. IPとPEのrouter-idを組み合わせた48ビットルート
- C. ASN、PEルータ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: [\(解答を表示する\)](#)

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: 192

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
```

要約はR1が10.0.0.0/8を受け取るように構成されていますが、より具体的なルートはR1によって受信されます。

Fast Ethernet0 / 0インターフェイスを介してR1に接続された、10.0.0.0/8サマリールートをネイバーからどのように受信する必要がありますか。

A. 要約条件が満たされていません。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。

B. 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 <ASnumber>10.0.0.0.255.0.0.0コマンドを設定する必要があります。

C. 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 number>10.0.0.00.0.0.255コマンドを設定する必要

があります。

D. 要約条件が満たされていませんルータ10 1 100.10には、null0を指す100.0.0/8のルートが必要です。

Answer: [\(解答を表示する\)](#)

最新問題: 193

エンジニアがネットワークを構成しており、ルーティングテーブルにない宛先アドレスのインターフェイスにパケットを転送する必要があります。このタスクを実行するには、何を構成する必要がありますか？

A. set ip next-hop

B. ipdefaultnext-hopを設定します

C. set ip next-hoprecursive

D. set ip next-hop verify-availability

Answer: B [\(メッセージを残す\)](#)

The **set ip default next-hop** command verifies the existence of the destination IP address in the routing table, and...

- if the destination IP address exists, the command does not policy route the packet, but forwards the packet based on the routing table.
- if the destination IP address **does not exist**, the command policy routes the packet by **sending it to the specified next hop**.

最新問題: 194

展示を参照してください。エンジニアはルータに静的ルートを設定しますが、エンジニア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。

この理由は何か？

```
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
```

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静的ルートのメトリックよりも低くなっています。

C. 静的ルートに設定されたADは、OSPFのADよりも高くなっています。

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: [\(解答を表示する\)](#)

セクション :レイヤー3テクノロジー

最新問題: 195

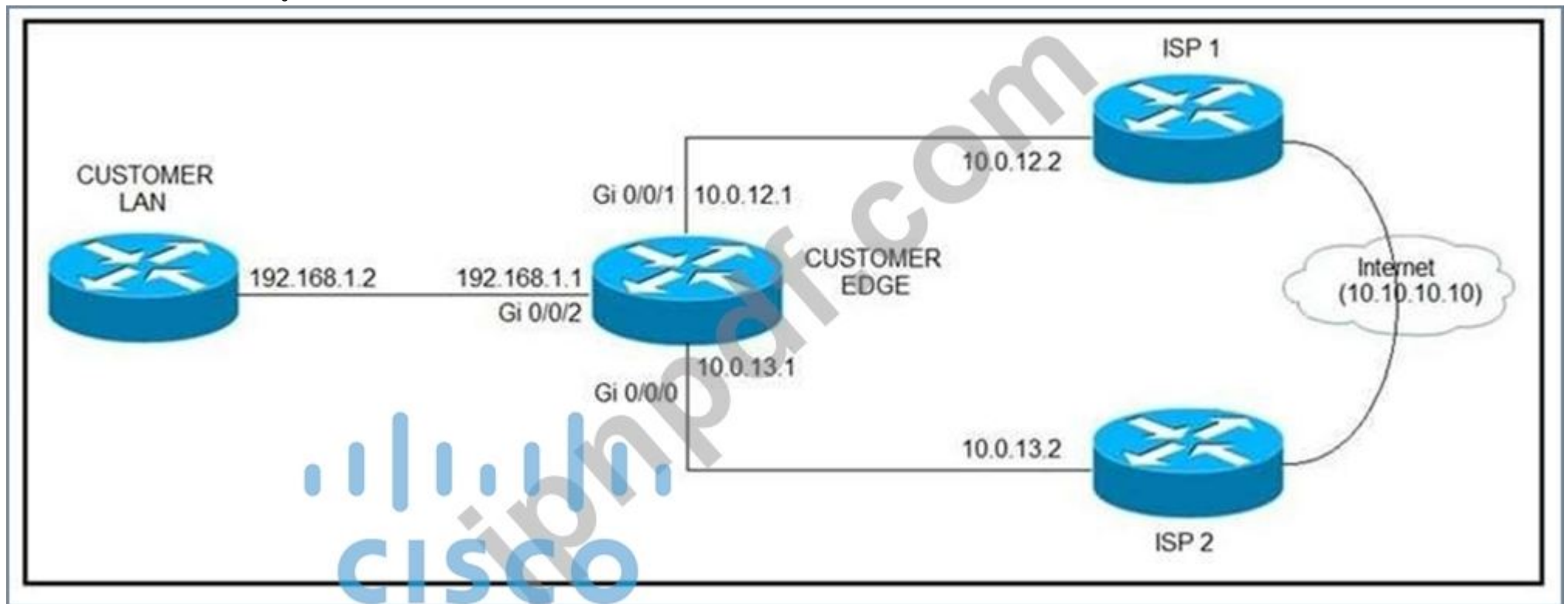
MPLS VPNのどのコンポーネントを使用してIPアドレスを拡張し、エンジニアがどのVPNに属しているかを識別できるようにしますか？

- A. RD
- B. 自民党
- C. VPNv4アドレスファミリ
- D. RT

Answer: [D \(メッセージを残す\)](#)

最新問題: 196

展示を参照してください。



ISP1とISP2はインターネットに直接接続します。顧客は冗長性を実現するために両方のISPリンクを追跡しており、ルータコンソールにCisco IOSIPSLA追跡出力を表示できません。IP SLA設定に欠落しているコマンドはどれですか？

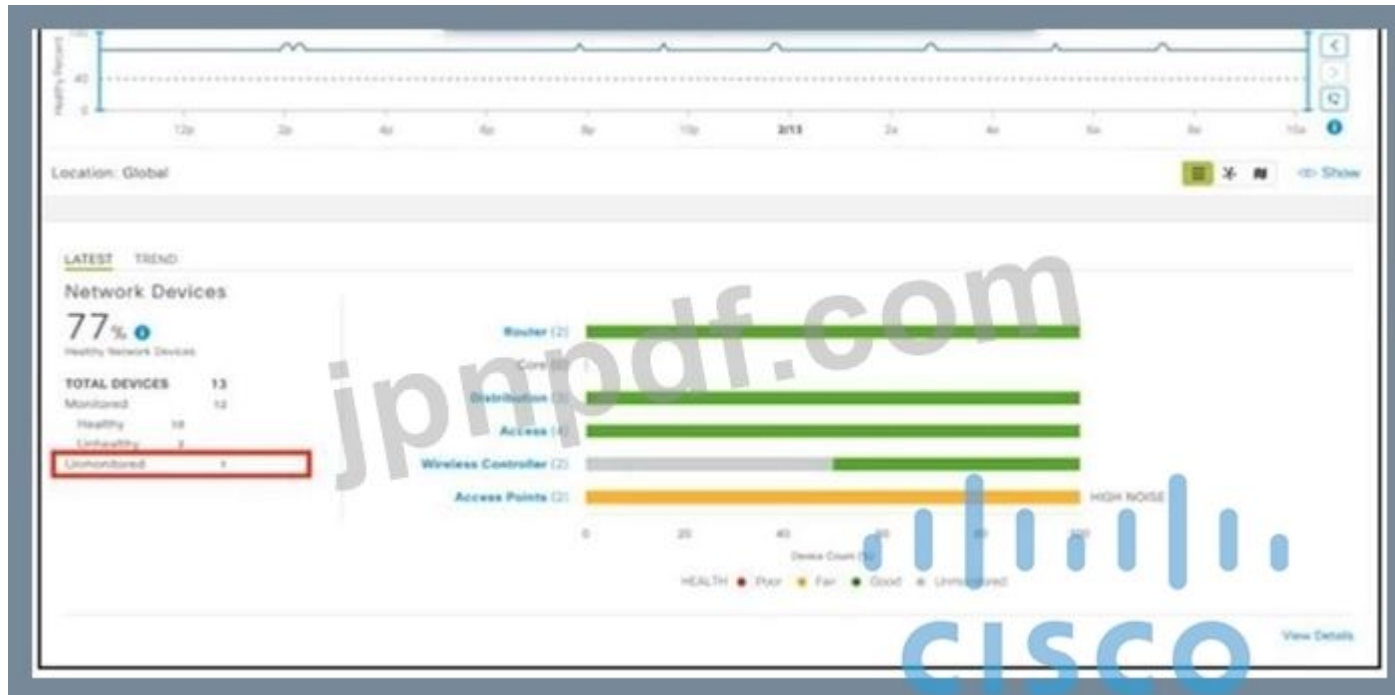
- A. 今すぐ開始時間
- B. 開始時刻0
- C. すぐに開始時刻
- D. 開始時刻00:00

Answer: [\(解答を表示する\)](#)

有効な 300-410 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の 300-410 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をGETする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (80030%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 197

別紙を参照してください。



ネットワーク管理者は、Cisco DNA Centerにルータを1つ追加し、ネットワークヘルスダッシュボードからその検出とヘルスを確認しました。ネットワーク管理者は、ルーターがまだ監視されていないものとして表示されていることを確認しました。Cisco DNA Centerにマウントするには、ルータに何を設定する必要がありますか。

- A. NetFlowデータを使用してルーターを構成します
- B. テレメトリデータを使用してルーターを構成します
- C. CiscoDNACenterに到達するためのルーティングを使用してルータを設定します
- D. SNMPv2cまたはSNMPv3トラップを使用してルーターを構成します

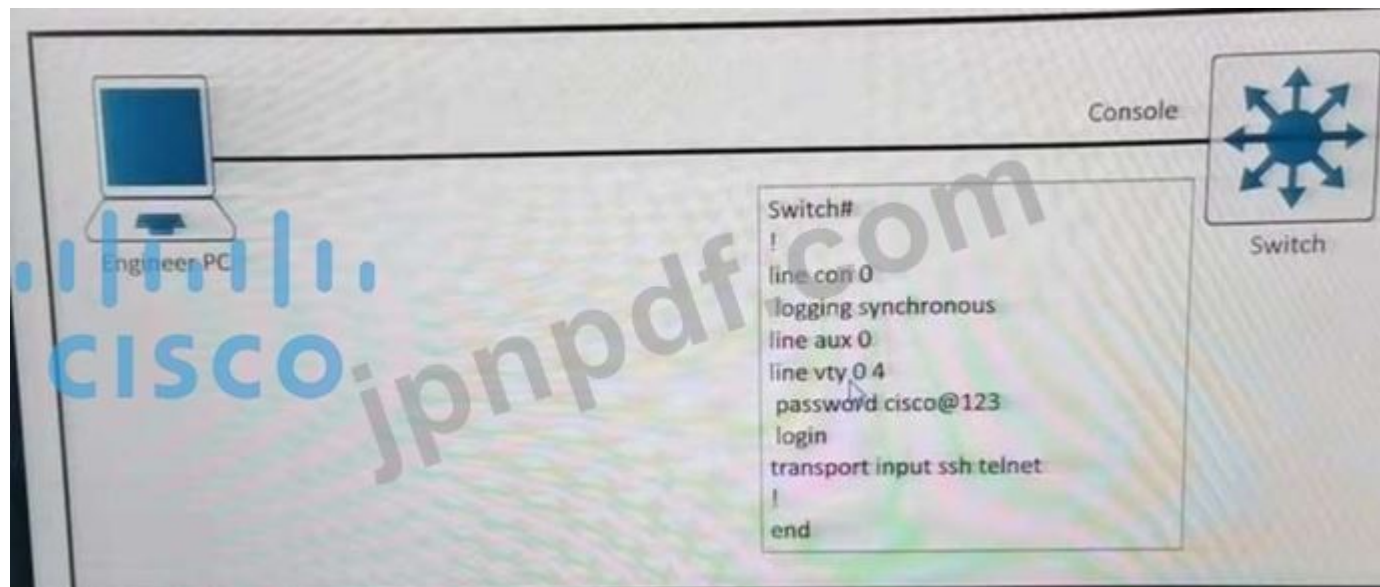
Answer: B (メッセージを残す)

説明

監視されていない：監視されていないデバイスは、指定された時間範囲内にAssuranceがテレメトリデータを受信しなかったデバイスです。

最新問題: 198

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の高床式はコンソールポートを介して接続できます。コンソールポートのどの構成で問題が解決しますか？

- A. exec 0.0
- B. ログインとパスワード
- C. トランスポート入力telnet
- D. 幹部なし

Answer: D (メッセージを残す)

最新問題: 199

展示を参照してください。

```
snmp-server community ciscotest1  
snmp-server host 192.168.1.128 ciscotest  
snmp-sever enable traps bgp
```

ネットワーク操作では、操作サブネットからこの構成を使用してデバイスの構成を読み書きできません。問題を解決する2つの構成はどれですか？ (2つ選択してください。)

- A. コミュニティ ciscotest1に加えてSNMPPrw権限を設定します。
- B. バージョン1に加えてSNMPPrw権限を構成します。
- C. アクセスリスト1を変更し、アクセスリストで操作サブネットを許可します。
- D. コミュニティ ciscotest1に加えてSNMPPrw権限を設定します。
- E. アクセスリスト1を変更し、アクセスリストでSNMPを許可します。

Answer: C,D (メッセージを残す)

最新問題: 200

エンジニアは、ソフトウェアイメージを操作しているときに、CiscoDNACenterがソフトウェアイメージをデバイスから直接アップロードできないことに気付きました。画像がアップロードされないのはなぜですか？

- A. デバイスをCiscoDNACenterに再同期する必要があります。
- B. デバイスのソフトウェアイメージはインストールモードです。

- C. デバイスがCiscoDNACenterへの接続を失いました。
- D. デバイスのソフトウェアイメージはバンドルモードです

Answer: B (メッセージを残す)

インストールモードのデバイスのソフトウェアイメージをアップロードする

[イメージリポジトリ]ページに、ソフトウェアイメージがインストールモードであると表示される場合があります。デバイスがインストールモードの場合、CiscoDNACenterはそのソフトウェアイメージをデバイスから直接アップロードできません。デバイスがインストールモードの場合、次の手順に示すように、イメージをゴールデンとしてマークする前に、まずソフトウェアイメージをCiscoDNACenterリポジトリに手動でアップロードする必要があります。

参照：

dna-center / 1-2-10 / user_guide / b_cisco_dna_center_ug_1_2_10 /
b_dnac_ug_1_2_10_chapter_0100.html

最新問題: 201

メンテナンスウィンドウ中に、管理者が誤ってTelnet関連の構成を削除しました。これにより、金曜日から日曜日の夜間のみ、内部ネットワーク (Eth0/0) からネットワーク外部へのTelnet接続が許可されます。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 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 Friday Saturday Sunday 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)

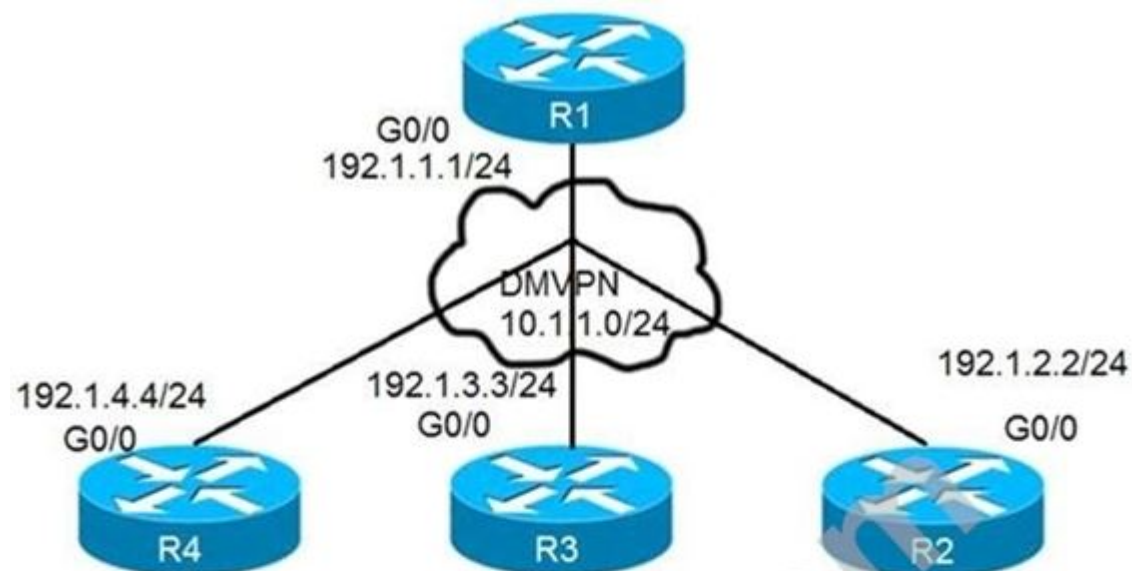
```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range changewindow
!
time-range changewindow
periodic Friday Saturday Sunday
```

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

Answer: D ([メッセージを残す](#))

最新問題: 202

展示品をご覧ください。



```

On R1:
R1(config)# interface tunnel 1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# tunnel source 192.1.1.1
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# ip nhrp network-id 111

```

```

On R2:
R2(config)# interface tunnel 1
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# tunnel source FastEthernet0/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# ip nhrp network-id 222
R2(config-if)# ip nhrp nhs 10.1.1.1
R2(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

```

```

On R3:
R3(config)# interface tunnel 1
R3(config-if)# ip address 10.1.1.3 255.255.255.0
R3(config-if)# tunnel source FastEthernet0/0
R3(config-if)# tunnel mode gre multipoint
R3(config-if)# ip nhrp network-id 333 R3(config-if)# ip nhrp nhs 10.1.1.1
R3(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

```

```

On R4: R4(config)# interface tunnel 1
R4(config-if)# ip address 10.1.1.4 255.255.255.0
R4(config-if)# tunnel source FastEthernet0/0
R4(config-if)# tunnel mode gre multipoint
R4(config-if)# ip nhrp network-id 444
R4(config-if)# ip nhrp nhs 10.1.1.1
R4(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

```

DMVPNのスポークツースポーク間にフェーズ3トンネルを確立することはできません。欠落している2つのコマンドはどれですか？ 2つ選択してください。）

- A. ハブルーターにip nhrpmapコマンドがありません。
- B. ハブルーターにipnhrpショートカットコマンドがありません。
- C. ハブルーターにip nhrpredirectコマンドがありません。
- D. スポークルーターにipnhrpショートカットコマンドがありません。
- E. スポークルーターにip nhrpredirectコマンドがありません。

Answer: ([解答を表示する](#))

最新問題: 203

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？

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
  ipv6 traffic-filter Deny_Telnet in
!

ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
  ipv6 access-map Deny_Telnet in
!

ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
  ipv6 access-map Deny_Telnet in
!

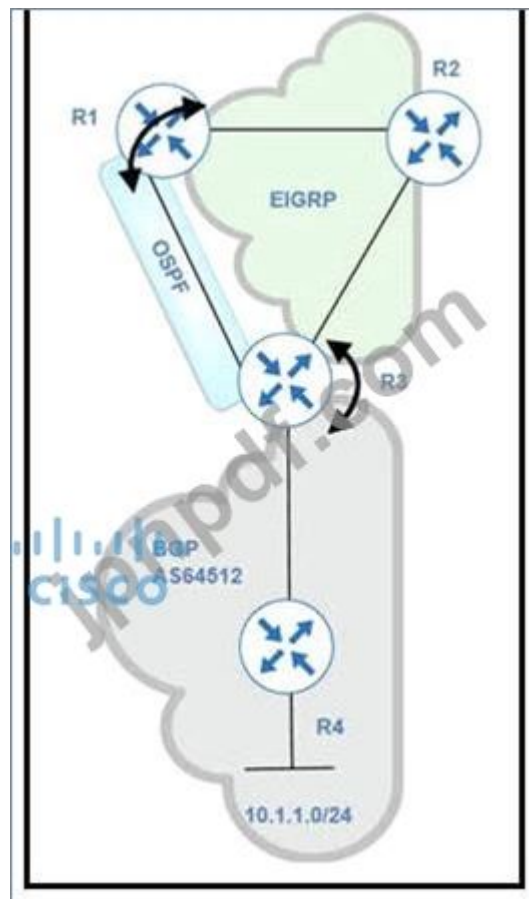
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
  ipv6 traffic-filter Deny_Telnet in
!
```

- 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: ([解答を表示する](#))

最新問題: 204

展示を参照してください。



BGPとEIGRPはR3で相互に再配布され、EIGRPとOSPFはR1で相互に再配布されます。ユーザーは、10.1.1.0/24プレフィックスでホストされているアプリケーションにパケット損失とサービスの中断を報告します。エンジニアは、パケット損失がない状態でR3からR4へのリンクをテストしましたが、debugiprouteコマンドを実行するとR3で頻繁にルーティングが変更されることに気がきました。どのアクションがサービスを安定させますか？

- A. 10.1.1.0/24プレフィックスにタグを付け、プレフィックスがR1のOSPFに再配布されないようにします。
- B. ローカル10.1.1.0/24プレフィックスでICMP pingを使用してR4からテストを繰り返し、サブネットのホスト側またはスイッチ側でレイヤー2エラーを修正します。
- C. OSPF配布リストをR3にアウトバウンドして、10.1.1.0/24プレフィックスがR3にアドバタイズされないようにします。
- D. R3を通過するトラフィックで高いCPUとパケット損失を引き起こすR3での頻繁なOSPF計算を減らします。

Answer: A (メッセージを残す)

再配布後、R3は2つのパスを介してネットワーク10.1.1.0/24について学習します。

+内部BGP (BGP) ADが200 およびメトリックが0)のR4からアドバタイズされます

+ OSPF (ADが110 (E2) およびメトリックが20)のR1からアドバタイズされます

したがって、R3はOSPFを介してADが低いパスを選択します

ただし、これはR3-> R2->R1->R3から受信されるループパスです。したがって、R4からアドバタイズされたルートが期限切れになると、ループされたパスもすぐに期限切れになり、R3はR4からのメインパスを再インストールします。

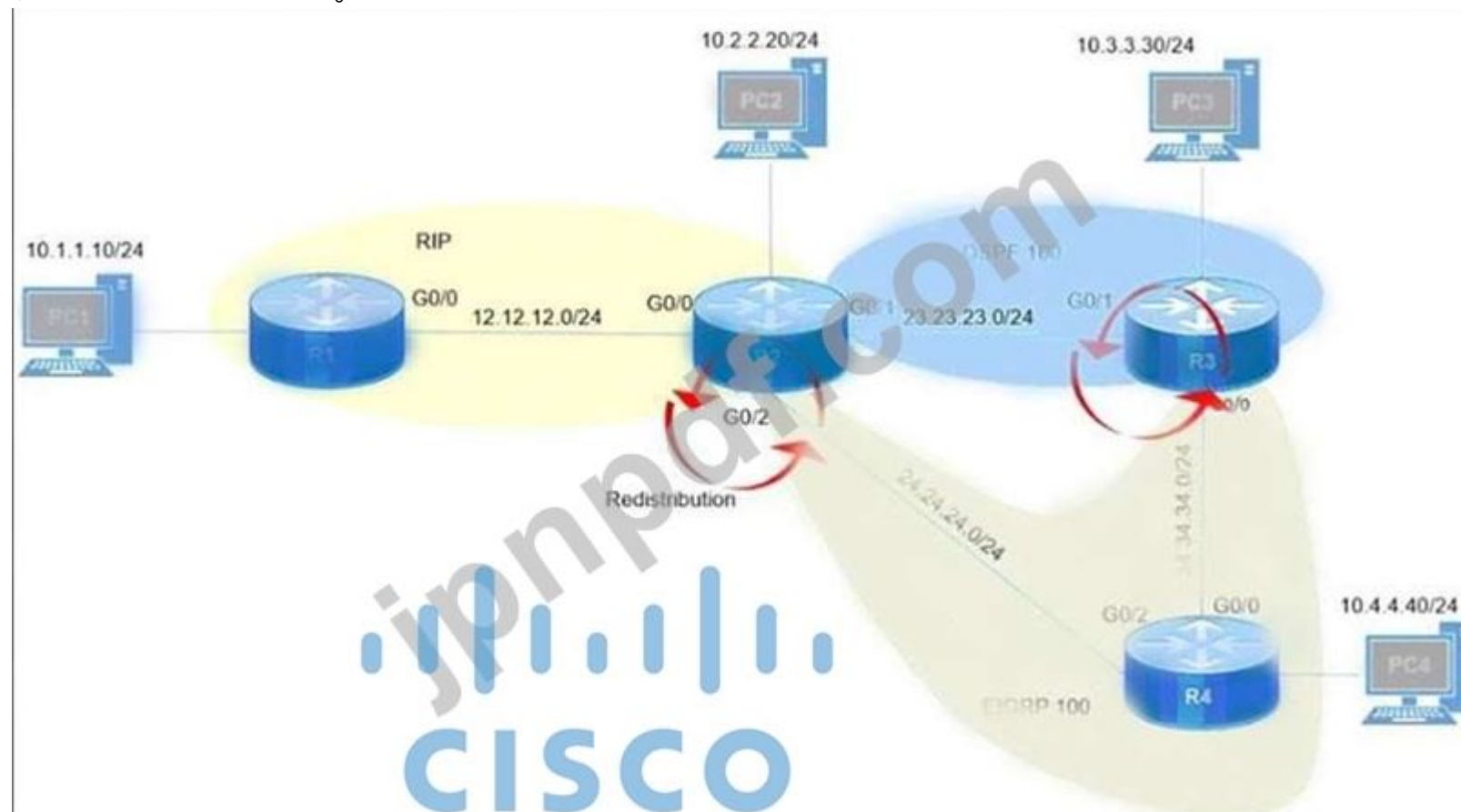
これが断続的な接続の原因です。

この問題は、10.1.1.0/24プレフィックスがR1のOSPFに再配布されないようにすることで解決できます。したがって、R3はR1からこのプレフィックスを学習しません。

または、別の解決策は、OSPF配布リストをR3にインバウンドして、10.1.1.0/24プレフィックスがR3にアドバタイズされないようにすることです。

最新問題: 205

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り、PC2 PC3になり、PC4はPC1に到達できなくなります。問題を解決するための2つの解決策は何ですか？ 2つ選択してください。)

- A. R2でRIPに再配布するときに、RIPルートをRIPにフィルターで戻す
- B. R2のRIPに再配布するときに、OSPFルートをRIPFROMEIGRPにフィルタリングします。
- C. R2で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でOSPFに再配布するときに、EIGRPからOSPFに戻るRIPおよびOSPFルートをフィルタリングします
- E. R3で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 (メッセージを残す)

説明

PC2でさえPC1に到達できないため、R2でのRIPの再配布に問題があります。RIPはOSPFおよびEIGRPよりも管理距離 (AD) 値が高いため、相互再配布を行うときにループされます。

最新問題: 206

```

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-client)
 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

```

エンジニアがBGPを設定し、現在の最適なパスではなく、10.77.255.57からのパスを最適なパスとして選択したいと考えています。問題を解決するアクションはどれですか？

- A. 現在の最適なパスのAS_PATHプリペンドを構成します
- B. 最適なパスとして選択するように上位のMEDを構成します
- C. 目的の最適なパスのAS_PATHプリペンドを構成します
- 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: D (メッセージを残す)

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 (64955 65003) 離れていることがわかります。ASが1つしかないパス (たとえば、172.16.254.234からのパス)がいくつかありますが、それらは最適なパスとして選択さ

れなかったため、AS_PATHを使用して最適なパスを決定しませんでした-回答Aと回答Cは正しくありません。
 出力のすべてのパスのメトリックは0であり、これはこの属性の最小（最良）値です。より高いMEDを構成すると、他のパスよりも優先されなくなり、回答Bは正しくありません。
 回答Dのみが残りますが、LOCAL_PREF属性はより高い値で構成する必要があるため、ここでの「より低いLOCAL_PREF」はより高い値を意味することを願っています。しかし、これが最良の答えです。

最新問題: 207

IPv6ファーストホップセキュリティデバイスの役割を左側から右側の対応する説明にドラッグアンドドロップします。

host	Receives router advertisements from valid routers, and no router solicitation are received.
router	Receives router solicitation and sends router advertisements.
monitor	Receives valid and rogue router advertisements and all router solicitation.
switch	Received router advertisements are trusted and are flooded to synchronize states.

Answer:

host	router
router	host
monitor	switch
switch	monitor

説明

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



最新問題: 208

展示を参照してください。

```
R1#show policy-map control-plane
Control Plane
Service-policy input: CoPP
Class-map: PERMIT (match-all)
 50 packets, 3811 bytes
 5 minute offered rate 0000 bps
 Match: access-group 100
Class-map: ANY (match-all)
 210 packets, 19104 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: access-group 199
 drop
Class-map: class-default (match-any)
 348 packets, 48203 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: any

R1#show access-list 100
Extended IP access list 100
 10 permit udp any any eq 23 (100 matches)
 20 permit tcp any any eq telnet (5 matches)
 30 permit tcp any eq telnet any (10 matches)

R1#show access-list 199
Extended IP access list 199
 10 deny tcp any eq telnet any (50 matches)
 50 permit ip any any (1 match)

R1#show running-config | section line vty
line vty 0 4
 login
 transport input telnet ssh
 transport output telnet ssh
```

SSHによるルーターR1へのアクセスを制限する2つのアクションはどれですか？ (2つ選択してください。)

- A. 行vtyでトランスポート出力sshを設定し、アクセスリスト199からシーケンス10を削除します。
- B. アクセスリスト100からシーケンス10を削除し、シーケンス20を追加してアクセスリストへの任意のeqtelnetのtcpを拒否します
199
- C. 行vtyでトランスポート入力sshを設定し、アクセスリスト100からシーケンス30を削除します。
- D. service-policyCoPPからclass-mapANYを削除します
- E. 行vtyでトランスポート出力sshを設定し、アクセスリスト100からシーケンス20を削除します。

Answer: C,D (メッセージを残す)

最新問題: 209

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引き続き存在します。どのアクションがルートをブロックしますか？

- A. route-mapコマンドのシーケンス10をpermitからdenyに変更します。
- B. 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-DLdeny20。
- C. 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。
- D. 標準の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: A (メッセージを残す)

最新問題: 210

展示を参照してください。



Cisco DNA Center Assurance DashboardのAPステータスは、アクセススイッチインターフェイスG1/0/14からの物理的な接続の問題を示しています。物理的な接続の問題を解決するために診断データを生成するコマンドはどれですか？

- A. show cable-diagnostics tdr interface 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. ケーブル診断のテストtdrインターフェイスGigabitEthernet1 / 0/14
- D. ケーブル診断tdrインターフェースGigabitEthernet1/0/14を確認してください

Answer: ([解答を表示する](#))

最新問題: 211

展示を参照してください。

```

R1 (config)# ip vrf CCNP
R1 (config-vrf)# rd 1:100
R1 (config-vrf)# exit
R1 (config)# interface Loopback0
R1 (config-if)# ip address 10.1.1.1 255.255.255.0
R1 (config-if)# ip vrf forwarding CCNP
R1 (config-if)# exit
R1 (config)# exit
R1# ping vrf CCNP 10.1.1.1
% Unrecognized host or address, or protocol not running.

```

展示を参照してくださいVRFCCNPを機能させるには、どのコマンドを構成する必要がありますか？

```
interface Loopback0
ip address 10.1.1.1 255.255.255.0
vrf forwarding CCNP

interface Loopback0
ip address 10.1.1.1 255.255.255.0

interface Loopback0
vrf forwarding CCNP

interface Loopback0
ip address 10.1.1.1 255.255.255.0
ip vrf forwarding CCNP
```

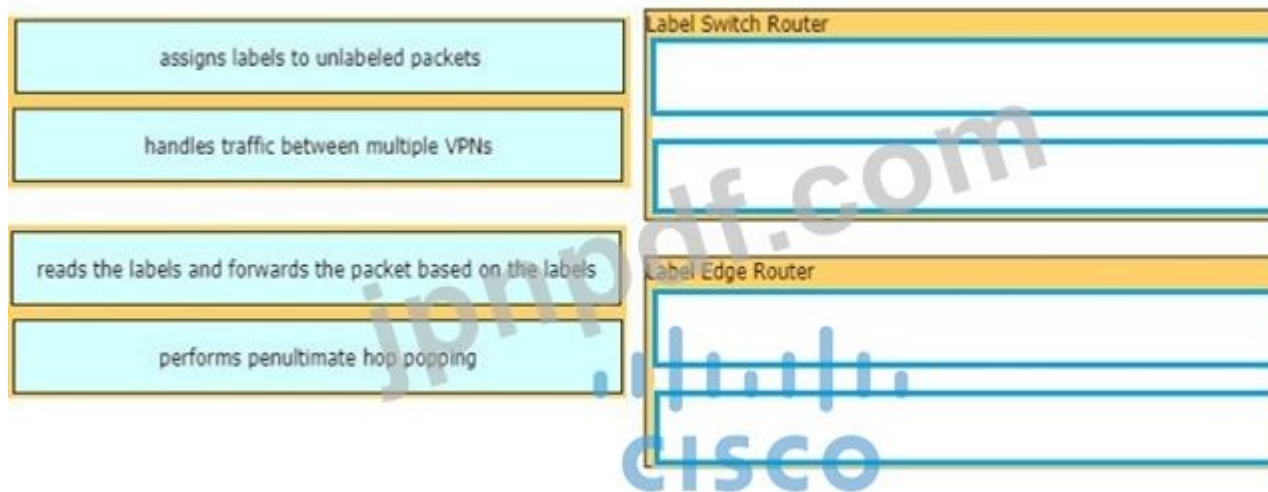
- A. オプションC
- B. オプションA
- C. オプションD
- D. オプションB

Answer: D (メッセージを残す)

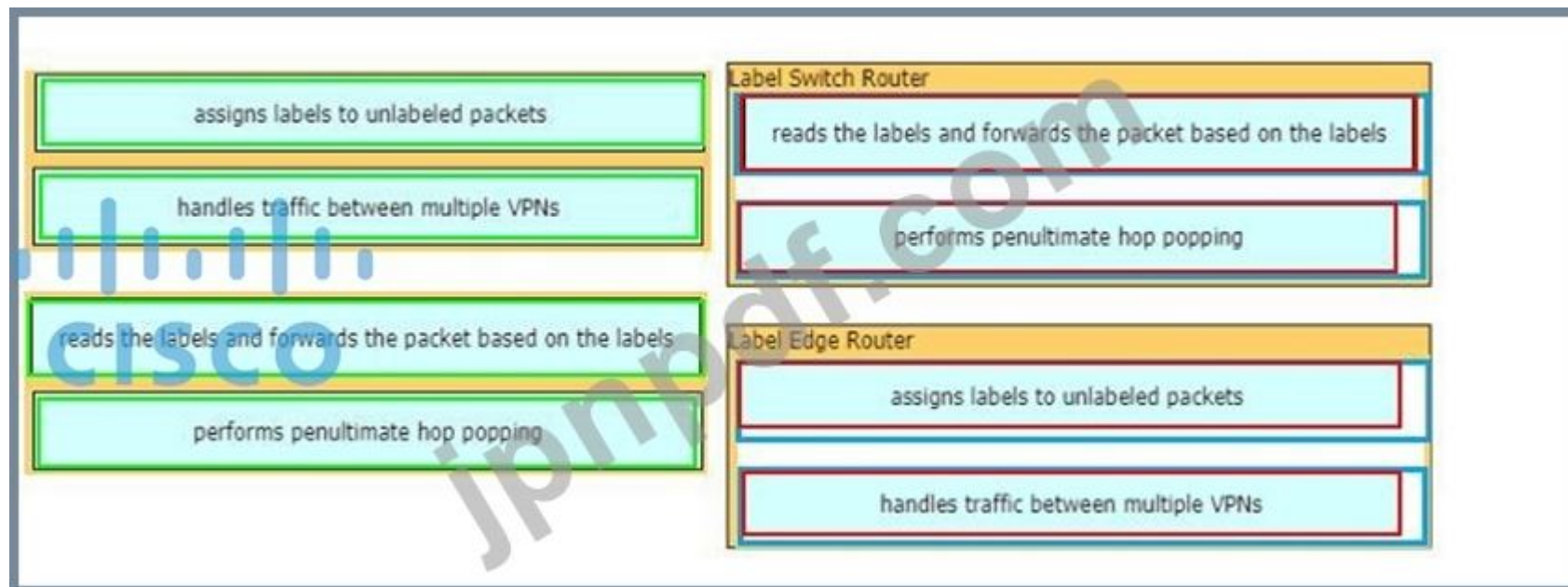
有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 212

操作を左から右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: 213

展示を参照してください。



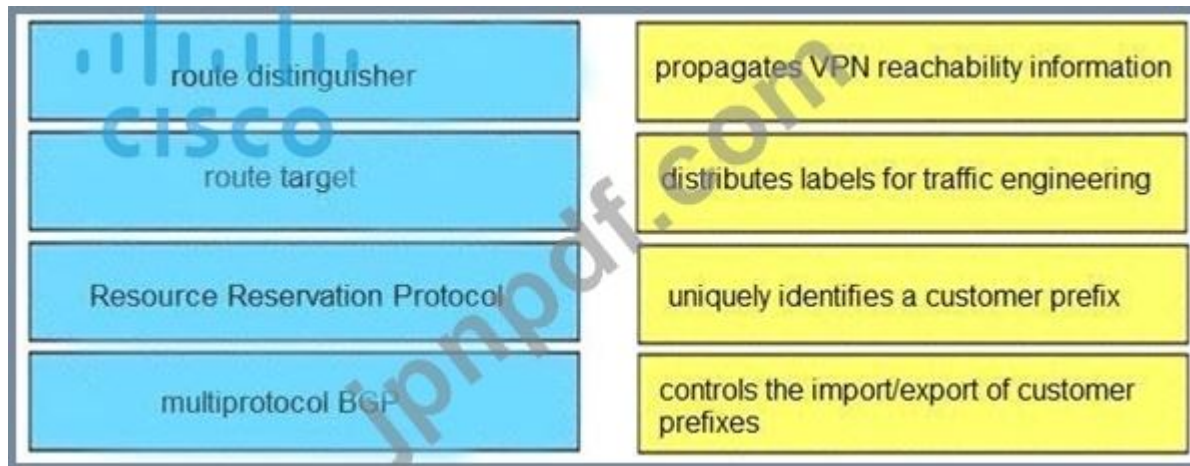
198A :0 :200C :: 1/64からルータ2へのTelnetトラフィックを拒否する設定はどれですか？

- A. `Ipv6 access-list-Deny_Telnet sequence 10 deny tcp host 198A :0 :200C :: 1/64 host 201A :0 :205C :: 1/64 ! int Gi0 / 0 Ipv6` トラフィック フィルター `Deny_Telnet in !`
- B. `Ipv6 access-list-Deny_Telnet sequence 10 deny tcp host 198A :0 :200C :: 1/64 host 201A :0 :205C :: 1/64 eq telnet ! int Gi0 / 0 Ipv6` トラフィック フィルター `Deny_Telnet in !`
- C. `Ipv6 access-list-Deny_Telnet sequence 10 deny tcp host 198A :0 :200C :: 1/64 host 201A :0 :205C :: 1/64 eq telnet ! int Gi0 / 0 Ipv6` `access-map Deny_Telnet in !`
- D. `Ipv6 access-list-Deny_Telnet sequence 10 deny tcp host 198A :0 :200C :: 1/64 host 201A :0 :205C :: 1/64 ! int Gi0 / 0 Ipv6` `access-map Deny_Telnet in !`

Answer: B ([メッセージを残す](#))

最新問題: 214

MPLS VPNの概念を左から、右の正しい説明にドラッグアンドドロップします。



Answer:



最新問題: 215

展示を参照してください。

```

R1#show policy-map control-plane
Control Plane
Class-map: NMS (match-all)
500461 packets, 24038351 bytes
5 minute offered rate 1390000 bps, drop rate 0 bps
police:
cir 50000 bps, bc 5000 bytes
conformed 50444 packets, 24031001 bytes; actions:
transmit
exceeded 990012 packets, 94030134 bytes; actions
drop conform 4000 bps, exceed 0 bps
R1#

```

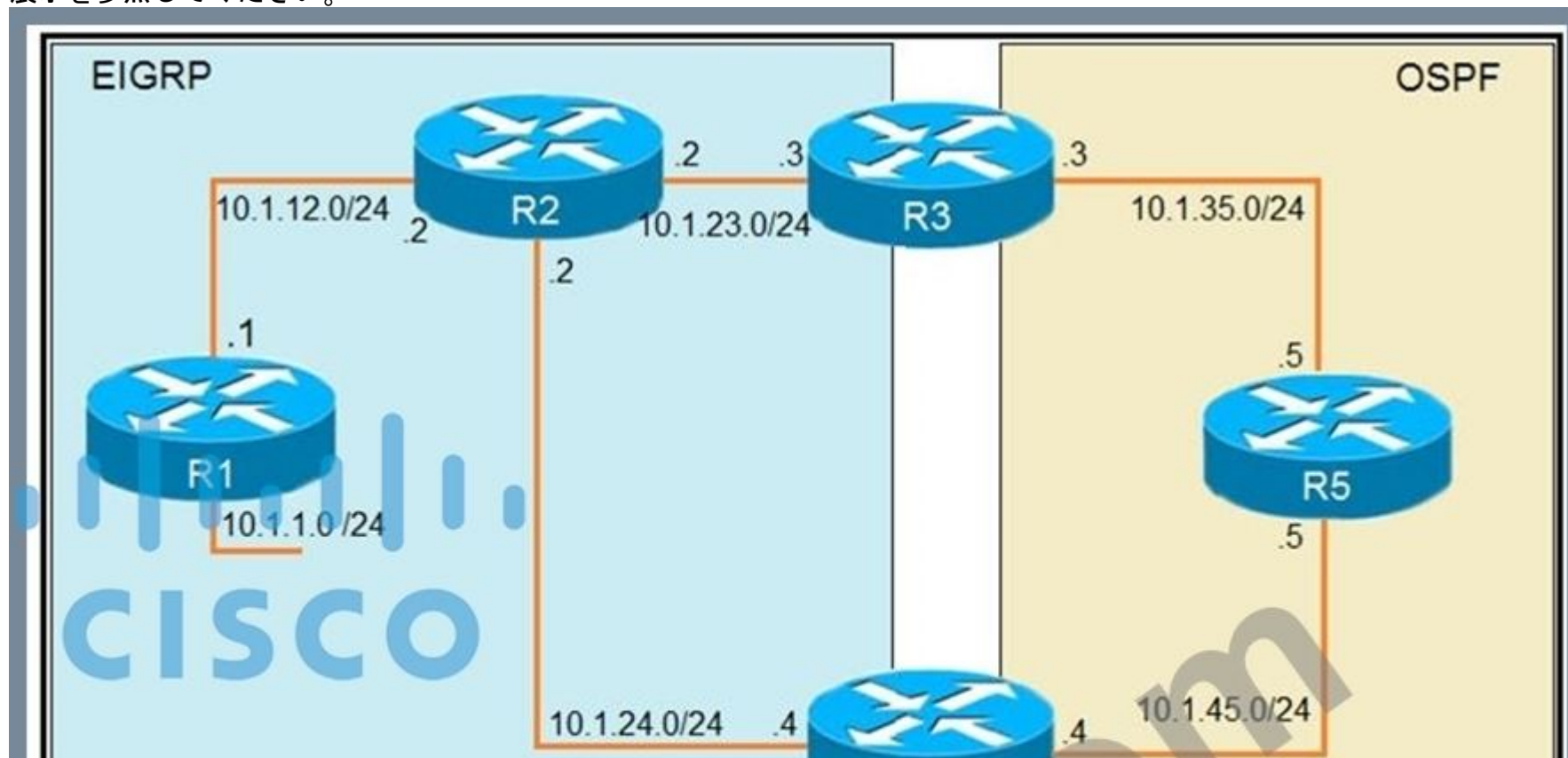
ある会社が複数のネットワーク管理システムツールを評価しています。SNMPデータによって生成されたトレンドグラフはNMSによって返され、複数のギャップがあるように見えます。問題のトラブルシューティング中に、エンジニアは関連する出力に気づきました。グラフのギャップを解決するものは何ですか？

- A. すべてのNMSツールに対応できる低い値にCIRレートを構成します
- B. クラスマップのexceed-rateコマンドを削除します。
- C. 適切なCoPPアクションを使用して、特定のプロトコルに基づいてNMSクラスマップを複数のクラスマップに分離します
- D. クラスマップNMSをコントロールプレーンポリシングの一部から削除します。

Answer: [\(解答を表示する\)](#)

最新問題: 216

展示を参照してください。



R4

```
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 truncated>
```

R5からのトレースルートの出力は、ネットワーク内のループを示しています。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)

```
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 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: B ([メッセージを残す](#))

最新問題: 217

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確認しました。

問題を解決する2つのアクションはどれですか？ 2つ選択してください。)



- A. R3でモードをモードトンネルからモードトランスポートに変更します。
- B. R2およびR3の暗号isakmpキー-ciscoアドレス10.1.1.1を削除します。
- C. R2およびR3でcrypto isakmpkeyciscoアドレス192.1.1.1を設定します。
- D. R2およびR3でcrypto isakmpkeyciscoアドレス0.0.0.0を設定します。
- E. モードをモードトランスポートからR2のモードトンネルに変更します。

Answer: ([解答を表示する](#))

セクション :VPNテクノロジー

最新問題: 218

展示を参照してください。管理者は、デフォルトルートのみを使用して任意のネットワークに到達するように、リモートの低リソースルーターへのルートアドバタイズメントを構成しましたが、失敗しました。この問題を解決するアクションはどれですか？

- A. シーケンス番号5の行をプレフィックスリストから削除します。
- B. distribute-listコマンドの方向をoutからinに変更します。
- C. distribute-listコマンドからprefixキーワードを削除します。
- D. シーケンス番号10の行をプレフィックスリストから削除します。

Answer: A ([メッセージを残す](#))

最新問題: 219

展示を参照してください。

```

ip dhcp pool 1
network 200.30.30.0/24
default-router 200.30.30.100
lease 40
!
ip dhcp pool 2
network 200.30.40.0/24
default-router 200.30.40.100
lease 40
!

```

財務部門のサーバーは、200.30.40.0 / 24ネットワーク上で一貫して到達可能ではなく、2か月ごとに新しいIPアドレスを取得します。この問題を解決するには、どの2つのアクションを実行する必要がありますか？ 2つ選択してください。）

- A. デフォルトゲートウェイ20030.30.100のネットワークでDHCPを使用するようにサーバーを構成します。
- B. サーバーのIPアドレスを除外するようにルーターを構成します。
- C. デフォルトゲートウェイ20030.40.100のネットワークでDHCPを使用するようにサーバーを構成します。
- D. 静的IPアドレスとデフォルトゲートウェイを使用してサーバーを構成します。

Answer: B,D (メッセージを残す)

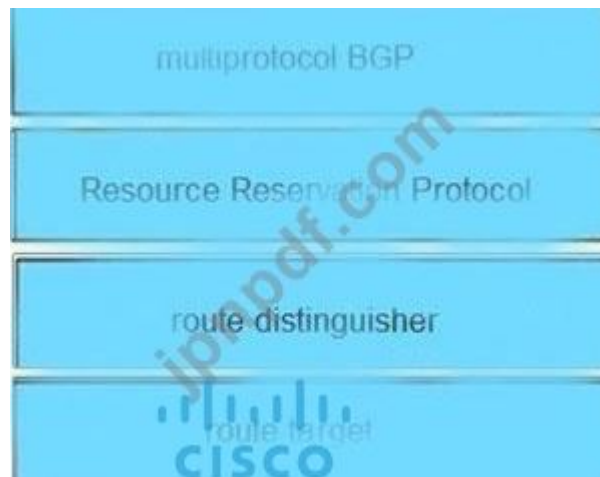
最新問題: 220

MPLS VPNの概念を左から、右の正しい説明にドラッグアンドドロップします。

route distinguisher	propagates VPN reachability information
route target	distributes labels for traffic engineering
Resource Reservation Protocol	uniquely identifies a customer prefix
multiprotocol BGP	controls the import/export of customer prefixes

Answer:

route distinguisher	multiprotocol BGP
route target	Resource Reservation Protocol
Resource Reservation Protocol	route distinguisher
multiprotocol BGP	route target



最新問題: 221

展示を参照してください。



自律システム番号AS65401の会社は、ARINからIPアドレスブロック209.165.200.224/27を取得しました。会社はより多くのIPアドレスを必要とし、ISP2からブロック209.165.202.128/27を割り当てられました。エンジニアはISP1であり、AS65401からISP2ルートを受信していると報告しています。R1のどの構成で問題が解決しますか？

A)

```
access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
neighbor 209.165.201.1 distribute-list 10 out
```

B)

```
access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
neighbor 209.165.201.1 distribute-list 10 in
```

C)

```
ip route 209.165.200.224 255.255.255.224 209.165.201.1
ip route 209.165.202.128 255.255.255.224 209.165.201.5
```

D)

```
ip route 0.0.0.0 0.0.0.0 209.165.201.1
ip route 0.0.0.0 0.0.0.0 100 209.165.201.5
```

- 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 ([メッセージを残す](#))

説明

<https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/23675-27.html>

最新問題: 222

2つのMPLSラベルの特徴は何ですか？ (2つ選択してください。)

- A. MPLSパケットには最大2つのラベルを付けることができます。
- B. LDPはTCPを使用して情報を確実に配信します。

- C. ラベルはレイヤー3ヘッダーの後のパケットに付けられます。
- D. ラベルエッジルーターは、受信したパケットのラベルを交換します。
- E. MPLSラベルは、転送等価クラスを識別する短い識別子です。

Answer: C,E (メッセージを残す)

最新問題: 223

エンジニアは、イベントの信頼できる暗号化された通知を管理サーバーに送信するようにCiscoルーターを設定しました。通知メッセージは信頼できますが、暗号化されていないことがわかりました。問題を解決するアクションはどれですか？

- A. SNMPv3インフォーム用にすべてのデバイスをprivで構成します。
- B. SNMPv3インフォーム用にすべてのデバイスをauthで構成します。
- C. すべてのデバイスをauthを使用してSNMPv3トラップ用に構成します。
- D. privを使用してSNMPv3トラップ用にすべてのデバイスを構成します。

Answer: (解答を表示する)

説明

SNMP通知は、トラップまたは通知要求として送信できます。このデバイスがトラップを受信したときに受信者が確認応答を送信しないため、トラップは信頼できません。「イベントに対して信頼性の高い暗号化された通知を送信する」ため、SNMP通知になります。暗号化については、「priv」を構成する必要があります。

最新問題: 224

ネットワークエンジニアは、NTPサーバーに同期されているコアスイッチのフラッピング (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刻は表示されません。スイッチのログに、デバイスの時計に従ってフラップの時間を表示できるコマンドはどれですか。

- A. 夏時間の時計の繰り返し2日曜日3月2:001日曜日11月2:00
- B. サービスタイムスタンプログ日時ローカルタイムshow-timezone
- C. 時計カレンダー有効
- D. サービスタイムスタンプログの稼働時間

Answer: D (メッセージを残す)

最新問題: 225

展示を参照してください。

```
Global RADIUS shared secret:*****
retransmission count:5
timeout value:10
following RADIUS servers are configured:
  myradius.cisco.users.com:
    available for authentication on port:1814
    available for accounting on port:1813
  10.1.1.1:
    available for authentication on port:1814
    available for accounting on port:1813
    RADIUS shared secret:*****
  10.2.2.3:
    available for authentication on port:1814
    available for accounting on port:1813
    RADIUS shared secret:*****
```

AAAサーバ10.1.1.1はデフォルトの認証およびアカウントング設定で設定されていますが、スイッチがサーバと通信できません。この問題を解決するアクションはどれですか。

- A. 認証ポートと一致します
- B. アカウント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 (メッセージを残す)

説明

コマンドのデフォルト

アカウントングポート :1813

認証ポート :1812

アカウントング : 有効

認証 : 有効

再送信回数 :1

アイドル時間 :0

サーバー監視 : 無効

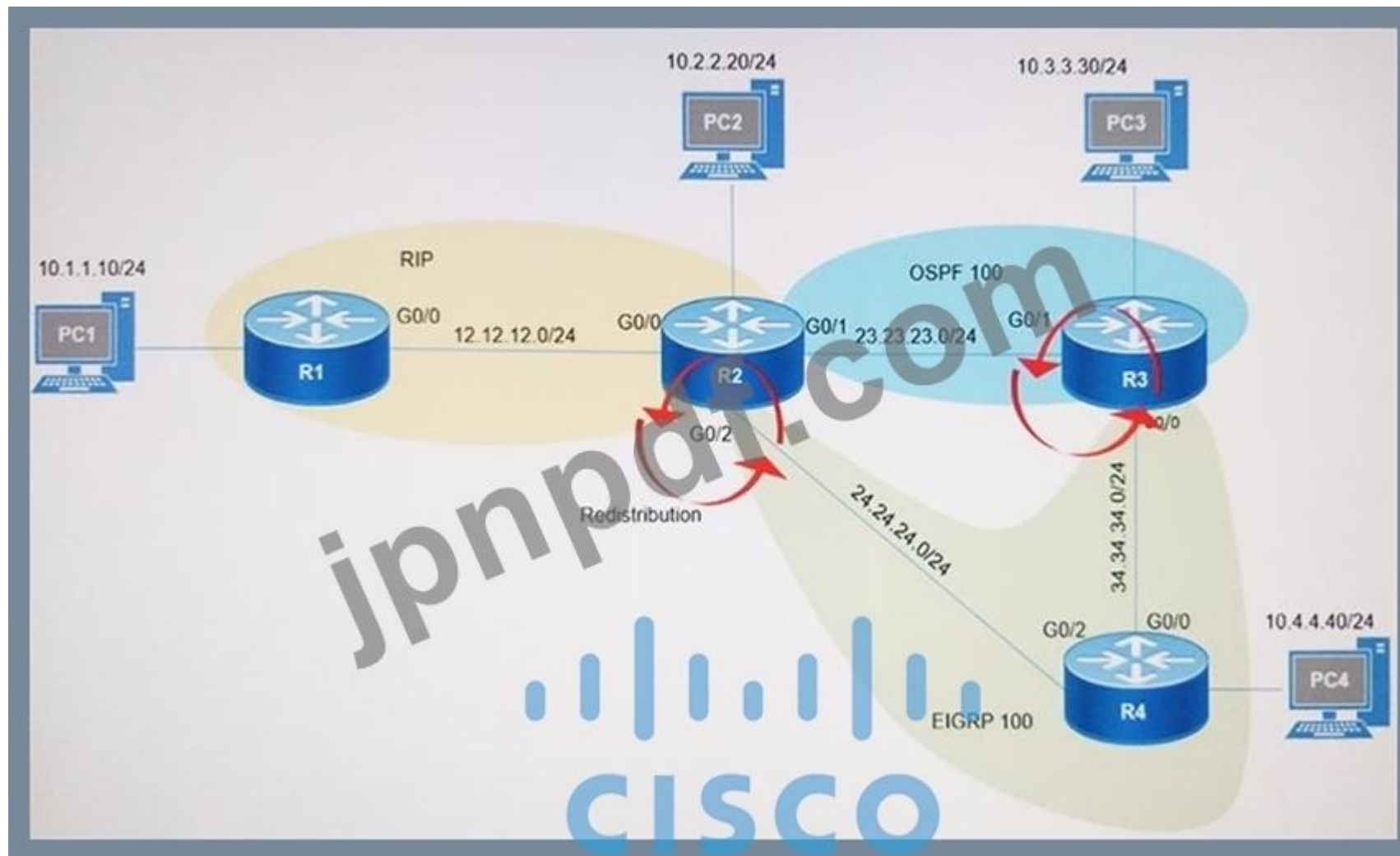
タイムアウト :5秒

ユーザー名のテスト :テスト

テストパスワード :テスト

最新問題: 226

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に到達できるように、エンジニアは問題を解決するためにどのアクションを実行できますか？

- A. OSPFからEIGRPに再配布される時に、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プロセスで管理距離100を設定します。
- C. 直接接続されたインターフェースをR2に再配布します。
- D. RIPからEIGRPに再配布する時に、プレフィックス10.1.1.0/24をフィルタリングします。

Answer: A ([メッセージを残す](#))

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **227**

IPv6ルーターアドバタイズメントガード機能を使用する代わりに、どの構成機能を使用して不正なルーターアドバタイズメントをブロックする必要がありますか？

- A. 許可されていないホストからのブロードキャストフレームをブロックするVACL

- B. ルーターアドバタイズメントに関連付けられた無差別ポートとノードの分離ポートを備えたPVLAN
- C. ルーターアドバタイズメントに関連付けられたコミュニティポートとノードの分離ポートを備えたPVLAN
- D. 許可されていないホストからのIPv4ACLブロッキングルーターアドバタイズメント

Answer: D (メッセージを残す)

説明
 IPv6ルーターアドバタイズメントガード機能は、ネットワーク管理者がネットワークデバイスプラットフォームに到着する不要または不正なルーターアドバタイズメントガードメッセージをブロックまたは拒否できるようにするためのサポートを提供します。ルーターアドバタイズメントは、デバイスがリンク上で自分自身をアナウンスするために使用されます。IPv6ルーターアドバタイズメントガード機能は、これらのルーターアドバタイズメントを分析し、許可されていないデバイスによって送信されたルーターアドバタイズメントを除外します。特定のスイッチプラットフォームは、管理者が「ユーザー」ポートに着信する可能性のあるRA ICMPメッセージをブロックするアクセス制御リスト (ACL)を設定することにより、ある程度の不正なRAフィルタリングをすでに実装できます。

最新問題: 228

MPLS VPNの概念を左から、右の正しい説明にドラッグアンドドロップします。

route distinguisher	propagates VPN reachability information
route target	distributes labels for traffic engineering
Resource Reservation Protocol	uniquely identifies a customer prefix
multiprotocol BGP	controls the import/export of customer prefixes

Answer:

route distinguisher	multiprotocol BGP
route target	Resource Reservation Protocol
Resource Reservation Protocol	route target
multiprotocol BGP	route distinguisher

参照 :

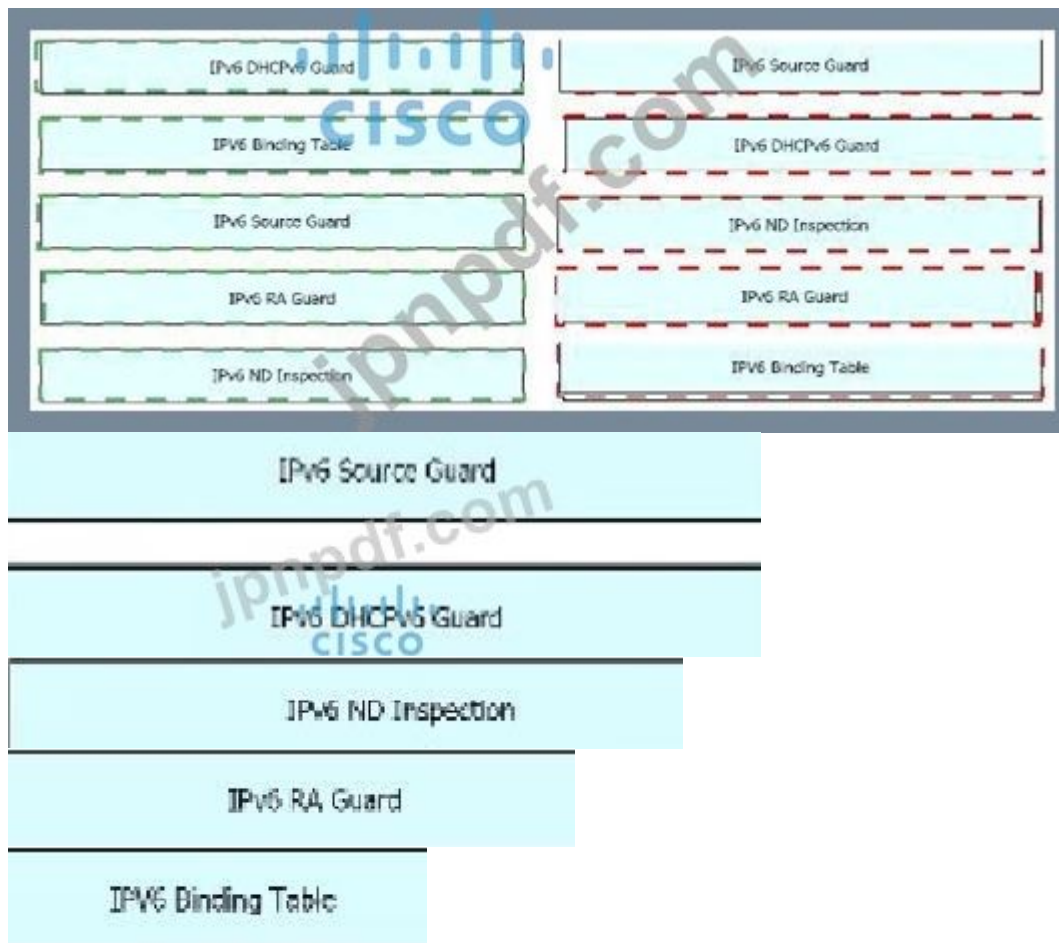
<https://www.rogerperkin.co.uk/featured/route-distinguisher-vs-route-target/>

最新問題: 229

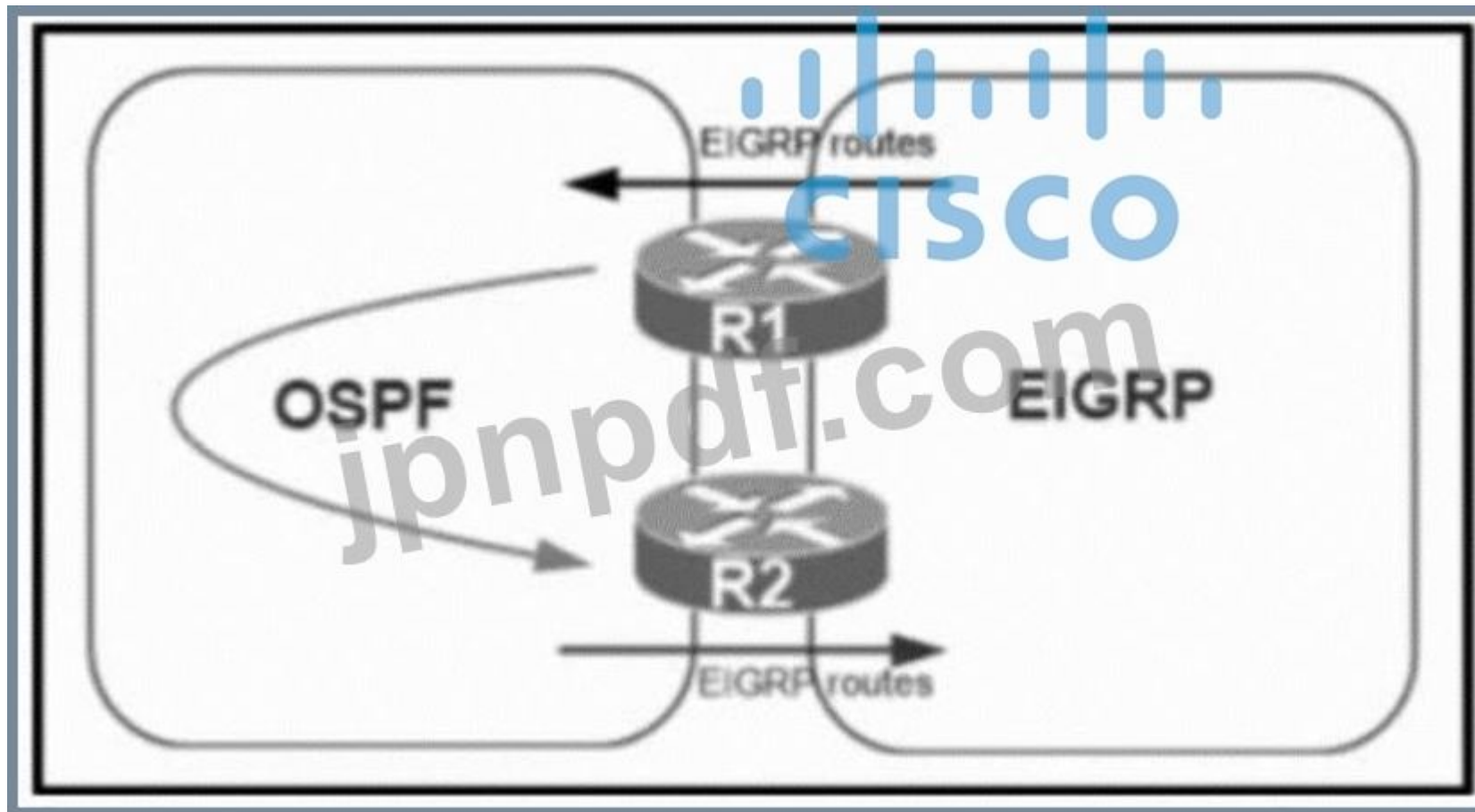
IPv6First-HopSecurity機能を左側から右側の定義にドラッグアンドドロップします。

IPv6 DHCPv6 Guard	Block a malicious host and permit the router from a legitimate route.
IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents.
IPv6 Source Guard	Create a binding table that is based on NS and NA messages.
IPv6 RA Guard	Filter inbound traffic on Layer 2 switch ports that are not in the IPv6 binding table.
IPv6 ND Inspection	Create IPv6 neighbors connected to the device from information sources such as NDP snooping.

Answer:



最新問題: 230



展示を参照してください。ネットワーク管理者がR1および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。問題を解決するアクションはどれですか？

- A. R1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。R2で同じタグを照合して、OSPFをEIGRPに再配布するときに許可します。
- B. EIGRPのサマリールートをOSPFにアドバタイズし、OSPFに再配布するときに特定のEIGRPルートを拒否します。
- C. R1のOSPFドメインにEIGRPネットワークルートのプレフィックスリストを適用して、EIGRPルーティングドメインに伝播します。
- D. R1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。R2の同じタグを照合して、OSPFをEIGRPに再配布するときに拒否します。

Answer: ([解答を表示する](#))

最新問題: 231

展示を参照してください。

```
snmp-server community Public RO 90
snmp-server community Private RW 90
R1#show access-list 90
Standard IP access list 90
 permit 10.11.110.11
 permit 10.11.111.12
```

```
Nov 6 06:45:11: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
10.11.110.12
Nov 6 06:45:12: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
10.11.110.12
```

ネットワーク管理者は、インターフェイスE1/0から発信されたホスト10.11.110.12からのこれらのコンソールメッセージに気づきます。管理者は、これがR1上のSNMPへの不正なアクセスの試みであると見なします。R1 E1/0に到達する試みを妨げるアクションはどれですか？

- A. インターフェイスE1/0でACL90を使用してIOSコントロールプレーン保護を設定します
- B. ホスト10.11.110.12を含む許可ステートメントをACL90に追加します
- C. インターフェイスE1/0にインバウンドACLを作成して、ホスト10.11.110.12からのSNMPを拒否します。
- D. インターフェイスE1/0でACL90を使用してIOS管理プレーン保護を設定します

Answer: C ([メッセージを残す](#))

最新問題: 232

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. 10.2.2.0/24
- B. 10.2.3.0/26

C. 10.1.4.0/26

D. 10.1.2.0/24

Answer: A ([メッセージを残す](#))

最新問題: 233

展示を参照してください。

```
R1#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login Console local
R1#show running-config | section line
line con 0
 logging synchronous
R1#
```

エンジニアが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。どのアクションが目的の構成を生成しますか？

A. グローバル設定にaaa authentication login default group tacacs+local-caseコマンドを追加します。

B. グローバル設定にaaa authentication login default noneコマンドを追加します。

C. aaa authentication login Console localコマンドで、大文字の「C」を小文字の「c」に置き換えます。

D. login authentication Consoleコマンドを回線構成に追加します

Answer: D ([メッセージを残す](#))

最新問題: 234

実装グループは、テストベッドを使用して「概念実証」を実行しており、クライアント1とクライアント2の両方が209.65.200.241のWEBサーバーにアクセスする必要があります。ネットワークアドレス指定、ルーティングスキーム、DHCPサービス、NTPサービス、およびFHRPサービスにいくつかの変更を加えた後、クライアント1が209.65.200.241アドレスにpingできないことを示すトラブルチケットが開かれました。サポートされているコマンドを使用して、この障害の原因を特定し、次の質問に答えてください。

障害状態はどのテクノロジーに関連していますか？

A. NTP

B. スイッチ間の接続

C. アクセスVLAN

D. ポートセキュリティ

E. VLANACL/ポートACL

F. 仮想インターフェースの切り替え

Answer: B ([メッセージを残す](#))

クライアントはAPIPAを取得しているため、DHCPが機能していないことがわかります。ただし、ASW1設定を詳しく調べると、問題はDHCPにあるのではなく、クライアントがVLAN 10に属している場合、ポートチャネルのトランクがVLAN 1~9のみを許可していることがわかります。VLAN10はそうではありません。ASW1でトランクをトラバースするため、問題はスイッチ間の接続、特にASW1のトランク設定にあります。

最新問題: 235

Router#sh ip route ospf

<output omitted>

Gateway is last resort is not set

10.0.0.0/24 is subnetted, 1 subnets

- o E2 10.0.0.0 [110/20] via 192.168.12.2, 00:00:10, Ethernet0/0
- o 192.168.3.0/24 [110/20] via 192.168.12.2, 00:00:50, Ethernet0/0

Router#

Router#show ip bgp

<output omitted>

	Network	Next Hop	Metric	LocPrf	Weight	Path
>*	192.168.1.1/32	0.0.0.0	0		32768	?
>*	192.168.3.0	192.168.12.2	20		32768	?
>*	192.168.12.0	0.0.0.0	0		32768	?

Router#show running-config | section router bgp

router bgp 65000

bgp log-neighbor-changes

redistribute ospf 1

Router#

展示を参照してください。エンジニアがOSPFをBGPに再配布しようとしていますが、すべてのルートが再配布されているわけではありません。

この問題の理由は何ですか？

- A. デフォルトでは、内部ルートと外部タイプ1ルートのみがBGPに再配布されます
- B. クラスフルネットワークのみがOSPFからBGPに再配布されます
- C. BGPコンバージェンスが遅いため、ルートは最終的にBGPテーブルに存在します
- D. デフォルトでは、内部OSPFルートのみがBGPに再配布されます

Answer: D (メッセージを残す)

セクション :レイヤー3テクノロジー

最新問題: 236

展示を参照してください。

```
ipv6 access-list INTERNET
permit ipv6 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA14::/64
permit tcp 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA13::/64 eq telnet
permit tcp 2001:DB8:AD59:BA21::/64 any eq http
permit ipv6 2001:DB8:AD59::/48 any
deny ipv6 any any log
```

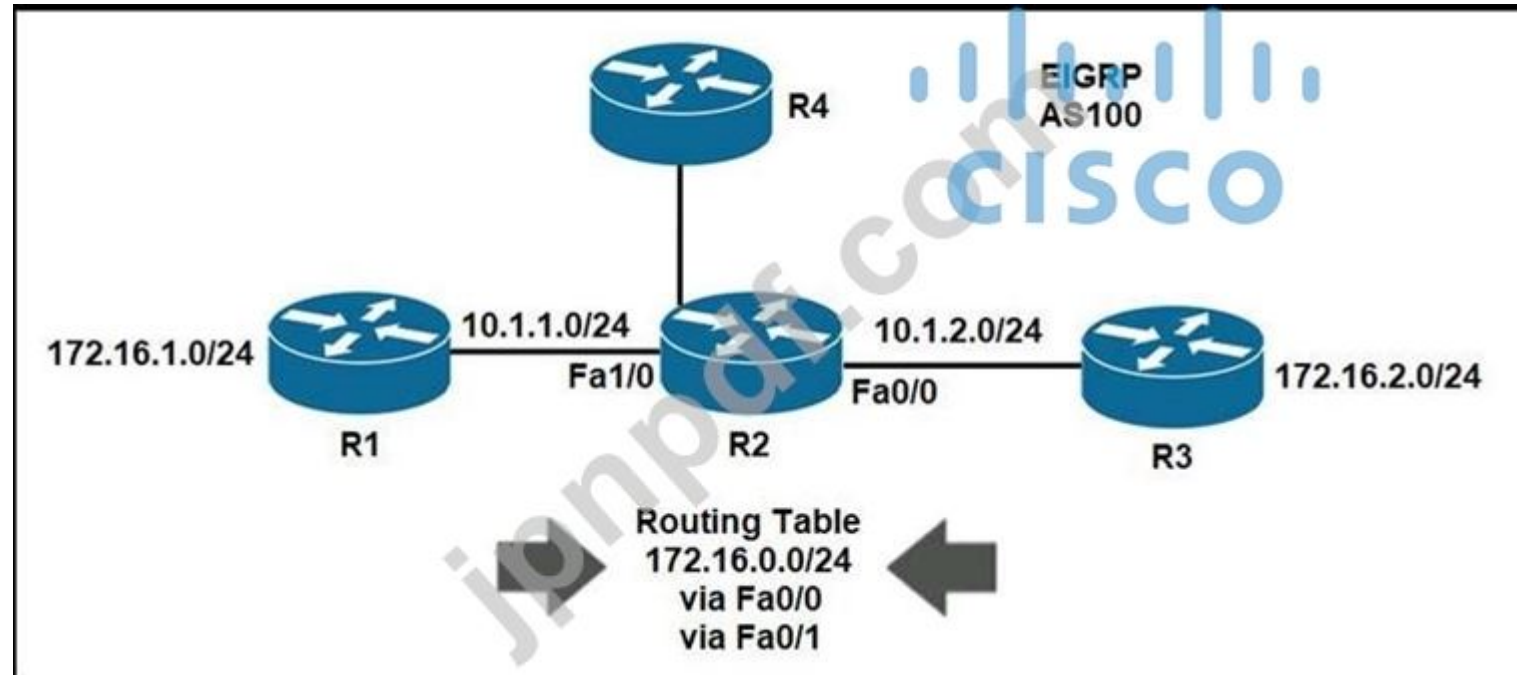
ルーターへのVTYアクセスを監視しているときに、エンジニアはルーターにフィルターがなく、ACLが構成されていても、ユーザー名とパスワードを使用して誰でもルーターにアクセスできることに気がきます。

この問題を解決するコマンドはどれですか？

- A. アクセスクラスのインターネット
 - B. ip access-group INTERNET in
 - C. ipv6 Traffic-filter INTERNET in
 - D. ipv6 access-class INTERNET in
- Answer: D ([メッセージを残す](#))

最新問題: 237

展示を参照してください。



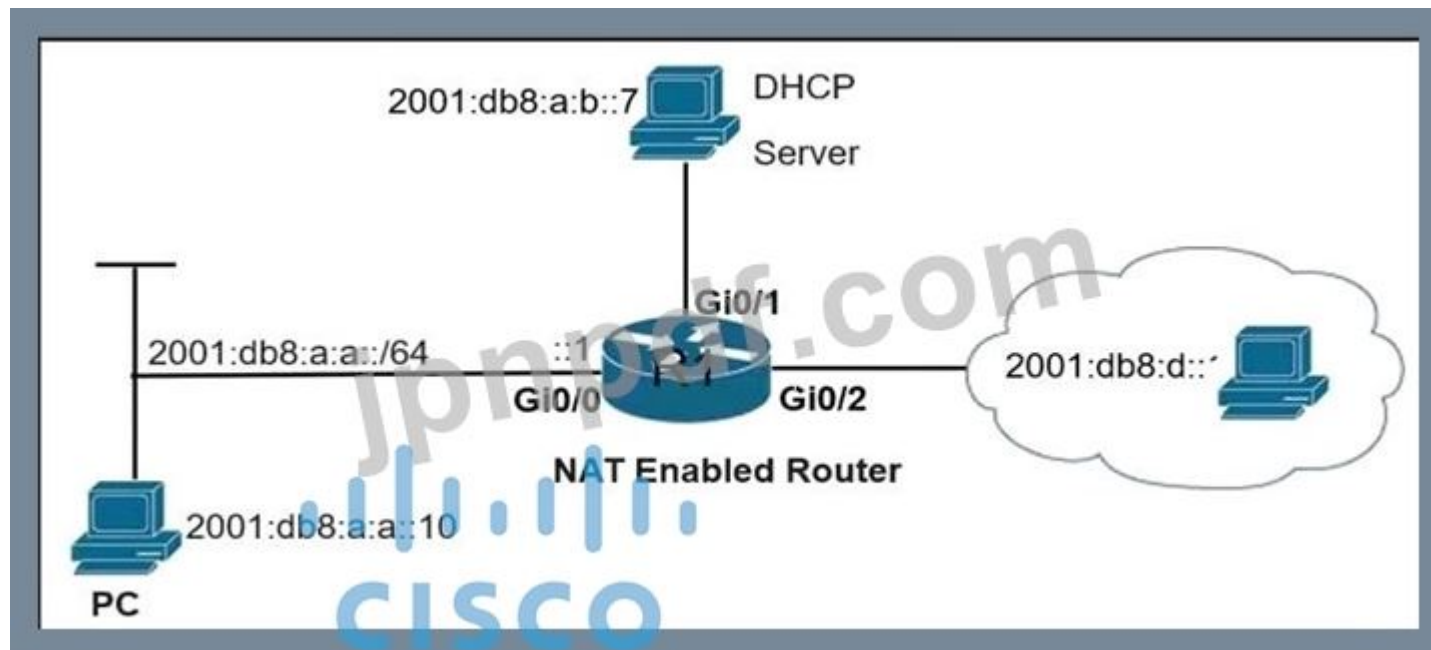
R2の背後にある172.16.2.7に到達しようとする、R4でパケットドロップが発生します。問題を解決するアクションはどれですか？

- A. 3つのルーターR1、R2、およびR3すべてで自動要約を有効にします
- B. メトリック254を使用してR2からR3に向かって/16のフローティング静的ルートを挿入します
- C. R2で自動要約を無効にする
- D. メトリック254を使用してR2からR3に向かって/24フローティング静的ルートを挿入します

Answer: ([解答を表示する](#))

最新問題: 238

展示を参照してください。



```

>>> PC ping 2001:db8:a:b::7
Pinging 2001:db8:a:b::7 with 32 bytes of data:
Reply from 2001:db8:a:b::7: time=46ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Ping statistics for 2001:db8:a:b::7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 46ms, Average = 41ms

```

```

R1# telnet 2001:db8:a:b::7
Trying 2001:DB8:A:B::7 ... Open
User Access Verification
Password:

```

```

R1# show ipv6 access-list TSHOOT
IPv6 access list TSHOOT
  permit tcp any host 2001:DB8:A:B::7 eq telnet (6 matches) sequence 10
  permit tcp host 2001:DB8:A:A::10 host 2001:DB8:A:B::7 eq telnet sequence 20
  permit tcp host 2001:DB8:A:A::10 host 2001:DB8:D::1 eq www sequence 30
  permit ipv6 2001:DB8:A:A::/64 any (67 matches) sequence 40

```

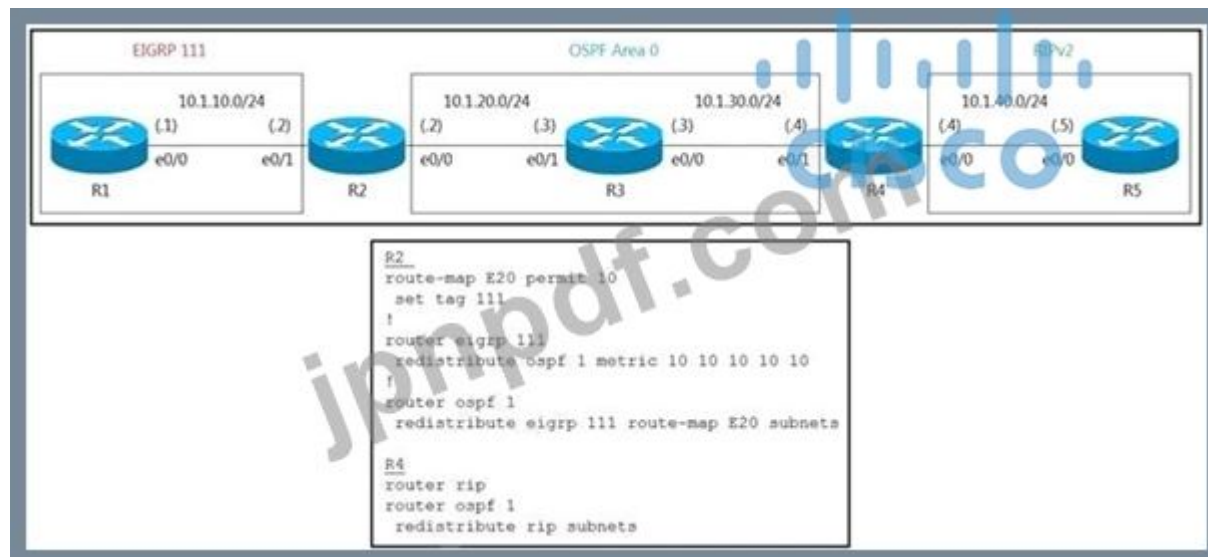
エンジニアが、PCからDHCPサーバーへの失敗したTelnetセッションのトラブルシューティングを行っています。問題を解決するアクションはどれですか？

- A. アクセスリストのシーケンス40のシーケンス20を削除して、Telnetを許可します。
- B. シーケンス20を削除し、シーケンス5としてIPv6トラフィックフィルターに追加し直します。
- C. シーケンス30を削除し、シーケンス5としてIPv6トラフィックフィルターに追加し直します。
- D. シーケンス10を削除してPCの送信元IPアドレスを追加し、シーケンス10として追加し直します。

Answer: B (メッセージを残す)

最新問題: 239

展示を参照してください。



R5は、EIGRPドメインで発信されたルートを受信しないようにする必要があります。問題を修正するためにR5ルーティングテーブルからEIGRPルートを削除する構成変更のセットはどれですか。

A. R4

ルートマップO2R拒否10

マッチタグ111

ルートマップO2R許可20

!

ルーターリップ

ospf1ルートマップO2Rメトリック1を再配布します

B. R2

ルートマップE20は20を拒否します

R4

ルートマップO2R拒否10

マッチタグ111

!

ルーターリップ

ospf1ルートマップO2Rメトリック1を再配布します

C. R4

ルートマップO2R許可10

マッチタグ111

ルートマップO2Rは20を拒否します

!

ルーターリップ

ospf1ルートマップO2Rメトリック1を再配布します

D. R4

ルートマップO2R拒否10

マッチタグ111

!

ルーターリップ

ospf1ルートマップO2Rメトリック1を再配布します

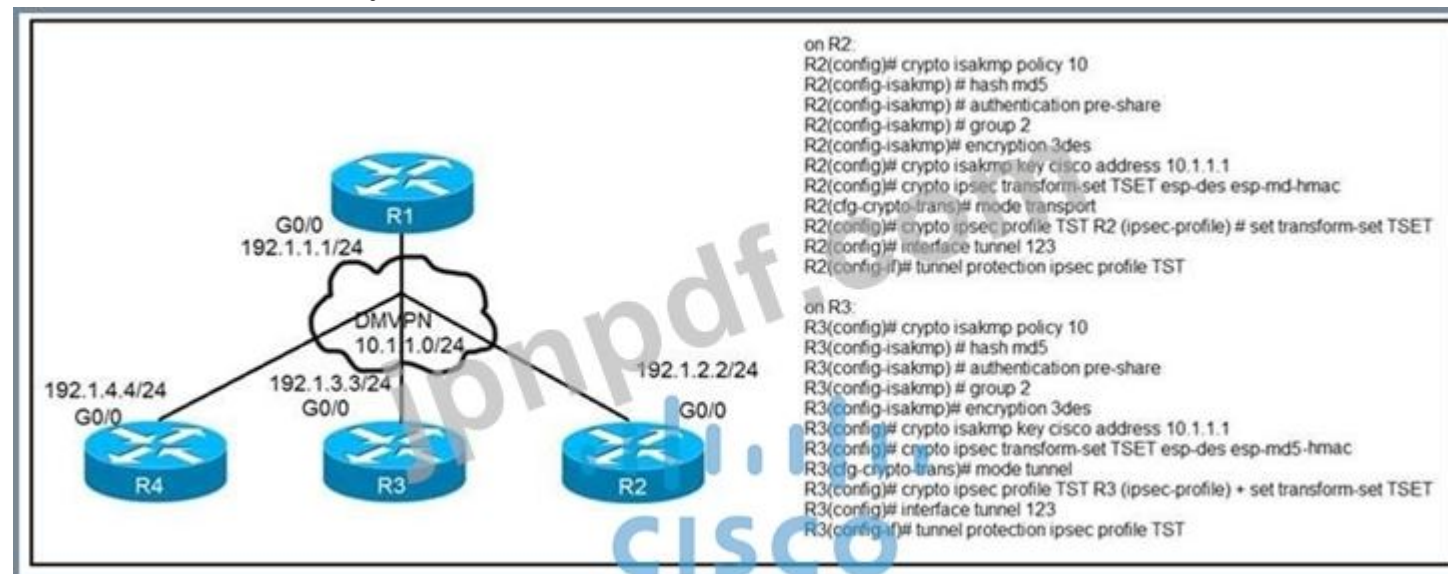
Answer: (解答を表示する)

この質問では、EIGRPドメインからのルートがOSPF タグ111を使用)、次にRIPv2に再配布されますが、フィルタリングは行われなため、R5はEIGRPドメインとOSPFドメインの両方からすべてのルートを学習します。R5にOSPFドメインからのルートのみを学習させたい場合は、タグ111を使用してルートを除外し、他のルートを許可する必要があります。

foute-mapO2Rpermit20」という行は、各ルートマップの最後にすべてが暗黙的に拒否されるため、他のルートを許可するために重要です。

最新問題: 240

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確認しました。問題を解決する2つのアクションはどれですか？ 2つ選択してください。)

- A. R2およびR3でcrypto isakmpkeyciscoアドレス0.0.0.0を設定します。
- B. R2およびR3の暗号isakmpキーCiscoアドレス10.1.1.1を削除します
- C. モードをモードトランスポートからR2のモードトンネルに変更します。
- D. R3でモードをモードトンネルからモードトランスポートに変更します
- E. R2およびR3でcrypto isakmpkeyciscoアドレス192.1.1.1を設定します

Answer: A,C (メッセージを残す)

最新問題: 241

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、メンテナンス中にリンクAからASNへのリンクAを介したバックアップリンクが存在するように、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トラフィックを削除する必要があります。

R1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A

B. オプションD

C. オプションB

D. オプションC

Answer: ([解答を表示する](#))

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をGETする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **242**

展示を参照してください。

```
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
```

この構成を適用した結果はどうなりますか？

- A. ルータは、次の名前のアクセスリストと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」。
- 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す。
- C. ルーターは、次の名前のアクセスリストと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。
BGP」。
- D. ルータは他のデバイスとBGPネイバーシップを形成できません。

Answer: ([解答を表示する](#))

最新問題: 243

同じインターフェイスを経由して同じネクストホップを経由し、同じキューイングポリシーを持つMPLS LSPのパケットをマッピングするために使用されるテーブルはどれですか？

- A. 自民党
- B. CEF
- C. FEC
- D. RIB

Answer: C ([メッセージを残す](#))

最新問題: 244

展示を参照してください。

```
R1(config)#route-map ADD permit 20
R1(config-route-map)#set tag 1

R1(config)#router ospf1
R1(config-router)#redistribute rip subnets route-map ADD
```

R1について正しい説明はどれですか。

- A. OSPFは、タグが1の場合にのみRIPルートを再配布します。
- B. R1は、OSPFに再配布する前に、RIPで学習したルートのメトリックに1を追加します。
- C. RIPで学習したルートは、タグ値1でOSPFに配布されます。
- D. RIPルートは変更なしでOSPFに再配布されます。

Answer: C ([メッセージを残す](#))

最新問題: 245

別紙を参照してください。

```
Jan 9 15:29:29.713: DHCP_SNOOPING: process new DHCP packet, message type: DHCPINFORM, input interface: Po2, MAC da: ffff.ffff.ffff, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0
Jan 9 15:29:29.713: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (1)
Jan 9 15:29:29.722: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan1.
Jan 9 15:29:31.509: DHCP_SNOOP(hlrm_set_if_input): Setting if_input to Po2 for pak. Was V11
Jan 9 15:29:31.509: DHCP_SNOOP(hlrm_set_if_input): Setting if_input to V11 for pak. Was Po2
Jan 9 15:29:31.509: DHCP_SNOOP(hlrm_set_if_input): Setting if_input to Po2 for pak. Was V11
Jan 9 15:29:31.517: DHCP_SNOOPING: received new DHCP packet from input interface (Port-channel2)
```

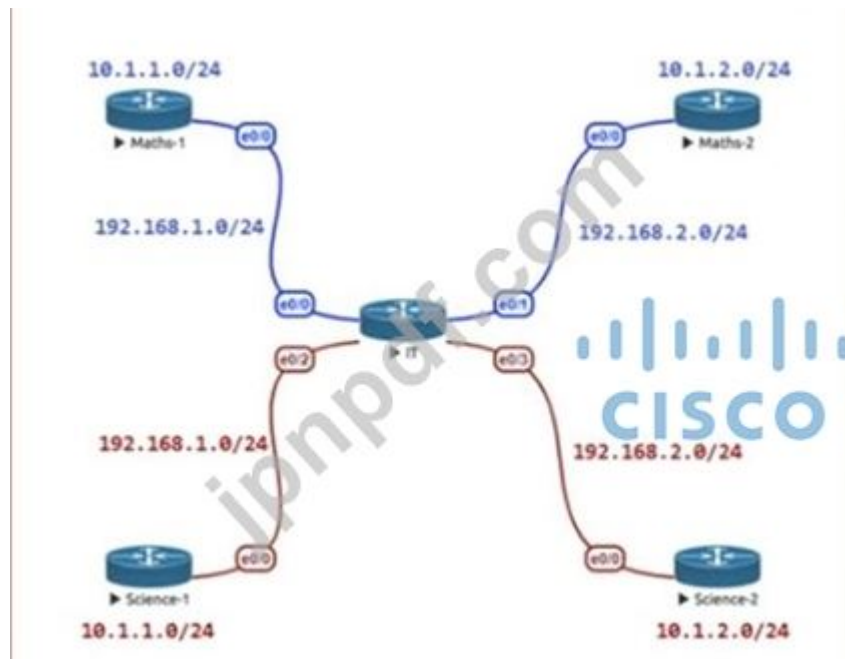
ネットワーク管理者は、Cisco Catalyst 3750-XスイッチでDHCPスヌーピングを有効にし、アップリンクポート (Port-channel2)を信頼できるポートとして設定します。クライアントはIPアドレスを受信していませんが、DHCPスヌーピングが無効になっている場合、クライアントはIPアドレスの受信を開始します。どのグローバルコマンドが問題を解決しますか？

- A. ip dhcp snooping
- B. ipdhcpリレー情報trustportchannel2
- C. IPDHCPスヌーピング情報オプションなし
- D. ip dhcp snooping trust

Answer: C ([メッセージを残す](#))

最新問題: 246

展示を参照してください。



数学部門と科学部門は企業のITルーターを介して接続しますが、数学部門のユーザーは科学部門にアクセスできないようにする必要があります。その逆も同様です。このタスクを実行する構成はどれですか。

A)

```

vrf definition Science
 address-family ipv4
 !
 interface E 0/2
  vrf forwarding Science
  ip address 192.168.1.1 255.255.255.0
  no shut
 !
 interface E 0/3
  vrf forwarding Science
  ip address 192.168.2.1 255.255.255.0
  no shut

```

B)

```

vrf definition Science
 address-family ipv4
 !
 interface E 0/2
  ip address 192.168.1.1 255.255.255.0
  no shut
 !
 interface E 0/3
  ip address 192.168.2.1 255.255.255.0
  no shut

```

C)

```

vrf definition Science
 !
 interface E 0/2
  ip address 192.168.1.1 255.255.255.0
  no shut
 !
 interface E 0/3
  ip address 192.168.2.1 255.255.255.0
  no shut

```

D)

```
⓪ vrf definition Science
  address-family ipv4
  !
  interface E 0/2
  ip address 192.168.1.1 255.255.255.0
  vrf forwarding Science
  no shut
  !
  interface E 0/3
  ip address 192.168.2.1 255.255.255.0
  vrf forwarding Science
  no shut
```

A. オプションB

B. オプションC

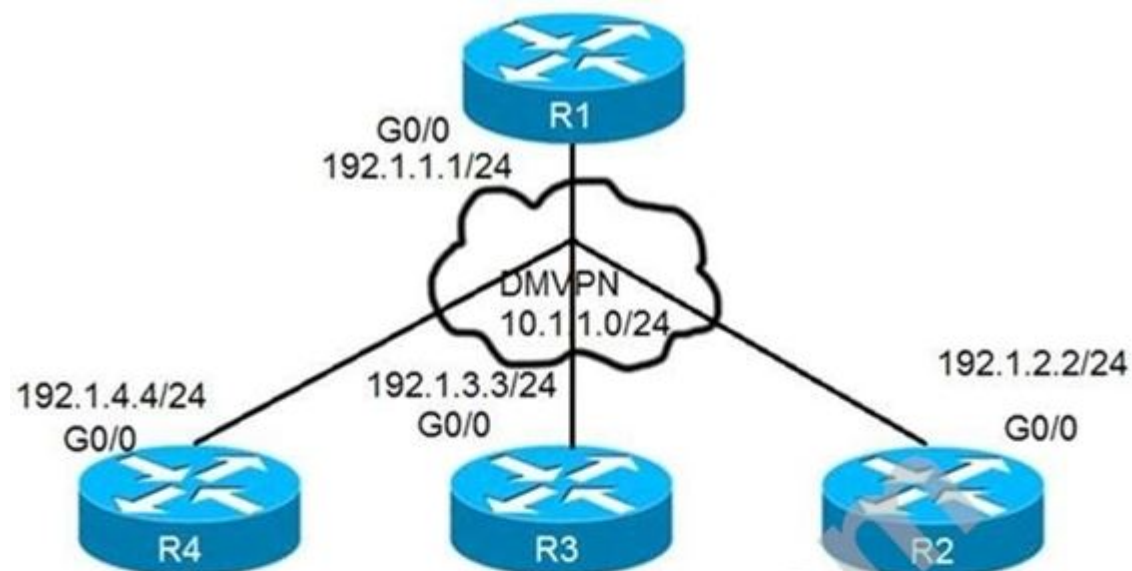
C. オプションD

D. オプションA

Answer: C ([メッセージを残す](#))

最新問題: **247**

展示品をご覧ください。



```

On R1:
R1(config)# interface tunnel 1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# tunnel source 192.1.1.1
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# ip nhrp network-id 111

```

```

On R2:
R2(config)# interface tunnel 1
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# tunnel source FastEthernet0/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# ip nhrp network-id 222
R2(config-if)# ip nhrp nhs 10.1.1.1
R2(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

```

```

On R3:
R3(config)# interface tunnel 1
R3(config-if)# ip address 10.1.1.3 255.255.255.0
R3(config-if)# tunnel source FastEthernet0/0
R3(config-if)# tunnel mode gre multipoint
R3(config-if)# ip nhrp network-id 333 R3(config-if)# ip nhrp nhs 10.1.1.1
R3(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

```

```

On R4: R4(config)# interface tunnel 1
R4(config-if)# ip address 10.1.1.4 255.255.255.0
R4(config-if)# tunnel source FastEthernet0/0
R4(config-if)# tunnel mode gre multipoint
R4(config-if)# ip nhrp network-id 444
R4(config-if)# ip nhrp nhs 10.1.1.1
R4(config-if)# ip nhrp map 10.1.1.1 192.1.1.1

```

DMVPNのスポークツースポーク間にフェーズ3トンネルを確立することはできません。欠落している2つのコマンドはどれですか？ 2つ選択してください。)

- A. スポークルータにipnhrpショートカットコマンドがありません。
- B. ハブルータにip nhrpredirectコマンドがありません。
- C. ハブルータにip nhrpmapコマンドがありません。
- D. スポークルータにip nhrpredirectコマンドがありません。
- E. ハブルータにipnhrpショートカットコマンドがありません。

Answer: ([解答を表示する](#))

最新問題: 248

操作を左から右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を実行します

ラベルエッジルーター :1ラベルとラベルなし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: 249

展示を参照してください。

```
aaa new-model
aaa group server radius RADIUS-SERVERS
aaa authentication login default group RADIUS-SERVERS local
aaa authentication enable default group RADIUS-SERVERS enable
aaa authorization exec default group RADIUS-SERVERS if-authenticated
aaa authorization network default group RADIUS-SERVERS if-authenticated
aaa accounting send stop-record authentication failure
aaa session-id common
!
line con 0
logging synchronous
stopbits 1
line vty 0 4
logging synchronous
transport input ssh
```

ネットワーク管理者は、RADIUSサーバーからSSHを使用してスイッチに正常にログインします。ネットワーク管理者がコンソールポートを使用してスイッチにアクセスすると、RADIUSサーバーはshell priv-lvl = 15"を返し、スイッチはenableコマンドの入力を要求します。コマンドが入力されると、拒否されます。この問題のトラブルシューティングと予約に使用されるコマンドセットはどれですか。

A. line con 0

AAA認証コンソール

承認幹部

!

行vty04

トランスポート入力ssh

B. line con 0

AAA認証コンソール

承認priv15

!

行vty04

トランスポート入力ssh

C. line con 0

AAA許可コンソールpriv15

!

行vty04

承認幹部

D. line con 0

AAA認証コンソール

！

行vty04


承認幹部

Answer: ([解答を表示する](#))

最新問題: 250

展示を参照してください。

```
R1#sh run | s bgp
router bgp 65001
no synchronization
bgp router-id 10.100.1.50
bgp log-neighbor-changes
network 10.1.1.0 mask 255.255.255.252
network 10.1.1.12 mask 255.255.255.252
network 10.100.1.50 mask 255.255.255.255
timers bgp 20 60
neighbor R2 peer-group
neighbor R4 peer-group
neighbor 10.1.1.2 remote-as 65001
neighbor 10.1.1.2 peer-group R2
neighbor 10.1.1.14 remote-as 65001
neighbor 10.1.1.14 peer-group R4
no auto-summary
```



BGPルートリフレクタ設定のトラブルシューティング中に、エンジニアは、リフレクトされたルートが隣接ルータから欠落していることに気が付きます。問題を解決するために必要な2つのBGP構成はどれですか？ 2つ選択してください)

- A. ネイバー10.1.1.14route-reflector-client
- B. ネイバー10.1.1.2route-reflector-client
- C. ネイバー10.1.1.2allowas-in
- D. ネイバーR2ルートリフレクタクライアント
- E. ネイバーR4ルートリフレクタクライアント

Answer: ([解答を表示する](#))

最新問題: 251

レイヤ3MPLSVPNでIPv4およびVPNv4アドレスファミリ構成を使用する2つの目的は何ですか？ (2つ選択してください。)

- A. VPNv4アドレスは、MPLSVPNラベルをアドバタイズするために使用されます。

- B. RDはIPv4ルートの前に付加され、一意になります。
- C. MP-BGPは、顧客間で重複するIPv4アドレスがネットワークを介してアドバタイズできるようにするために使用されます。
- D. MPLSラベルにタグを付けるにはIPv4アドレスが必要です。
- E. VPNv4アドレスは、IPv4プレフィックスの前に付加される64ビットルート識別子で構成されます。

Answer: B,E ([メッセージを残す](#))

説明

VPNv4アドレスは、IPv4プレフィックスの前に付けられた64ビットのRoute Distinguisher (RD)で構成されます。これは、異なるVRFにあるルートを一意にするためです。

最新問題: 252

OSPFv3アドレスファミリー構成のOSPFv3プロセスにIPv4インターフェイスを追加する構成はどれですか。

- A. ルーター ospfv3 1
アドレスファミリー ipv4ユニキャスト
- B. Router (config-router) #ospfv3 1 ipv4 area 0
- C. Router (config-if) #ospfv3 1 ipv4 area 0
- D. ルーター ospfv3 1
アドレスファミリー ipv4

Answer: B ([メッセージを残す](#))

最新問題: 253

VRFインスタンスの2つの特徴は何ですか？ (2つ選択してください。)

- A. すべてのVRFは、顧客のルーティングテーブルとCEFテーブルを共有します。
- B. インターフェイスは1つのVRFに関連付けられている必要があります。
- C. 各VRFには、異なるルーティングテーブルとCEFテーブルのセットがあります
- D. Pデバイスに接続されたカスタマーサイトのVPNメンバーシップによって定義されます。
- E. 顧客サイトをさまざまなVRFに関連付けることができます

Answer: (解答を表示する)

参照 :

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-s/mp-l3-vpns-15-s-book/mp-bgp- mpls-vpn.pdf

最新問題: 254

展示を参照してください。

```
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) #
```

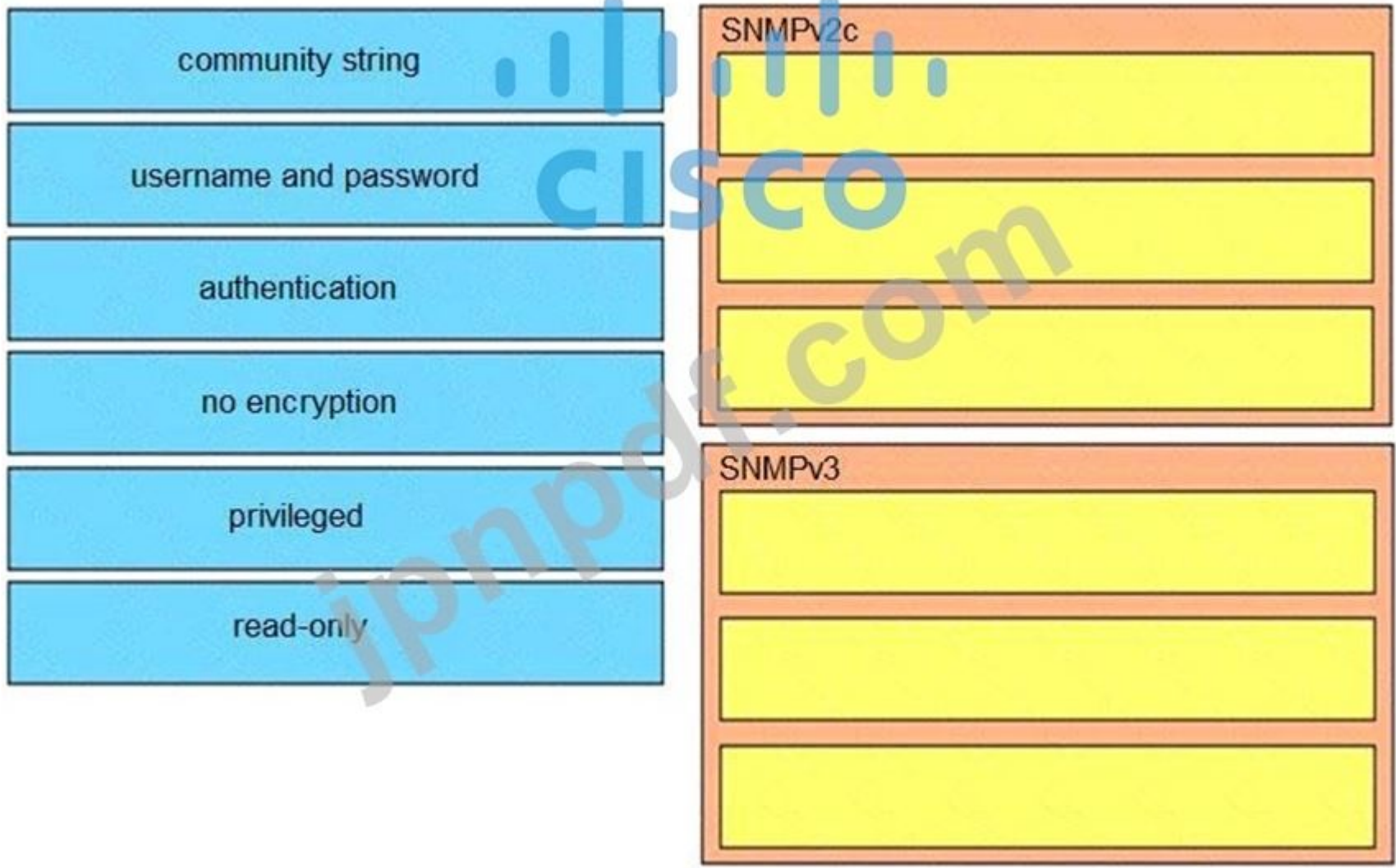
コンソールに接続している管理者は、リモートユーザーがログインしたときにデバッグメッセージを表示しません。リモートログインのデバッグメッセージが確実に表示されるようにするアクションはどれですか。

- A. `aaanew-model`構成コマンドを入力します。
- B. `loggingconsole`デバッグ設定コマンドを入力します。
- C. `terminalmonitorexec`コマンドを入力します。
- D. `transportinputssh`コンフィギュレーションコマンドを入力します。

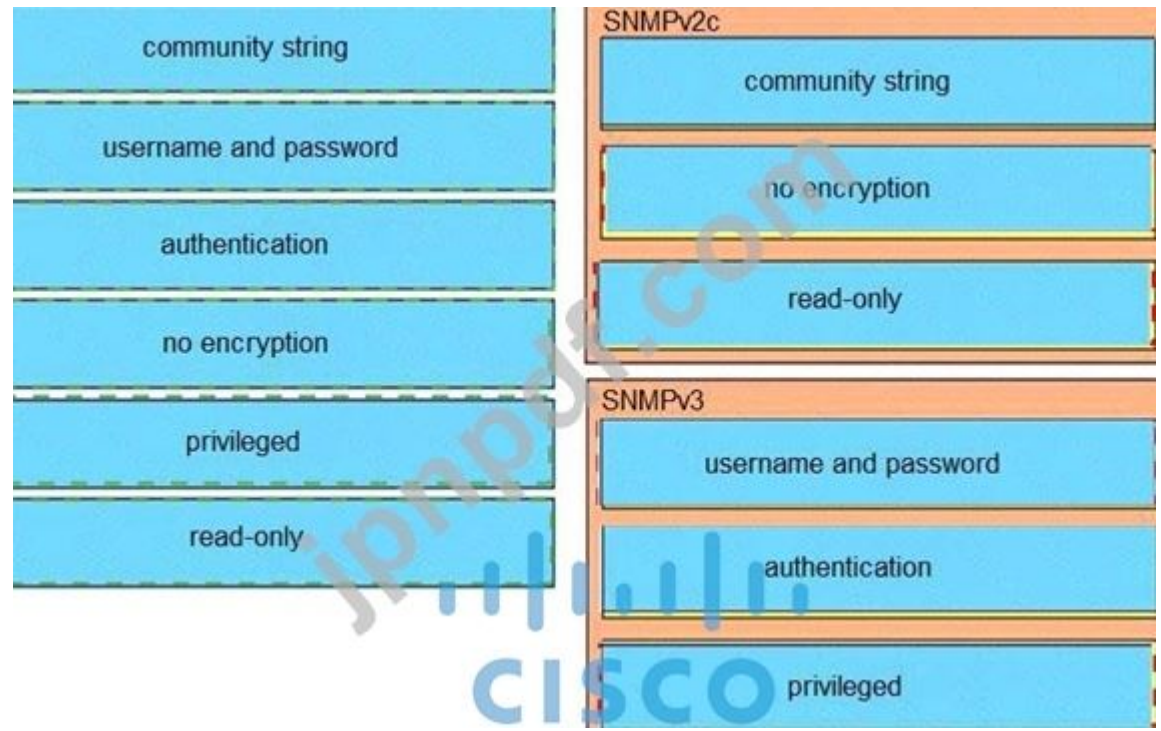
Answer: B ([メッセージを残す](#))

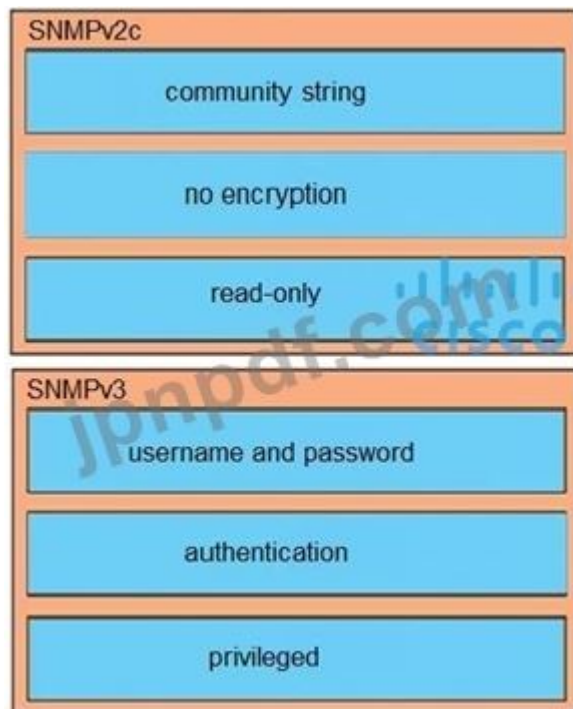
最新問題: 255

Cisco IOSデバイスのSNMP属性を左側から、右側の正しいSNMPv2cまたはSNMPV3カテゴリにドラッグアンドドロップします。



Answer:





最新問題: 256

展示を参照してください。

```
Cat3850-Stack-2# show policy-map
```

```
Policy Map LIMIT_BGP
```

```
Class BGP
```

```
drop
```

```
Policy Map SHAPE_BGP
```

```
Class BGP
```

```
Average Rate Traffic Shaping  
cir 10000000 (bps)
```

```
Policy Map POLICE_BGP
```

```
Class BGP
```

```
police cir 1000k bc 1500  
conform-action transmit  
exceed-action transmit
```

```
Policy Map COPP
```

```
Class BGP
```

```
police cir 1000k bc 1500  
conform-action transmit  
exceed-action drop
```

CPU宛てのBGPトラフィックを1Mbpsに制限し、より高速で送信されるBGPトラフィックを無視するコントロールプレーンポリシーはどれですか。

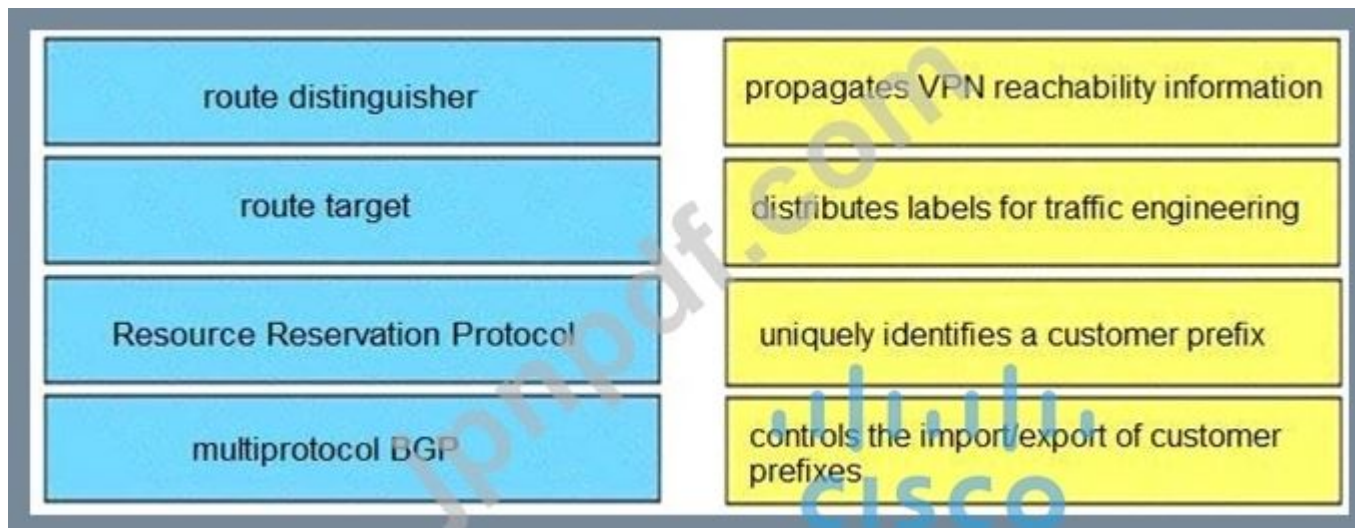
- A. ポリシーマップPOLICE_BGP
- B. ポリシーマップSHAPE_BGP
- C. ポリシーマップLIMIT_BGP
- D. ポリシーマップCOPP

Answer: D ([メッセージを残す](#))

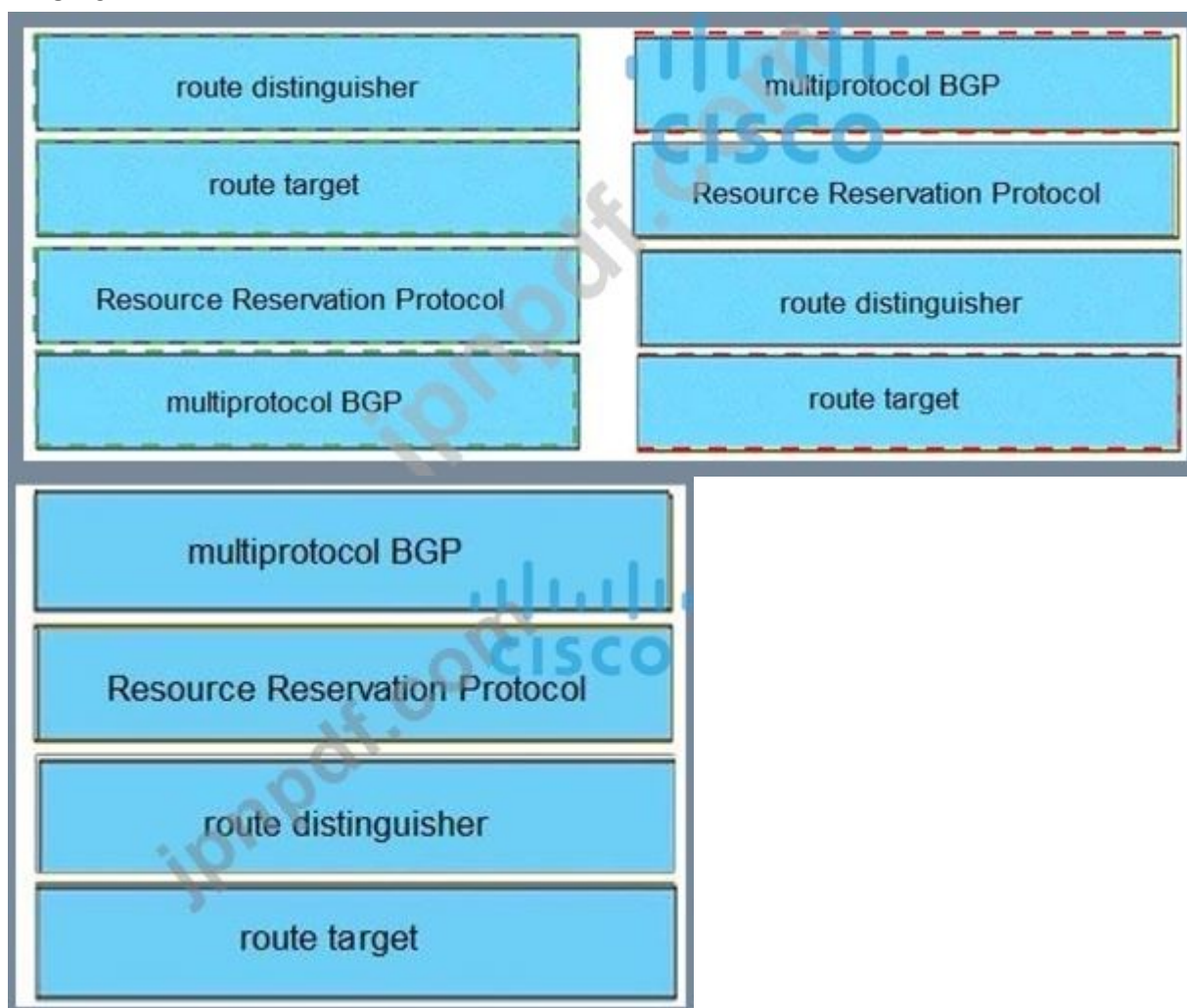
有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 257

MPLS VPNの概念を左から、右の正しい説明にドラッグアンドドロップします。

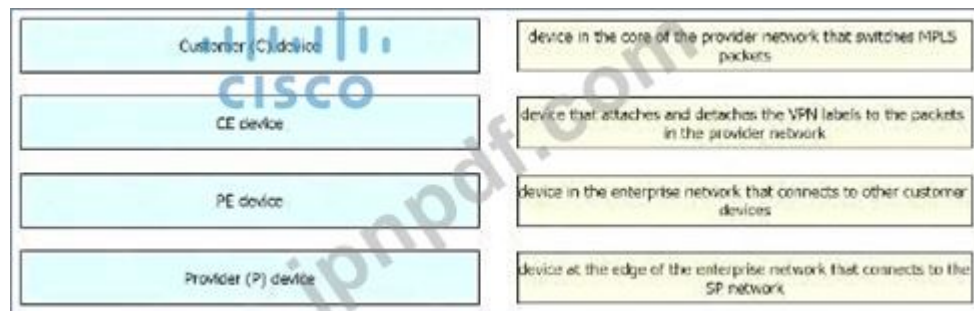


Answer:



最新問題: 258

MPLSVPNデバイスタイプを左から右の定義にドラッグアンドドロップします。

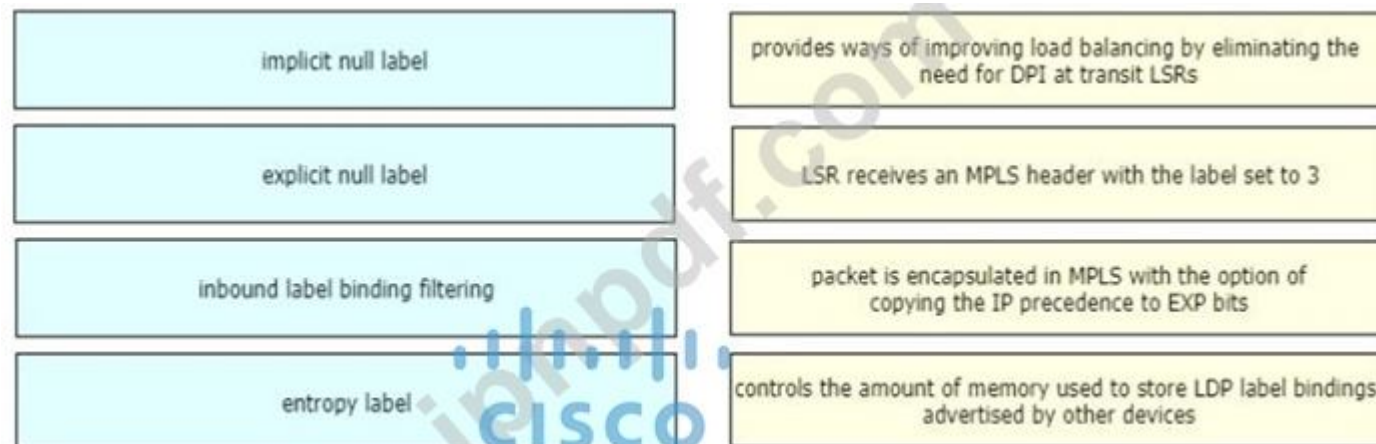


Answer:



最新問題: 259

LDP機能を左から右の説明にドラッグアンドドロップします



Answer:



参照 :

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/15-sy/mp-ldp-15-sy-book/mp-ldp-inbound-filtr.html

最新問題: 260

展示を参照してください。

```

Router#show ip bgp vpv4 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-client)
 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

```

エンジニアがBGPを設定し、現在の最適なパスではなく、10.77.255.57からのパスを最適なパスとして選択したいと考えています。問題を解決するアクションはどれですか？

- A. 現在の最適なパスのAS_PATHプリペンドを構成します
- B. 最適なパスとして選択するように上位のMEDを構成します
- C. 目的の最適なパスのAS_PATHプリペンドを構成します
- 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: D (メッセージを残す)

説明

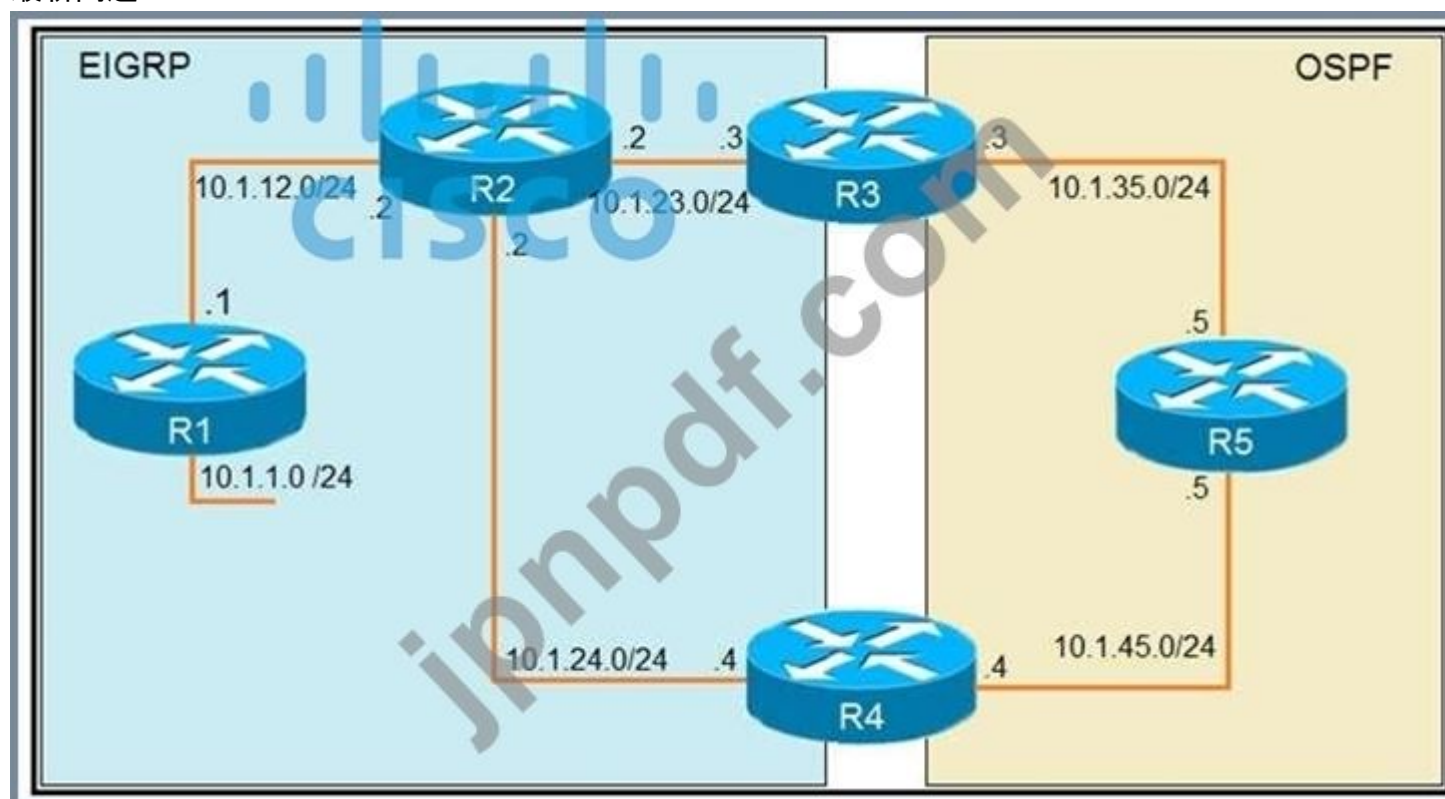
出力から、現在の最適なパスは10.57.255.11 ("... valid、confed-external、best"を含む)からであり、このパスは2 AS (64955 65003) 離れていることがわかります。ASが1つしかないパス (たとえば、172.16.254.234からのパス)がいくつかありますが、それらは最適なパスとして選択されなかったため、AS_PATHを使用して最適なパスを決定しませんでした-回答Aと回答Cは正しくありません。

出力のすべてのパスのメトリックは0であり、これはこの属性の最小(最良)値です。より高いMEDを構成すると、他のパスよりも優先されな

くなります-回答Bは正しくありません。

回答Dのみが残りますが、LOCAL_PREF属性はより高い値で構成する必要があるため、ここでの「より低いLOCAL_PREF」はより高い値を意味することを願っています。しかし、これが最良の答えです。

最新問題: 261



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
```

展示品をご覧ください。R5からネットワーク10.1.1.0/24に到達可能性を提供するために、ネットワーク管理者はEIGRPをR3のOSPFに再配布しますが、R4がR5を介して到達するために最適ではないパスを使用していることに気がきます。

10.1.1.0/24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、問題を修正するアクションはどれですか？

- A. 外部EIGRPの管理距離を90に変更します。
- B. OSPFのR4に向けてR5のアウトバウンド配布リストを適用します。
- C. R5でOSPFの管理距離を200に変更します。
- D. OSPFをR4のEIGRPに再配布します。

Answer: A ([メッセージを残す](#))

セクション：混合質問

最新問題: 262

MPLSレイヤ3VPNサービスはどのように展開されますか？

- A. RDとRTの値はVRFの下で一致する必要があります。
- B. VRFでのインポートとエクスポートのRT値は常に同じである必要があります。
- C. ラベルスイッチパスは、ローカルPEルータとリモートPEルータの間で使用可能である必要があります。
- D. VRFでのRD値とRT値は、リモートPEルータで一致する必要があります。

Answer: C ([メッセージを残す](#))

セクション：混合質問

最新問題: 263

MPLSVPNデバイスタイプを左から右の定義にドラッグアンドドロップします。

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:



最新問題: 264

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スタッフが通常の営業時間内にオフィスに来て、SSH経由でデバイスにアクセスできないこの問題を解決するには、どの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。

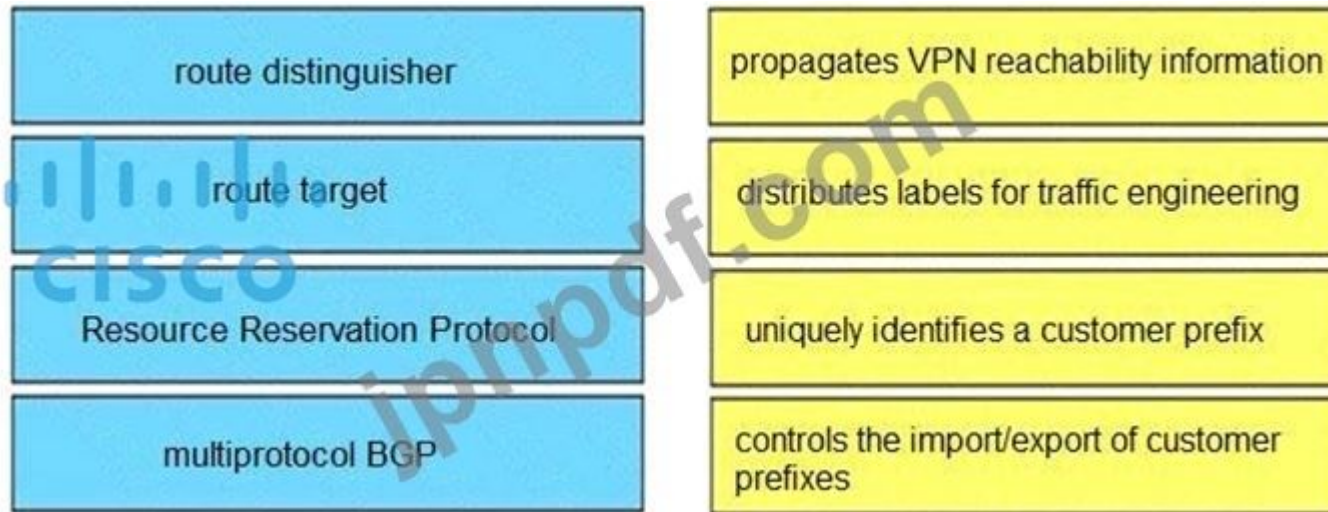
Answer: A ([メッセージを残す](#))

説明

ACLに許可する必要がありますtcp10110.1.1.1 0.0.0.0

最新問題: 265

MPLS VPNの概念を左から、右の正しい説明にドラッグアンドドロップします。



Answer:



```
R1(config)#route-map ADD permit 20
R1(config-route-map)#set tag 1

R1(config)#router ospf1
R1(config-router)#redistribute rip subnets route-map ADD
```

展示を参照してください。R1について正しい説明はどれですか。

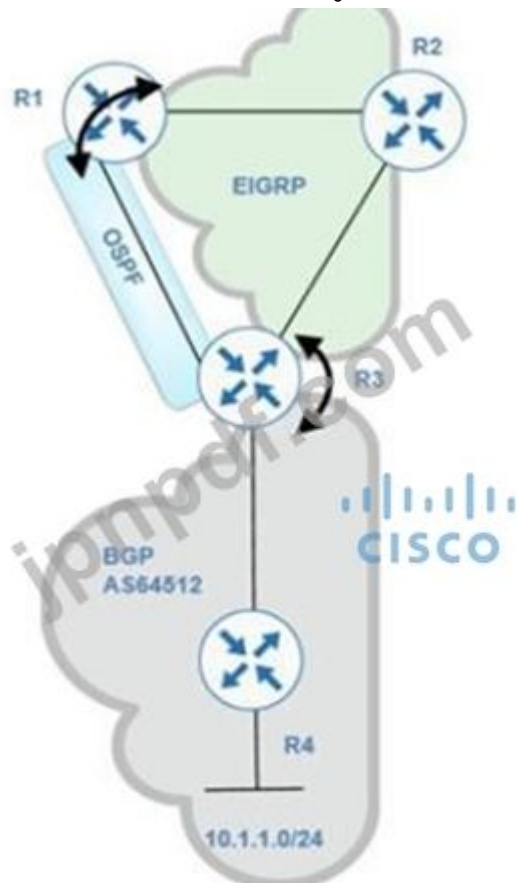
- A. OSPFは、タグが1の場合にのみRIPルートを再配布します。
- B. RIPで学習したルートは、タグ値1でOSPFに配布されます。
- C. R1は、OSPFに再配布する前に、RIPで学習したルートのメトリックに1を追加します。
- D. RIPルートは変更なしでOSPFに再配布されます。

Answer: ([解答を表示する](#))

セクション : レイヤー3テクノロジー

最新問題: 267

出品物をご参照ください。



ルーティングプロトコルは、R3とR1で相互に再配布されます。ユーザーは、10.1.1.0/24プレフィックスでホストされているサービスへの断続的な接続を報告します。show ip route profileコマンドを実行すると、R3でルーティングアップデートの大幅な変更が通知されます。サービスをどのように安定させる必要がありますか？

- A. BGPの使用に関する問題は、別のプロトコルを使用してR3のEIGRPに再配布することで解決する必要があります。
- B. R3でiBGPの管理距離を200から100に減らすことにより、ルーティンググループを修正する必要があります
- C. R3でOSPFの管理距離を110から80に減らすことにより、ルーティンググループを修正する必要があります
- D. iBGPの使用に関する問題は、R3とR4の間でeBGPを実行することで修正する必要があります

Answer: [\(解答を表示する\)](#)

説明

再配布後、R3は2つのパスを介してネットワーク10.1.1.0/24について学習します。+内部BGP (BGP) ADが200 およびメトリック0)のR4からアドバタイズされます+ OSPF ADが110 (E2)のR1からアドバタイズされます および20)したがって、R3はOSPFを介してADが低いパスを選択します
ただし、これはR3-> R2->R1->R3から受信されるループパスです。したがって、R4からアドバタイズされたルートが期限切れになると、ループされたパスもすぐに期限切れになり、R3はR4からのメインパスを再インストールします。これが断続的な接続の原因です。この問題を解決するために、iBGPのADを110未満の値に下げて、OSPFアドバタイズされたルートよりも優先されるようにすることができます。

最新問題: 268

```
router# show ip route
.....
D 192.168.32.0/19 [90/25789217] via 10.1.1.1
R 192.168.32.0/24 [120/4] via 10.1.1.2
O 192.168.32.0/26 [110/229840] via 10.1.1.3
```

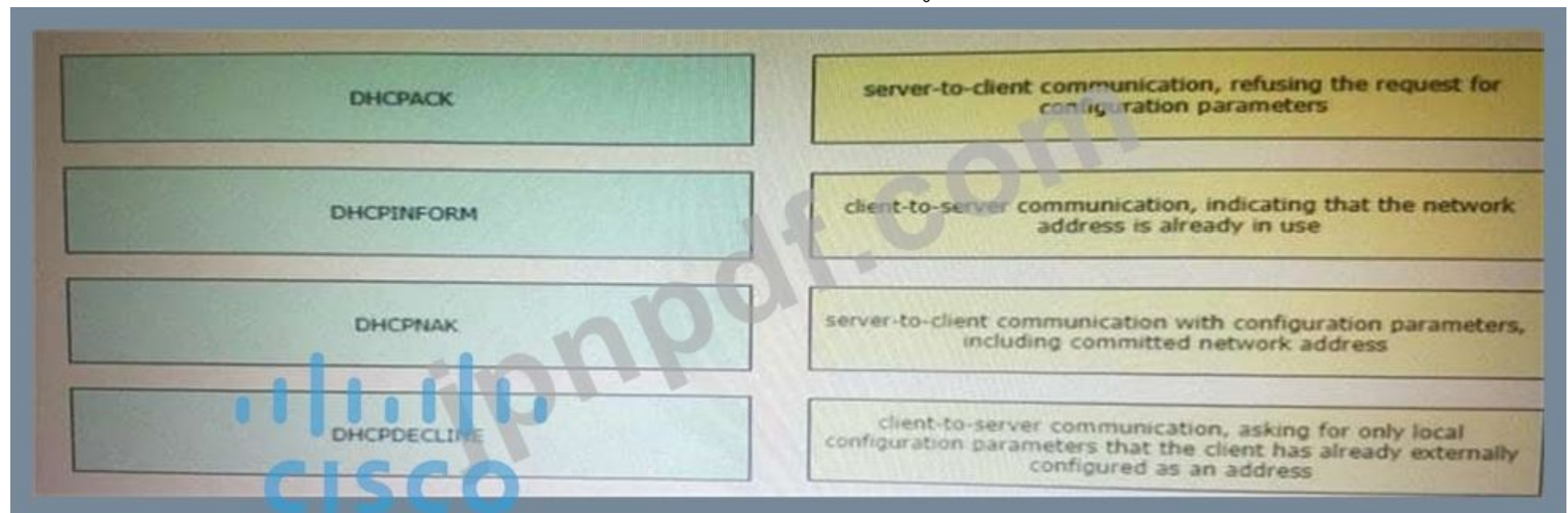
展示を参照してください。エンジニアが192.168.32.100を10.1.1.1経由で転送しようとしていますが、10.1.1.2経由で転送されました。10.1.1.1を介してパケットを転送するアクションは何ですか？

- A. /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。
- B. プレフィックスが/24以上の192.168.32.0ルートを受信するようにEIGRPを設定します。
- C. 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。
- D. より低いメトリックで192.168.32.0ルートを受信するようにEIGRPを設定します。

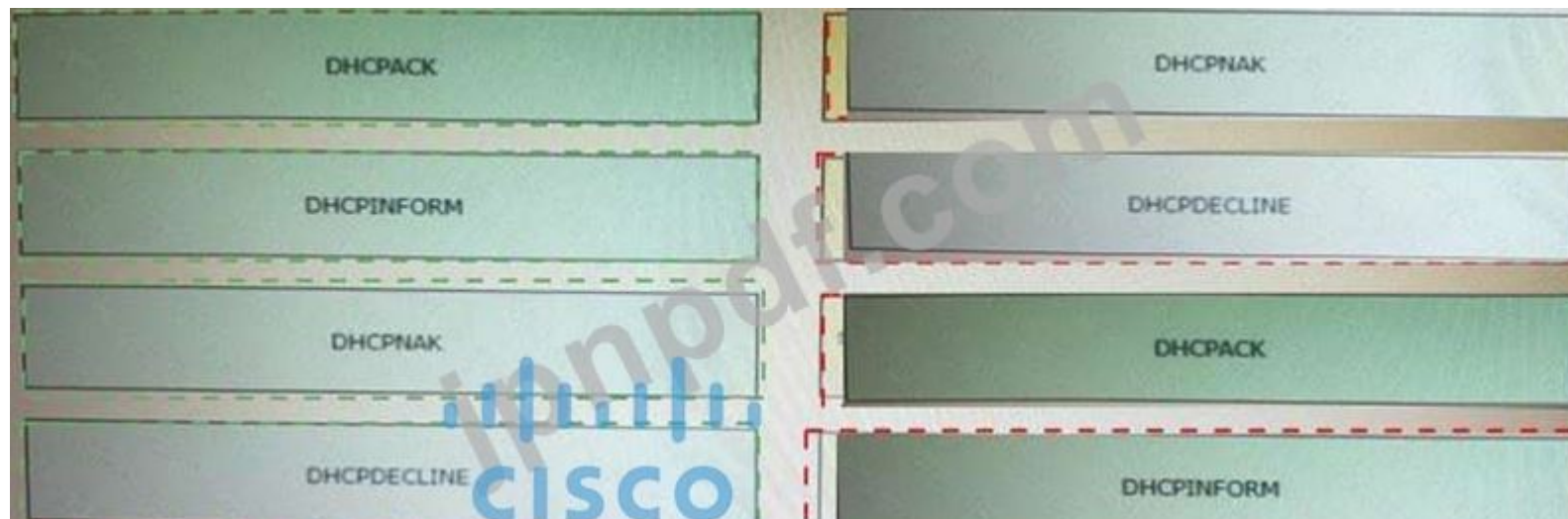
Answer: [B \(メッセージを残す\)](#)

最新問題: 269

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



Answer:



説明

DHCPACK=コミットされたネットワークアドレスを含む構成パラメーターを使用したサーバーからクライアントへの通信。

DHCPINFORM =クライアントからサーバーへの通信。クライアントがすでに外部でアドレスとして構成している、ローカル構成パラメーターのみを要求します。

DHCPNAK =サーバーからクライアントへの通信、構成パラメーターの要求を拒否します。

DHCPDECLINE =クライアントからサーバーへの通信。これは、ネットワークアドレスがすでに使用されていることを示します。

最新問題: 270

MPLSVPN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。

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: 271

展示を参照してください。

```
TAC+: TCP/IP open to 171.68.118.101/49 failed --
Destination unreachable; gateway or host down
AAA/AUTHEN (2546660185): status = ERROR
AAA/AUTHEN/START (2546660185): Method=LOCAL
AAA/AUTHEN (2546660185): status = FAIL
As1 CHAP: Unable to validate Response. Username chapuser: Authentication failure
```

ユーザー認証が拒否されるのはなぜですか？

- A. TACACS +サーバーは「ユーザー」を予期していますが、NTクライアントは「ドメイン/ユーザー」を送信します。
- B. TACACS +サーバーがダウンしており、ユーザーはローカルデータベースにいます。
- C. ユーザーがCHAP用に設定されているため、TACACS+サーバーはユーザーを拒否します。
- D. TACACS +サーバーがダウンしており、ユーザーはローカルデータベースにありません。

Answer: D (メッセージを残す)

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (80030%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 272

展示を参照してください。

```

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, s stale, m multipath, b backup-path, f FIB failure,
               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   MsRcvd  MsgSent  Tblver  InQ  OutQ  Up/Down  State/PfxRcd
192.168.2.2   4     65000    8         7         4    0    0  00:03:08      0

R3#

```

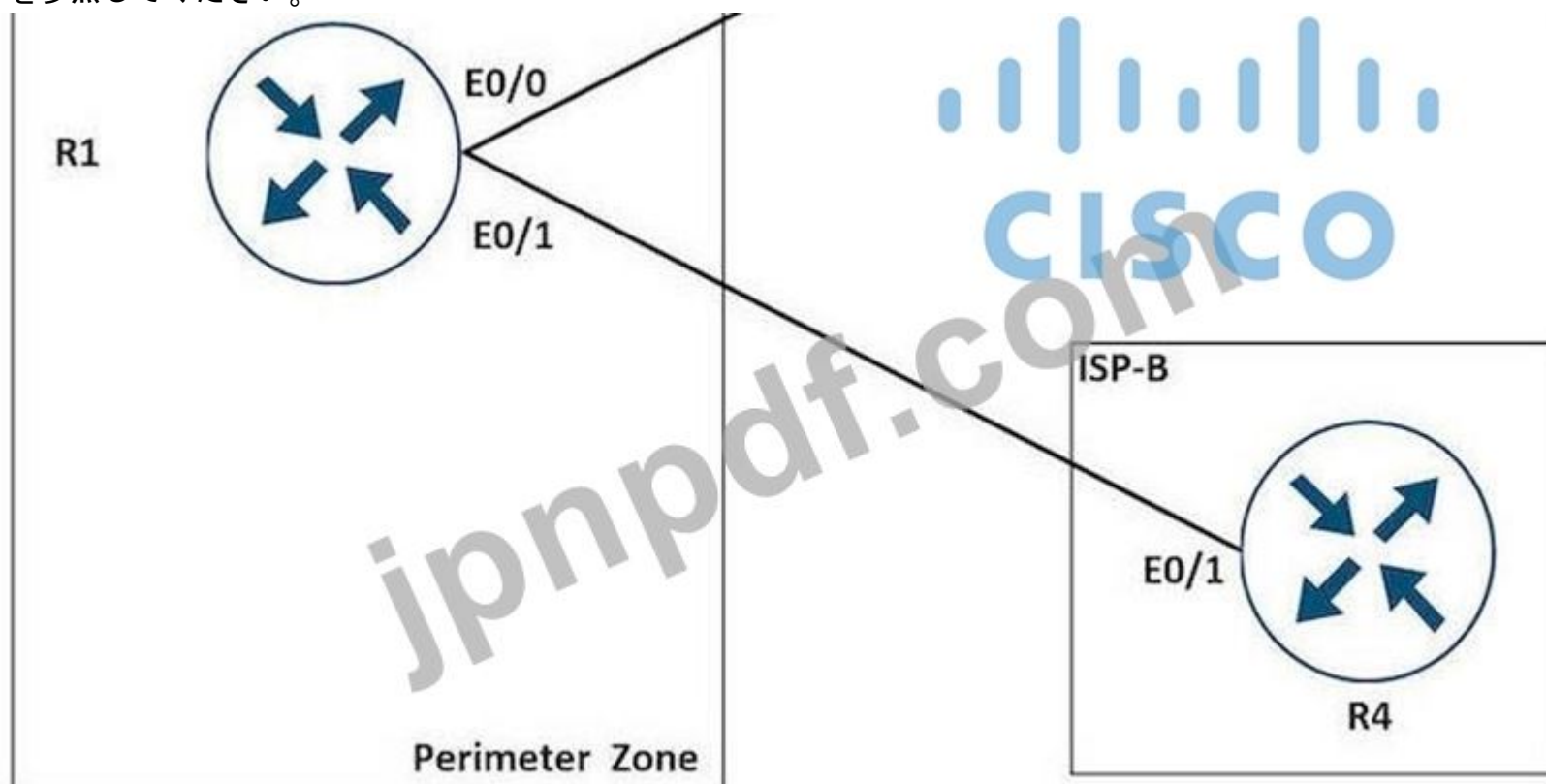
R2はルートリフレクターであり、R1とR3はルートリフレクタークライアントです。ルートはR1から172.16.25.0/24へのルートを学習しますが、R3にアドバタイズしません。ルートがアドバタイズされない理由は何ですか？

- A. R2にはネクストホップへのルートがないため、R2はプレフィックスをクライアントにアドバタイズしません。
- B. ルートリフレクターのセットアップには、ルーター間に完全なBGPメッシュが必要です。
- C. ルートリフレクターの設定では、分類プレフィックスのみが1つの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す。
- D. 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。

Answer: C (メッセージを残す)

最新問題: 273

展示を参照してください。



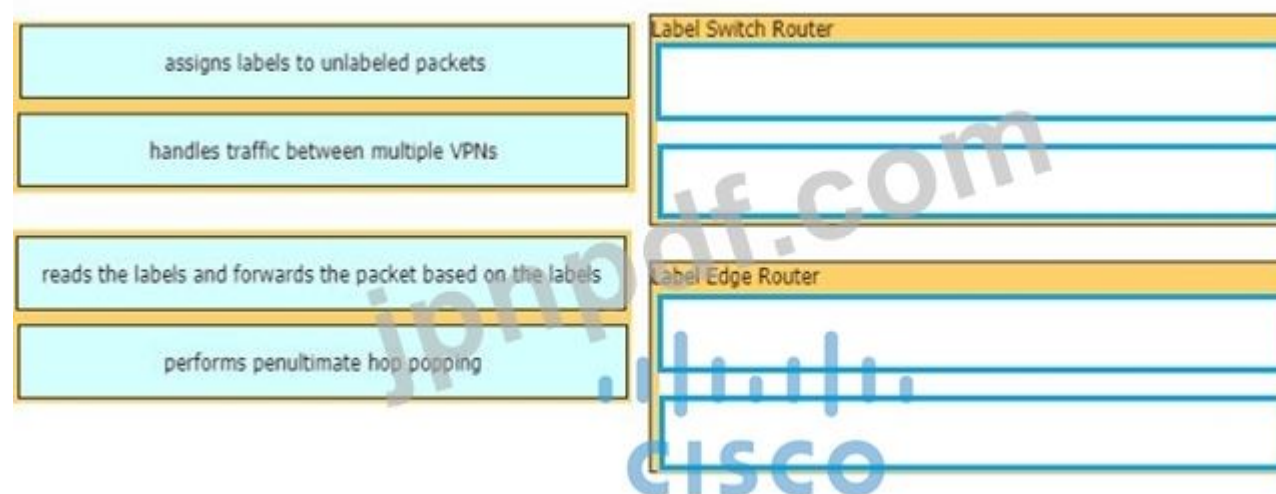
ネットワークはサイバー攻撃を受けています。SSHでR1に接続し、SSHセッションを介してターミナルモニターを有効にして、攻撃の発信元と宛先を見つけるネットワークエンジニア。セッションにはメッセージが殺到し、エンジニアは問題のトラブルシューティングを行うことができませんでした。R1でこの問題を解決するコマンドはどれですか？

- A. ターミナルモニターなし
- B. #terminalモニターなし
- C. (config)#no terminal monitor
- D. (config)#terminalモニターなし

Answer: B (メッセージを残す)

最新問題: 274

操作を左から右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: 275

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

```

隣接関係が発生しない隣接関係を発生させる2つの構成はどれですか。2つ選択してください

A. ニューヨーク

```
router ospf 1
```

```
 エリア0認証メッセージダイジェスト
```

B. ニューヨーク

```
 インターフェイスE0/0
```

```
no ip ospf message-digest-key 1 md5 Cisco123
```

```
ip ospf authentication-key Cisco123
```

C. LA

```
 インターフェイスE0/0
```

```
ip ospf message-digest-key 1 md5 Cisco123
```

D. LA

```
router ospf 1
```

```
 エリア0認証メッセージダイジェスト
```

E. LA

```
 インターフェイスE0/0
```

```
ip ospf authentication-key Cisco123
```

Answer: C,D (メッセージを残す)

最新問題: 276

IPv6First-HopSecurity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。

IPv6 DHCPv6 Guard	Block a malicious host and permit the router from a legitimate route.
IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents.
IPv6 Source Guard	Create a binding table that is based on NS and NA messages.
IPv6 RA Guard	Filter inbound traffic on Layer 2 switch ports that are not in the IPv6 binding table.
IPv6 ND Inspection	Create IPv6 neighbors connected to the device from information sources such as NDP snooping.

Answer:



最新問題: 277

展示を参照してください。

```
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Down User reset
* Jun 28 14:41:57: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.2.2 IPv4 Unicast
topology base removed from session User reset
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Up
R1#show clock
*15:42:00.506 CET Fri Jun 28 2019
```

エンジニアがデバイスのBGPのトラブルシューティングを行っていますが、デバイスのクロックがログエントリのタイムスタンプに対応していないことを発見しました。2つの時間の間の一貫性を保証するアクションはどれですか？

- A. グローバルコンフィギュレーションモードでservice timestamps loguptimeコマンドを設定します。
- B. グローバルコンフィギュレーションモードでlogging clocks synchronizeコマンドを設定します。
- C. グローバルコンフィギュレーションモードでservice timestamps logdatetime localtimeコマンドを設定します。
- D. デバイスのクロックがNTPサーバーと同期していることを確認します。

Answer: (解答を表示する)

説明

<https://community.cisco.com/t5/networking-documents/router-log-timestamp-entries-are-different-from-the-syste>

最新問題: 278

エンジニアがネットワークを構成しており、ルーティングテーブルに宛先アドレスのインターフェイスにパケットを転送する必要があります。このタスクを実行するには、何を構成する必要がありますか？

- A. set ip next-hop
- B. ip default next-hopを設定します
- C. set ip next-hop recursive
- D. set ip next-hop verify-availability

Answer: B (メッセージを残す)

The **set ip default next-hop** command verifies the existence of the destination IP address in the routing table, and...

- if the destination IP address exists, the command does not policy route the packet, but forwards the packet based on the routing table.
- if the destination IP address **does not exist**, the command policy routes the packet by **sending it to the specified next hop**.

最新問題: 279

展示を参照してください。

```
R1(config)#route-map ADD permit 20
R1(config-route-map)#set tag 1

R1(config)#router ospf1
R1(config-router)#redistribute rip subnets route-map ADD
```

R1について正しい説明はどれですか。

- A. RIPルートは変更なしでOSPFに再配布されます
- B. R1は、OSPFに再配布する前に、RIPで学習したルートのメトリックに1を追加します
- C. OSPFは、タグが1の場合にのみRIPルートを再配布します。
- D. RIPで学習したルートはタグ値1でOSPFに配布されます

Answer: D ([メッセージを残す](#))

最新問題: 280

MPLSの概念を左側から右側の説明にドラッグアンドドロップします。

label edge router	allows an LSR to remove the label before forwarding the packet
label switch router	accepts unlabeled packets and imposes labels
forwarding equivalence class	group of packets that are forwarded in the same manner
penultimate hop popping	receives labeled packets and swaps labels

Answer:



最新問題: 281

展示を参照してください。

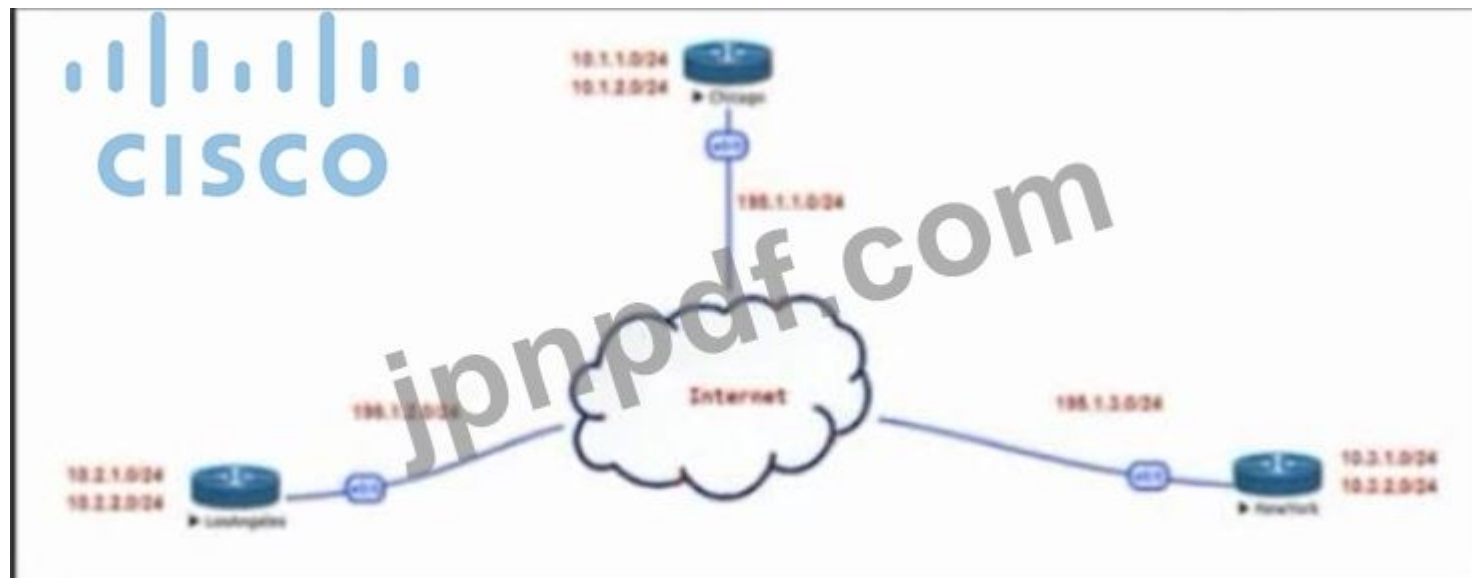
```
R1#show running-config section dhcp
ip dhcp excluded-address 192.168.1.1 192.168.1.49
ip dhcp pool DHCP
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
  dns-server 8.8.8.8
  lease 0 12
```

ユーザーから、DHCPサーバーからIPアドレスを取得できないとの報告がありました。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2時間を超えてアクティブになっているユーザーはいません。現在のリソース内の問題を修正するアクションはどれですか？

- A. DHCPリース時間を小さい値に設定します
- B. DHCPリース時間をより大きな値に構成します
- C. サブネットマスクをDHCPプールのnetwork192.168.1.0255.255.254.0コマンドに変更します
- D. network192.168.2.0255.255.255.0コマンドをDHCPプールに追加します

Answer: ([解答を表示する](#))

最新問題: 282



Chicago

```

interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source E0/0
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp map multicast dynamic
 no ip next-hop-self eigrp 111
 tunnel protection ipsec profile IPSec-PROFILE
!
router eigrp 111
 network 192.168.1.0
 network 10.0.0.0
  
```

展示を参照してください。ロサンゼルスとニューヨークのルーターはシカゴからルートを受信していますが、相互には受信していません。どちらの構成で問題が解決しますか？

- A. インターフェースTunnel1
no ip split-horizon eigrp 111
- B. インターフェーストンネル1
ip next-hop-self eigrp 111
- C. インターフェースTunnel1
トンネルモードIpsecIpv4
- D. インターフェースTunnel1

トンネル保護ipsecプロファイルIPSec-PROFILE

Answer: A ([メッセージを残す](#))


説明

このトポロジでは、シカゴのルーター (Hub)は、ロサンゼルス (Spoke1)ルーターからトンネルインターフェイスで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でニューヨーク (Spoke2)とも接続されていることです。EIGRPスプリットホライズンを無効にしない場合、ハブはSpoke1からSpoke2へのルートおよびその逆のルートの中継しません。これは、インターフェイスTunnel1でこれらのルートを受信したため、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 (splithorizonルール)。したがって、スポークがお互いを認識していることを確認するために、ハブルータでスプリットホライズンを無効にする必要があります。

最新問題: 283

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#
```



エンジニアが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。

エンジニアはコンソールを使用して接続し、トラブルシューティング時に表示された出力を見つけます。

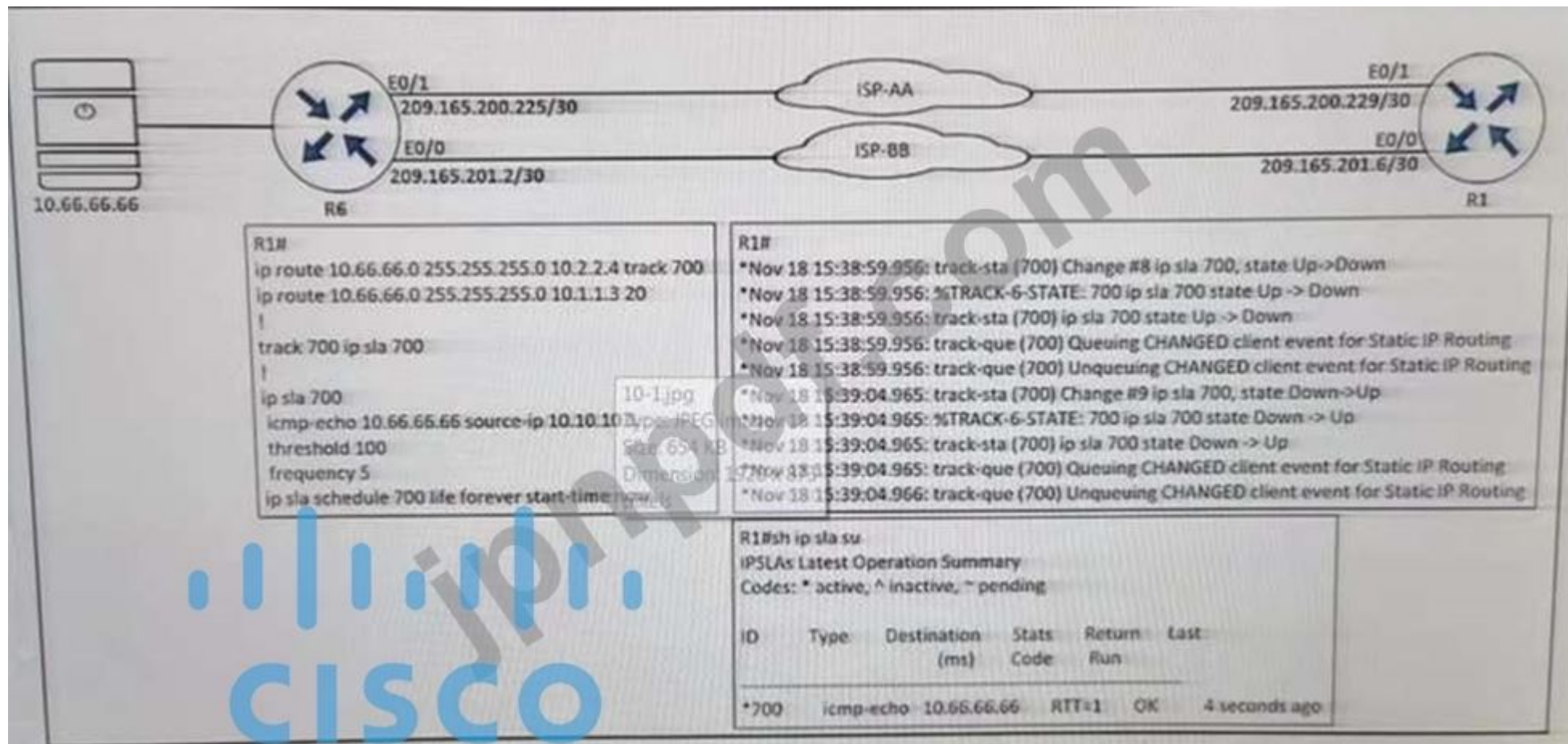
デバイスでSSHを有効にするには、構成モードでどのコマンドを使用する必要がありますか？

- A. ipsshバージョン2
- B. 暗号鍵はrsaを生成します
- C. ip ssh enable
- D. no ip ssh disable

Answer: B ([メッセージを残す](#))

最新問題: 284

展示を参照してください。



エンジニアは、ISPリンクフラッピングの問題を回避するためにR1でIPSLAを構成しました。ただし、設計どおりに機能していません。IPSLAは、トラフィックをセカンダリ接続に切り替える前に30秒待機し、プライマリリンクが使用可能で安定したときに、20秒後にプライマリリンクに戻る必要があります。どの構成で問題が解決しますか？

A. R1 (config)#ip sla 700

R1 (config-ip-sla)#delay down 30 up 20

B. R1 (config)#ip sla 700

R1 (config-ip-sla)#delay down 20 up 30

C. R1 (config)#track 700 ip sla 700

R1 (config-track)#delay down 30 up 20

D. R1 (config)#track 700 ip sla 700

R1 (config-track)#delay down 20 up 30

Answer: C (メッセージを残す)

最新問題: 285

展示を参照してください。

```

ip dhcp pool 1
network 200.30.30.0/24
default-router 200.30.30.100
lease 40
!
ip dhcp pool 2
network 200.30.40.0/24
default-router 200.30.40.100
lease 40
!

```

財務部門のサーバーは、200.30.40.0 / 24ネットワーク上で一貫して到達可能ではなく、2か月ごとに新しいIPアドレスを取得します。この問題を解決するには、どの2つのアクションを実行する必要がありますか？ 2つ選択してください。）

- A. デフォルトゲートウェイ20030.40.100のネットワークでDHCPを使用するようにサーバーを構成します。
- B. サーバーのIPアドレスを除外するようにルーターを構成します。
- C. デフォルトゲートウェイ20030.30.100のネットワークでDHCPを使用するようにサーバーを構成します。
- D. 静的IPアドレスとデフォルトゲートウェイを使用してサーバーを構成します。

Answer: B,D (メッセージを残す)

最新問題: 286

アドレスを左側から右側の正しいIPv6フィルター目的にドラッグアンドドロップします。

permit ip 2001:d8b:800:200c:: /117
2001:0DBB:800:2010::/64 eq 443

permit ip 2001:D88:800:200C::e/126
2001:0DBB:800:2010::/64 eq 514

permit ip 2001:d8b:800:200c::800 /117
2001:0DBB:800:2010::/64 eq 80

permit ip 2001:D8B:800:200C::c/126
2001:0DBB:800:2010::/64 eq 123

Permit NTP from this source
2001:0D8B:0800:200c::1f

Permit syslog from this source
2001:0D88:0800:200c::1c

Permit HTTP from this source
2001:0D8B:0800:200c::0fff

Permit HTTPS from this source
2001:0D8B:0800:200c::07ff

Answer:

<pre> permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443 </pre>	<pre> permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123 </pre>
<pre> permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514 </pre>	<pre> permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514 </pre>
<pre> permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80 </pre>	<pre> permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80 </pre>
<pre> permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123 </pre>	<pre> permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443 </pre>

説明

同じ回答はすでに以下で更新されています：

<pre> permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123 </pre>
<pre> permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514 </pre>
<pre> permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80 </pre>
<pre> permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443 </pre>

HTTPとHTTPSはそれぞれTCPポート80と443で実行されるため、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。しかし、2001:d88:800:200c::c/126は2001:d88:800:200c:0:0:0:cから2001:d88:800:200c:0:0:0:fの範囲でしかないため、この質問にはいくつかのタイプミスがあるかもしれません。0:0:f(合誂つのホスト)。ホストは対象外です

2001:0D88:0800:200c::1f、2001:D88:800:200c::e/126についても同じで、

2001:d88:800:200c:0:0:0:cから2001:d88:800:200c:0:0:0:fであり、ホスト2001:0D88:0800:200c::1cは対象外です。

有効な **300-410** 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の **300-410** 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をゲットする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**80030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 287

MPLSクラウド全体のPルーターのコントロールプレーンで機能する2つのプロトコルはどれですか。2つ選択してください)

A. 自民党

- B. ECMP
- C. LSP
- D. MPLS OAM
- E. 出欠確認

Answer: A,E (メッセージを残す)

最新問題: 288

示す:



NTPは、ネットワークインフラストラクチャとCiscoDNACenter全体で設定されます。NTPの問題が17:15にCiscoDNACenterで報告されました。問題を解決するアクションはどれですか？

- A. WLCとNTPサーバー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. CiscoDNACenterとNTPサーバー間の到達可能性を確認して解決します
- D. WLCでNTPを確認および設定し、CiscoDNACenterと同期します

Answer: (解答を表示する)

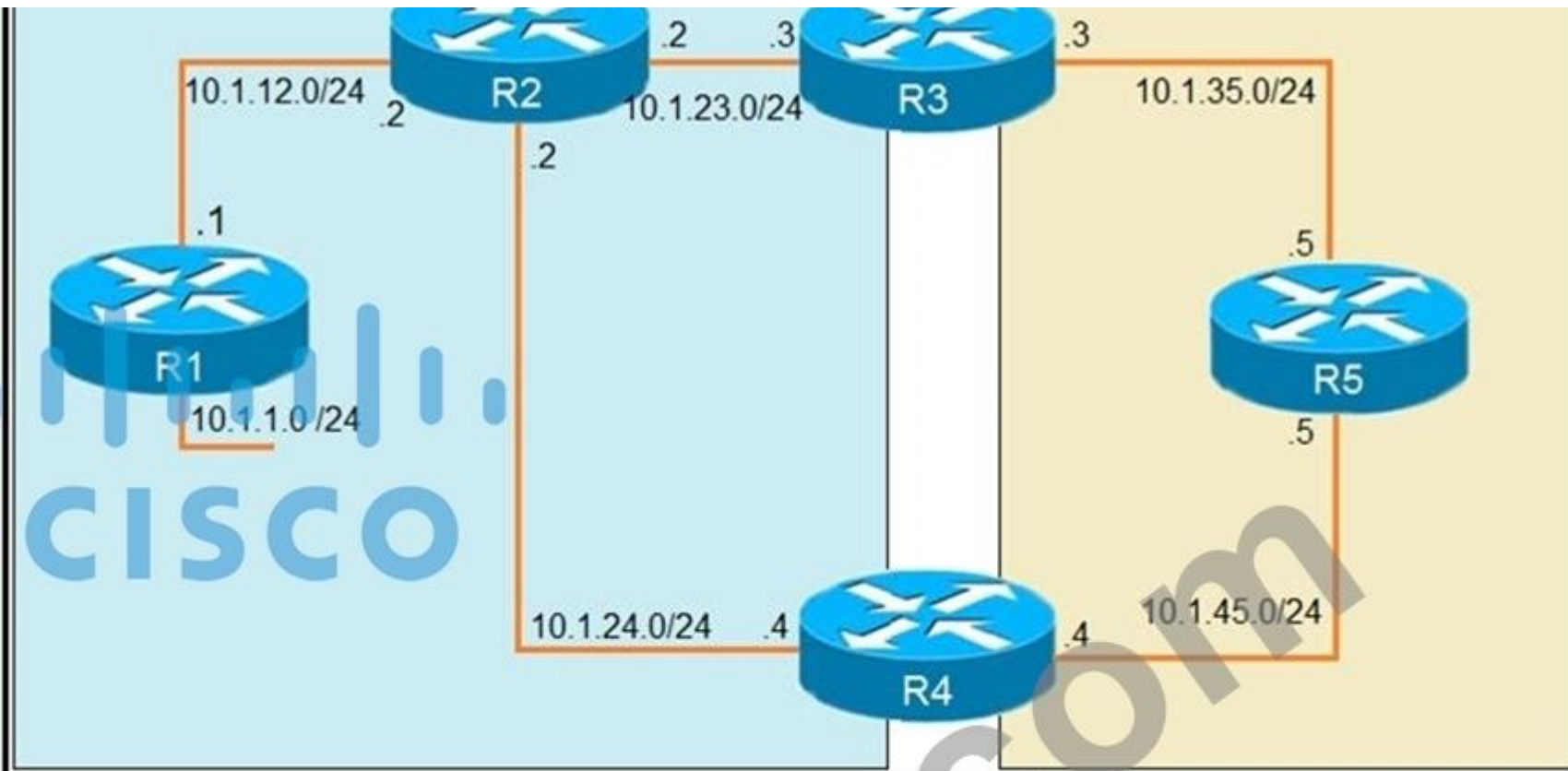
説明

Cisco DNA Centerとデバイス間の過度のタイムラグ :CiscoDNACenterとデバイスのIPアドレス間の時間差が大きすぎています。時差が3分を超えると、CiscoDNACenterはデバイスデータを正確に処理できません。

最新問題: 289

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 truncated>
```

R5からのトレースルートの出力は、ネットワーク内のループを示しています。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)

```
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 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 ([メッセージを残す](#))

説明

ループの理由は、R2が10.1.1.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、OSPF再配布ステートメントでは、BWメトリックの値が高く、遅延の値が1であるためです。したがって、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、ループを引き起こします。これで、R5はR3から10.1.1.0/24を学習し、R4がEIGRPに再配布するのと同じルートをR4にアドバタイズします。R3がOSPFでEIGRPを再配布するときにタグ1を設定し、R4が再配布中にタグ1ですべてのOSPFルートを拒否した場合、R3は10.1.1.0/24を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。

展示を参照してください。

```
TAC+: TCP/IP open to 171.68.118.101/49 failed --
Destination unreachable, gateway or host down
AAA/AUTHEN (2546660185): status = ERROR
AAA/AUTHEN/START (2546660185): Method=LOCAL
AAA/AUTHEN (2546660185): status = FAIL
As1 CHAP: Unable to validate Response. Username chapuser: Authentication failure
```

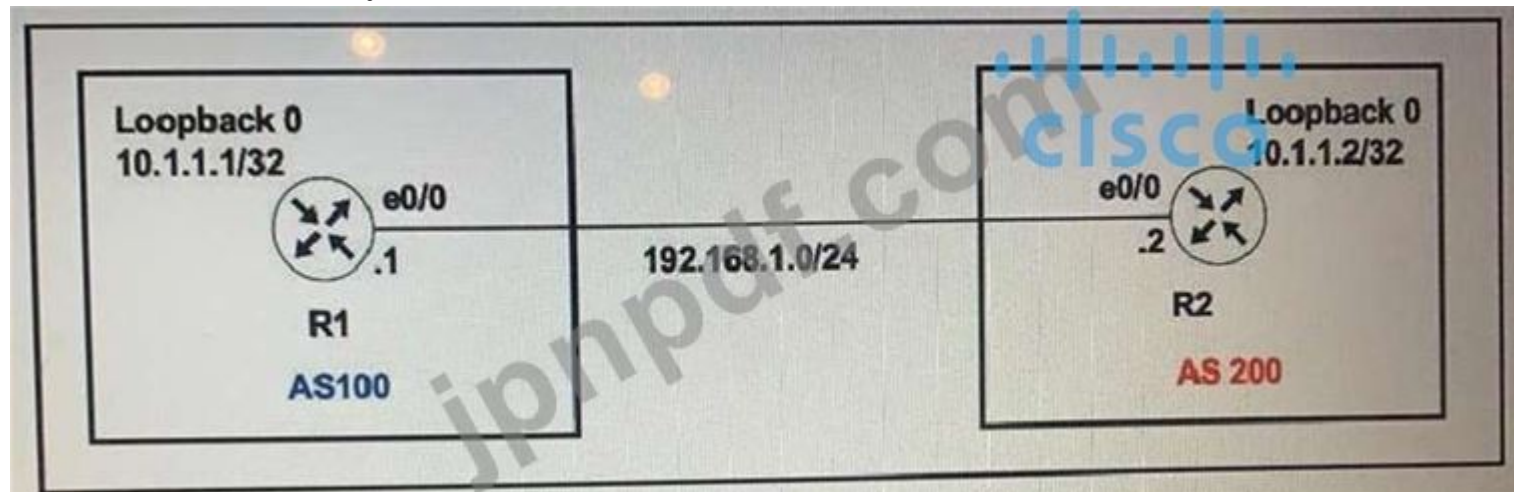
ユーザー認証が拒否されるのはなぜですか？

- A. TACACS +サーバーがダウンしていて、ユーザーがローカルデータベースに存在していません
- B. ユーザーがCHAP用に設定されているため、TACACS+サーバーはユーザーを拒否します
- C. TACACS +サーバーがダウンしており、ユーザーはローカルデータベースにいます
- D. TACACS +サーバーは「user」を予期していますが、NTクライアントは「domain\user」を送信します

Answer: D ([メッセージを残す](#))

最新問題: 291

展示を参照してください。



R1およびR2の構成は次のとおりです。

```
R1
router bgp 100
neighbor 10.1.1.2 remote-as 200

R2
router bgp 200
neighbor 10.1.1.1 remote-as 100
```

隣人は来ていません。ネイバーを起動する構成の2つのセットはどれですか？ 2つ選択してください。)A)

R2

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1  
!  
router bgp 200  
neighbor 10.1.1.1 disable-connected-check  
neighbor 10.1.1.1 update-source loopback 0
```

B)

R2

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1  
!  
router bgp 200  
neighbor 10.1.1.1 ttl-security hops 1  
neighbor 10.1.1.1 update-source loopback 0
```

C)

R1

```
ip route 10.1.1.2 255.255.255.255 192.168.1.2  
!  
router bgp 100  
neighbor 10.1.1.2 disable-connected-check  
neighbor 10.1.1.2 update-source Loopback0
```

D)

R1

```
ip route 10.1.1.2 255.255.255.255 192.168.1.2  
!  
router bgp 100  
neighbor 10.1.1.1 ttl-security hops 1  
neighbor 10.1.1.2 update-source loopback 0
```

E)

R2

```
ip route 10.1.1.2 255.255.255.255 192.168.1.2  
!  
router bgp 100  
neighbor 10.1.1.2 ttl-security hops 1  
neighbor 10.1.1.2 update-source loopback 0
```

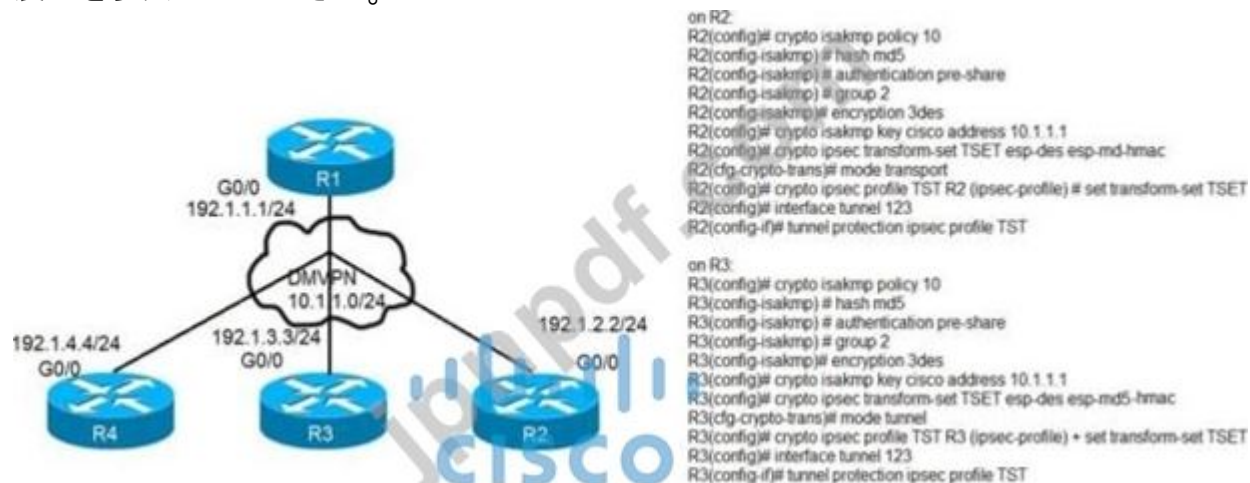
- A. オプションA
- B. オプションB
- C. オプションC
- D. オプションD
- E. オプションE

Answer: A,C (メッセージを残す)

The `neighbor disable-connected-check` command is used to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address.

最新問題: 292

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確認しました。

問題を解決した2つのアクションはどれですか？ (2つ選択してください。)

- A. 暗号isakmpキーのCiscoアドレス10.1.1.1を削除します。R2とR3で。
- B. モードをモードトランスポートからR2のモードトンネルに変更します。
- C. R2およびR3でcrypto isakmpkeyciscoアドレス192.1.1.1を設定します。
- D. R2およびR3でcrypto isakmpkeyciscoアドレス0.0.0.0を設定します。
- E. 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。

Answer: D,E (メッセージを残す)

最新問題: 293

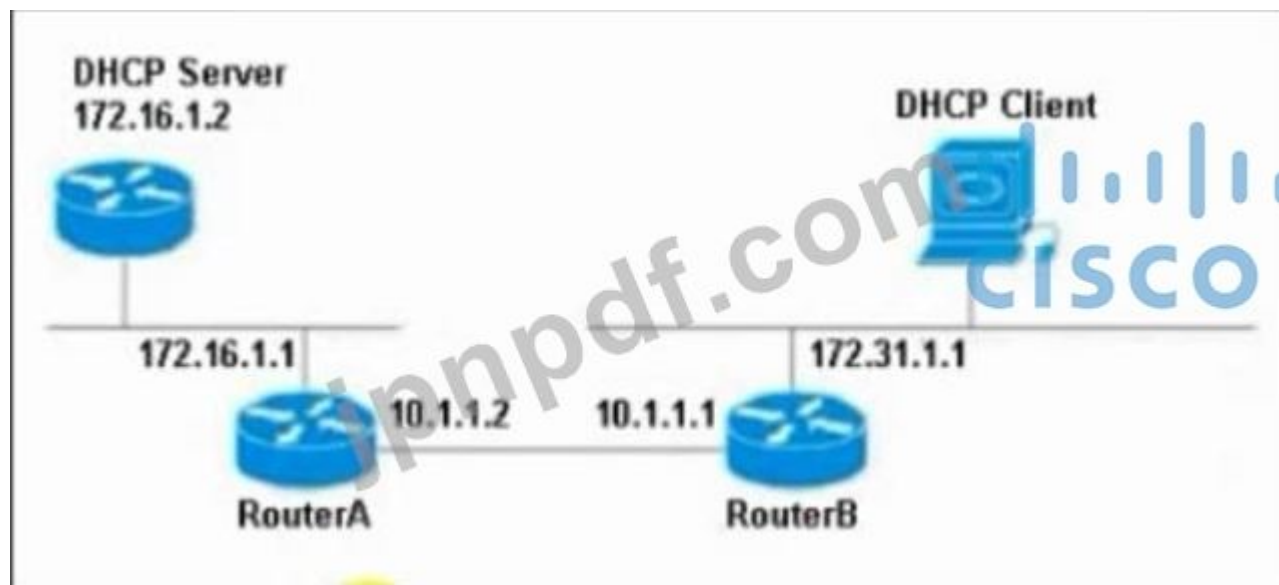
```
Ipv6 unicast-routing
!
Router ospfv3 4
  Router-id 192.168.1.1
!
Interface E 0/0
  Ipv6 enable
  Ip address 10.1.1.1 255.255.255.0
  Ospf3 4 area 0 ipv4
  No shut
!
Interface Loopback0
  Ipv6 enable
  Ipv4 172.16.1.1 255.255.255.0
  Ospf3 4 area 0 ipv4
```

展示を参照してください。ネットワーク管理者は、E 0/0インターフェイスでIPv6用にブランチルーターを構成しました。隣接ルーターは要件を満たすように完全に構成されていますが、隣接関係が確立されていません。IPv6ネイバーを起動するために、ブランチルーターの問題を修正するアクションはどれですか。

- A. E0/0インターフェイスでnoospfv3 4 area 0 ipv4コマンドを使用して、IPv4のOSPFを無効にします。
- B. address-family ipv4 unicastコマンドを使用して、ルータospfv34プロセスでIPv4アドレスファミリーを有効にします。
- C. no ipv6 enableコマンドを使用して、E0/0インターフェイスでIPv6を無効にします
- D. address-family ipv4 unicastコマンドを使用して、E0/0インターフェイスでIPv4アドレスファミリーを有効にします

Answer: B ([メッセージを残す](#))

最新問題: 294



展示を参照してください。DHCPクライアントがDHCPサーバーからIPアドレスを受信できないRouterBは次のように構成されています。インターフェイスfastethernet0/0

説明クライアントDHCPID394482431

IPアドレス1723111 255 255.255 0

!

ip route 172.16.1.0 255 255 255.0 10.1.1.2

この問題を解決するには、RouterBのfastethernet 0/0インターフェイスでどのコマンドが必要ですか？

- A. RouterB (config-if)#ip helper-address 172.16.1.2
- B. RouterB(config-if)#ip helper-address 255.255 255 255
- C. RouterB (config-if)#ip helper-address 172.16.1.1
- D. RouterB (config-if)#ip helper-address 172.31.1.1

Answer: ([解答を表示する](#))

最新問題: 295

展示を参照してください。

The screenshot shows a network diagram with an FTP Server and a Switch. The FTP Server has IP 10.0.0.2/24 and is configured with 'Username: cisco', 'Password: cisco', and 'File to download: IOS.bin'. The Switch is connected to the FTP Server via E0/1 VLAN2 and has IP 10.0.0.1 255.255.255.0. The switch configuration includes 'ip ftp source-interface vlan 2'. A terminal window on the FTP Server shows a successful ping from 10.0.0.1 to 10.0.0.1. Another terminal window on the Switch shows a failed copy command: 'Switch#copy ftp://cisco:cisco@10.0.0.2/IOS.bin flash:/' resulting in '%Error opening ftp://cisco:cisco@10.0.0.2/IOS.bin (No such file or directory)'.

エンジニアはIOS.binをコピーできません

問題を解決するアクションはどれですか？

- A. FTPサーバーからファイルをダウンロードするためのファイル権限を許可します。
- B. copy flash :ftp://cisco@10.0.0.2/IOS.binコマンドを使用します。
- C. ファイルをダウンロードするためにスイッチフラッシュまたはUSBドライブにメモリスペースを作ります。
- D. FTPサーバーに存在しないIOS.binファイルを追加します。

Answer: D ([メッセージを残す](#))

最新問題: 296

展示を参照してください。

The screenshot shows a terminal window with the following configuration commands for Router R1:

```
R1(config)#route-map ADD permit 20
R1(config-route-map)#set tag 1

R1(config)#router ospf1
R1(config-router)#redistribute rip subnets route-map ADD
```

R1について正しい説明はどれですか。

- A. OSPFは、タグが1の場合にのみRIPルートを再配布します。
- B. RIPルートは変更なしでOSPFに再配布されます。
- C. RIPで学習したルートは、タグ値1でOSPFに配布されます。
- D. R1は、OSPFに再配布する前に、RIPで学習したルートのメトリックに1を追加します。

Answer: C (メッセージを残す)

最新問題: 297

展示を参照してください。



エンジニアは、ISP1およびISP2への設定済みデフォルトルートの到達可能性を監視しています。利用可能な場合は、ISP1からのデフォルトルートが優先されます。この問題はどのように解決されますか？

- A. icmp-echoコマンドを使用して、両方のデフォルトルートを追跡します
- B. 頻度を定義してスケジュールすることによりIPSLAを開始します
- C. 両方のデフォルトルートに同じADを使用する
- D. trackおよびipslaコマンドの番号を照合してIPSLAを開始します

Answer: ([解答を表示する](#))

最新問題: 298

展示を参照してください。

```
R200#show ip bgp summary
BGP router identifier 10.1.1.1, local AS number 65000
BGP table version is 26, main routing table version 26
1 network entries using 132 bytes of memory
1 path entries using 52 bytes of memory
2/1 BGP path/bestpath attribute entries using 296 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 28 bytes of memory
BGP using 508 total bytes of memory
BGP activity 24/23 prefixes, 24/23 paths, scan interval 60 secs
Neighbor      V    AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.0.2.2     4 65100 20335   20329     0  0    0 00:02:04  Idle (PfxCt)
R200#
```

どのような状況でBGPネイバーはアイドル状態のままになりますか？

- A. プレフィックスがBGPピアから受信されない場合
- B. プレフィックスが上限に達した場合
- C. インバウンド方向にプレフィックスリストが適用されている場合
- D. プレフィックスが上限を超えた場合

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: 299

示す :

```
policy-map COPP-7600
class COPP-CRITICAL-7600
  police cir 2000000 bc 62500
  conform-action transmit
  exceed-action transmit
!
class class-default
  police cir 200000 bc 6250
  conform-action transmit
  exceed-action drop
!
class-map match-all COPP-CRITICAL-7600
  match access-group name COPP-CRITICAL-7600
!
ip access-list extended COPP-CRITICAL-7600
  permit ip any any eq http
  permit ip any any eq https
```

Coppポリシーが適用された後、BGPはフラッピングしています。問題を解決するための2つの解決策は何ですか？
(2つ選択してください)

- A. COPP-CRITICAL-7600ACLでBGPを設定します
- B. デフォルトクラスでCIRの値を高く設定して、トラフィックのピーク時にさらに多くのパケットを許可します
- C. クラスCOPP-CRITICAL-7600でCIRの値を高く設定します
- D. クラスCOPP-CRITICAL-で、2色のポリサーではなく3色のポリサーを構成します。
- E. IP CEFtoCoPPポリシーとBGPを機能するように構成します

Answer: ([解答を表示する](#))

ポリシーマップCOPP-7600は (ACL条件に基づいて)HTTPおよびHTTPSトラフィックのみをレート制限するため、BGPパケットはクラス「class-default」で処理され、超過したBGPパケットはドロップされます。したがって、この問題を解決するには2つの方法があります。

+ 「permittcpanyanyeqbgp」というステートメントを使用してBGPをACLに追加します

+ 2MbpsはWebトラフィックには低すぎるため、デフォルトクラスでCIRの値を高く設定します (http&https)

最新問題: 300

LDPはMPLSトポロジでどの機能を提供しますか？

- A. LSRのMPLSトポロジでホップバイホップ転送を提供します。
- B. 異なるVRF間でMPLSVPNのルートを交換します。
- C. MPLSトポロジで複数のVPNをPルーターに接続できるようにします。

D. LSRがIPルートを交換するための手段を提供します。

Answer: A (メッセージを残す)

最新問題: 301

OSPFv3アドレスファミリ構成のOSPFv3プロセスにIPv4インターフェイスを追加する構成はどれですか。

A. ルーターospfv3 1

アドレスファミリipv4ユニキャスト

B. ルーターospfv3 1

アドレスファミリipv4

C. Router (config-if) #ospfv3 1 ipv4 area 0

D. Router (config-router) #ospfv3 1 ipv4 area 0

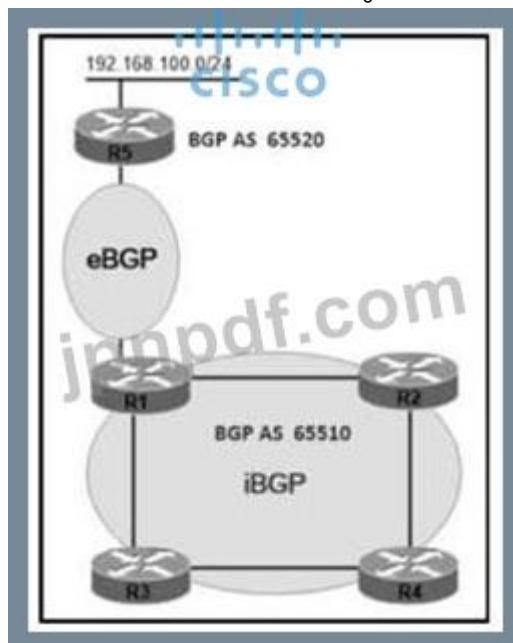
Answer: A (メッセージを残す)

有効な 300-410 問題集は GoShiken.com が提供された合格しやすい 300-410 試験問題集！ GoShiken.com が最新の 300-410 試験問題集を提供しています。GoShiken.com 300-410 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-410 問題集をGETする人はこちら: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (80030%OFF問題集溶と正解付きで 30%w特別割引コード:

Freepdfdumps)

最新問題: 302

展示を参照してください。



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pingまたはtracerouteネットワークを実行できません 192.168.100.0/24この問題を解決するアクションはどれですか。

A. 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

B. 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

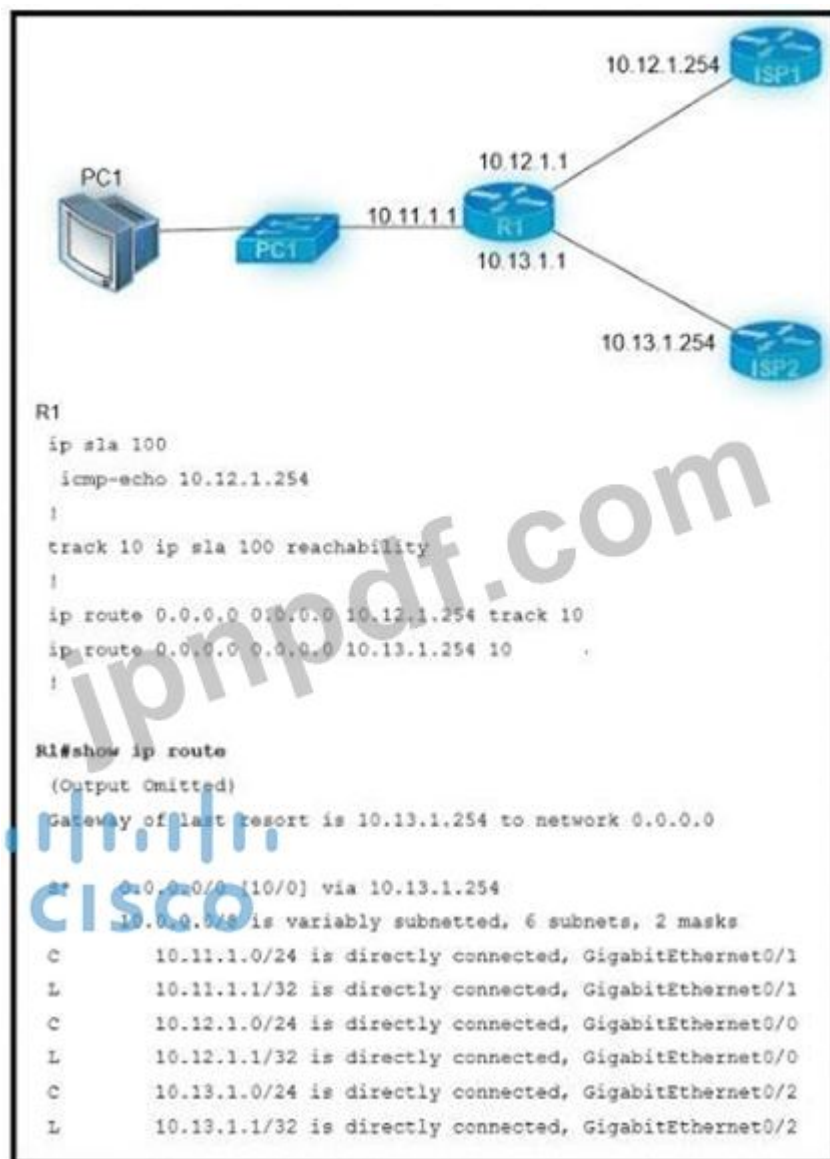
C. R4をルートリフレクターサーバーとして構成し、R2とR3をルートリフレクタークライアントとして構成します。

D. 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

Answer: C (メッセージを残す)

最新問題: 303

展示を参照してください。



エンジニアは、ISP1およびISP2への設定済みデフォルトルートの到達可能性を監視しています。利用可能な場合は、ISP1からのデフォルトルートが優先されます。この問題はどのように解決されますか？

- A. 両方のデフォルトルートに同じADを使用する
- B. trackおよびipslaコマンドの番号を照合してIPSLAを開始します
- C. 頻度を定義してスケジュールすることによりIPSLAを開始します
- D. icmp-echoコマンドを使用して、両方のデフォルトルートを追跡します

Answer: C (メッセージを残す)

最新問題: 304

エンジニアは、ルーティングテーブルに存在しない宛先IPアドレスに対してポリシーベースのルーティングを構成しました。set ip default next-hopコマンドを設定するためのポリシーを通じて、パケットはどのように処理されますか。

- A. パケットは特定のネクストホップに転送されません。
- B. パケットは静的ルートに基づいて転送されます。
- C. パケットはルーティングテーブルに基づいて転送されます。
- D. パケットは特定のネクストホップに転送されます。

Answer: ([解答を表示する](#))

最新問題: 305

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#
```

エンジニアが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。エンジニアはコンソールを使用して接続し、トラブルシューティング時に表示された出力を見つけます。デバイスでSSHを有効にするには、構成モードでどのコマンドを使用する必要がありますか？

- A. no ip ssh disable
- B. 暗号鍵はrsaを生成します
- C. ipsshバージョン2
- D. ip ssh enable

Answer: B ([メッセージを残す](#))

最新問題: 306

エンジニアは、ルートに影響を与えるポリシーでアクセスリストNON-CISCOを設定しました

```
route-map PBR, deny, sequence 5
Match clauses:
 ip address (access-list): NON-CISCO
Set clauses:
Policy routing matches: 0 packets, 0 bytes
route-map PBR, permit, sequence 10
Match clauses:
Set clauses:
 ip next-hop 192.168.1.5
Policy routing matches: 388213827 packets, 222009685077 bytes
```

このルートマップ設定の2つの効果は何ですか？ (2つ選択してください。)

- 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ルックアップ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: ([解答を表示する](#))

<https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds-ce.html>

Valid 300-410 Dumps shared by GoShiken.com for Helping Passing 300-410 Exam! GoShiken.com now offer the **newest 300-410 exam dumps**, the GoShiken.com 300-410 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com 300-410 dumps with Test Engine here: <https://www.goshiken.com/Cisco/300-410-mondaishu.html> (**800** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)