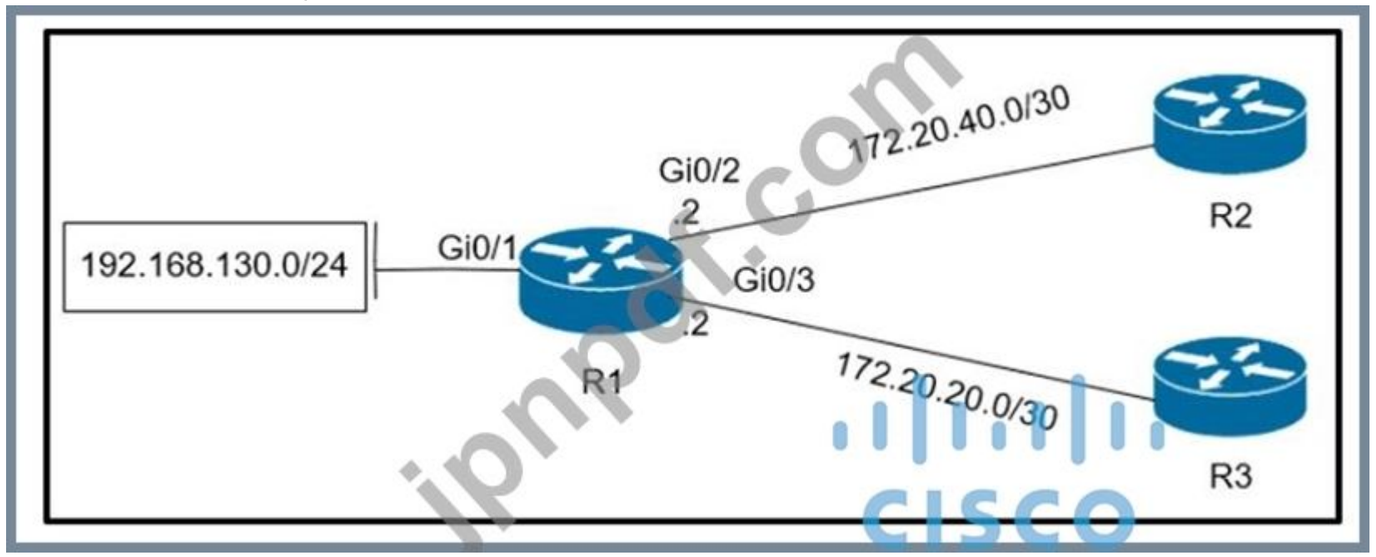
Cisco.300-410J.v2022-05-02.q85

試験コード:	300-410J
試験名称:	Implementing Cisco Enterprise Advanced Routing and Services (300-410日本語版)
認定資格:	Cisco
無料問題数:	85
バージョン:	v2022-05-02
アクセス数:	963
ページビュー数:	850
https://www.jpnpdf.com/Cisco.300-410J.v2022-05-02.q85-mondaishu.html	

最新問題: **1**
MPLSレイヤー3 VPN構成でトラフィックの負荷を分散できるコマンドはどれですか。
A. マルチパスeibgp 2
B. 最大パス2
C. 最大パスibgp 2
D. マルチパス2
Answer: C (メーッセージを残す)

最新問題: **2**
展示を参照してください。



192.168.130.0/24ネットワークから送信されたトラフィックをR2に転送するようにR1にポリシーを構成する構成はどれですか。

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

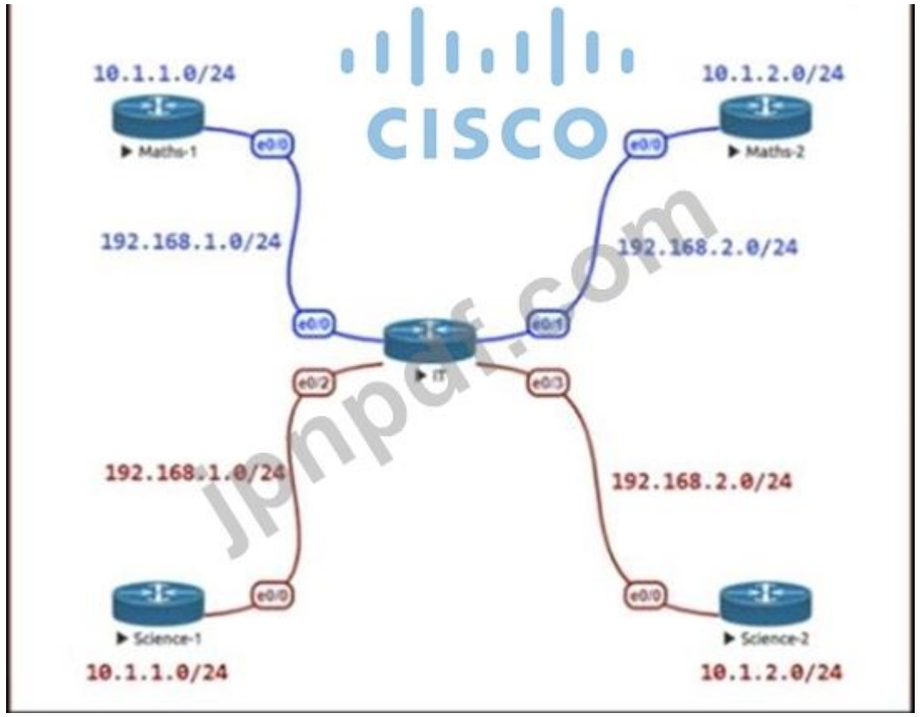
B.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.2
```

C.
```
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
```

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

最新問題**: 3**
展示を参照してください。



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。

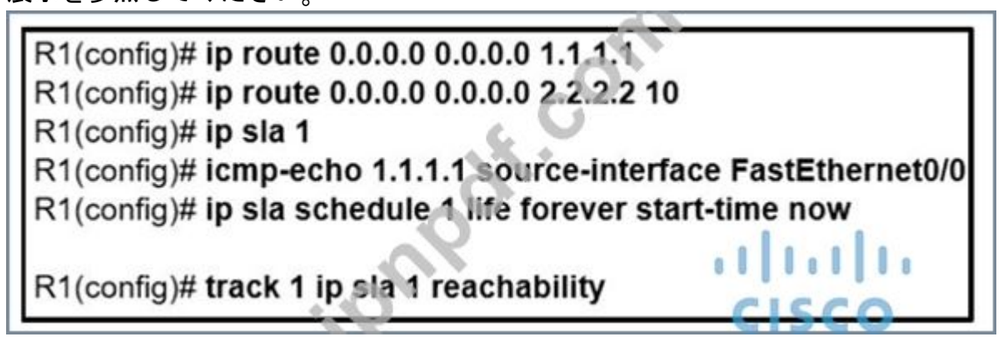
A. vrf定義科学
アドレスファミリipv4
！
インターフェイスE0 / 2
IPアドレス192.168.1.1255.255.255.0
閉じない
！
インターフェイスE0 / 3
IPアドレス192.168.2.1255.255.255.0
閉じない

B. vrf定義科学
！
インターフェイスE0 / 2
IPアドレス192.168.1.1255.255.255.0
閉じない
！
インターフェイスE0 / 3
IPアドレス192.168.2.1255.255.255.0
閉じない

C. vrf定義科学
アドレスファミリipv4

！
インターフェイスE0 / 2
vrf転送科学
IPアドレス192.168.1.1255.255.255.0
閉じない
！
インターフェイスE0 / 3
vrf転送科学
IPアドレス192.168.2.1
D. vrf定義科学
アドレスファミリipv4
！
インターフェイスE0 / 2
IPアドレス192.168.1.1255.255.255.0
vrf転送科学
閉じない
！
インターフェイスE0 / 3
IPアドレス192.168.2.1255.255.255.0
vrf転送科学
閉じない
Answer: C (メーッセージを残す)

最新問題**: 4**
展示を参照してください。



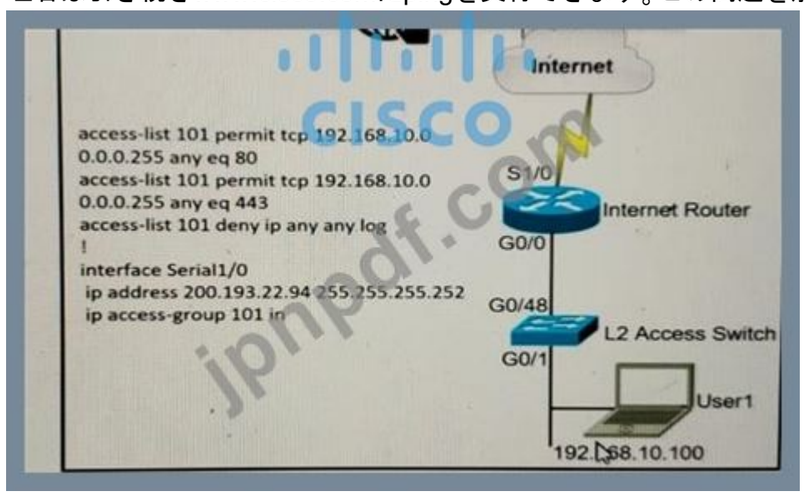
IP SLAは、プライマリがダウンしているときにバックアップのデフォルトルートを使用するように設定されていますが、希望どおりに機能していません。どのコマンドが問題を修正しますか？
A. R1（config）#p route 0.0.0.0.0.0.0.2.2.2.2 10 track 1
B. R1（config）#p route 0.0.0.0.0.0.0.2.2.2.2
C. R1（config）#ip sla track 1
D. R1（config）#p route 0.0.0.0.0.0.0.1.1.1.1 track 1
Answer: D (メーッセージを残す)
Reference:

Note: By default Static Router AD value-1 hence ip route 0.0.0.0. 0.0.0.0. 1.1.1.1 track 1 means AD-1 which must be less than of back up route AD.
Define the backup route to use when the tracked object is unavailable. !--- The administrative distance of the backup route must be greater than !--- the administrative distance of the tracked route. !--- If the primary gateway is unreachable, that route is removed !--- and the backup route is installed in the routing table !--- instead of the tracked route.
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-with-default-routes-using-I.html
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118962-configure-asa-00.html

最新問題**: 5**
ユーザーは、ローカルDHCPサーバーからリモートの企業DHCPサーバーに移動されました。移動後、ユーザーは誰もネットワークを使用できなくなりました。
このセットアップが正しく機能しないのはどの問題ですか？ （2つ選択してください）
A. DHCPサーバーのIPアドレス構成がローカルにありません
B. 新しいDHCPサーバーへのルートがありません
C. 802.1XがDHCPトラフィックをブロックしています
D. 自動QoSがDHCPトラフィックをブロックしています。
E. ブロードキャストドメインが大きすぎてDHCPを適切に伝播できません
Answer: A,B (メーッセージを残す**)**

最新問題**: 6**
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. 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。
B. MPLSラベルは、転送等価クラスを識別する短い識別子です。
C. LDPは、信頼性の高い情報配信のためにTCPを使用します。
D. 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。
E. ラベルはレイヤー3ヘッダーの後のパケットに適用されます。
Answer: B,C (メーッセージを残す**)**

最新問題**: 7**
ネットワーク管理者は、User1ラップトップからインターネットに向かうhttpおよびhttpsトラフィックのみが会社のセキュリティポリシーに準拠することを許可するように任務を負っています。管理者は引き続きwww.cisco.comにpingを実行できます。この問題を解決するには、アクセスリスト101を適用する必要があるインターフェイスはどれですか。

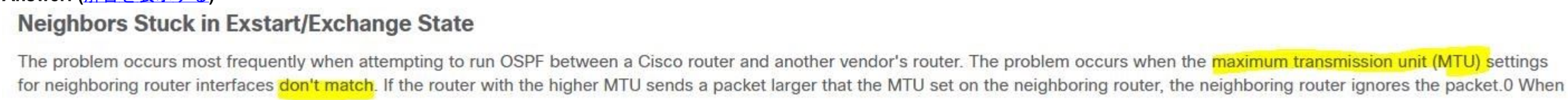


A. 発信方向のインターフェースG0 / 0。
B. 入力方向のインターフェースG0 / 48
C. 発信方向のインターフェースS1 / 0。
D. 入力方向のインターフェースG0 / 0。
Answer: D (メーッセージを残す**)**

最新問題**: 8**
VRF-Liteセットアップ実装を介したルート識別子の役割は何ですか？
A. IPアドレスを拡張して、所属するVFPインスタンスを識別します。
B. VRF-Liteセットアップのマルチキャスト配信を可能にし、IGPルーティングプロトコル機能を拡張します
C. 2つ以上のVRFインスタンス間のルートのインポートとエクスポートを管理します
D. VRF-Liteセットアップのマルチキャスト配信を可能にし、EGPルーティングプロトコル機能を拡張します
Answer: (解答を表示する**)**

最新問題**: 9**
TCP枯渇を引き起こす可能性があるプロトコルはどれですか？ （2つ選択してください）
A. FTP
B. TFTP
C. SMTP
D. HTTPS
E. SNMP
Answer: B,E (メーッセージを残す**)**

最新問題**: 10**
エンジニアは2つのルーター間の動的ルーティングを必要とし、OSPF隣接関係を確立できません。show ip ospf neighborコマンドの出力は、ネイバーの状態がEXSTART / EXCHANGEであることを示しています。
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. パスワードを一致させる
B. helloタイマーを一致させる
C. MTUを一致させる
D. ネットワークタイプに一致
Answer: (解答を表示する**)**



最新問題**: 11**
展示を参照してください。1.1.1.0/24をフィルタリングしながら、ネイバーからのルートを復元するアクションはどれですか。
A. アクセスリストを変更して、許可するのではなく拒否するようにします。
B. アクセスリストに2行目を追加して、許可します。

C. アクセスリストを拒否するのではなく許可するようにルートマップを変更します
D. ルートマップに2番目のシーケンスを追加するpermit 20
Answer: C (メーッセージを残す**)**

最新問題**: 12**
展示を参照してください。

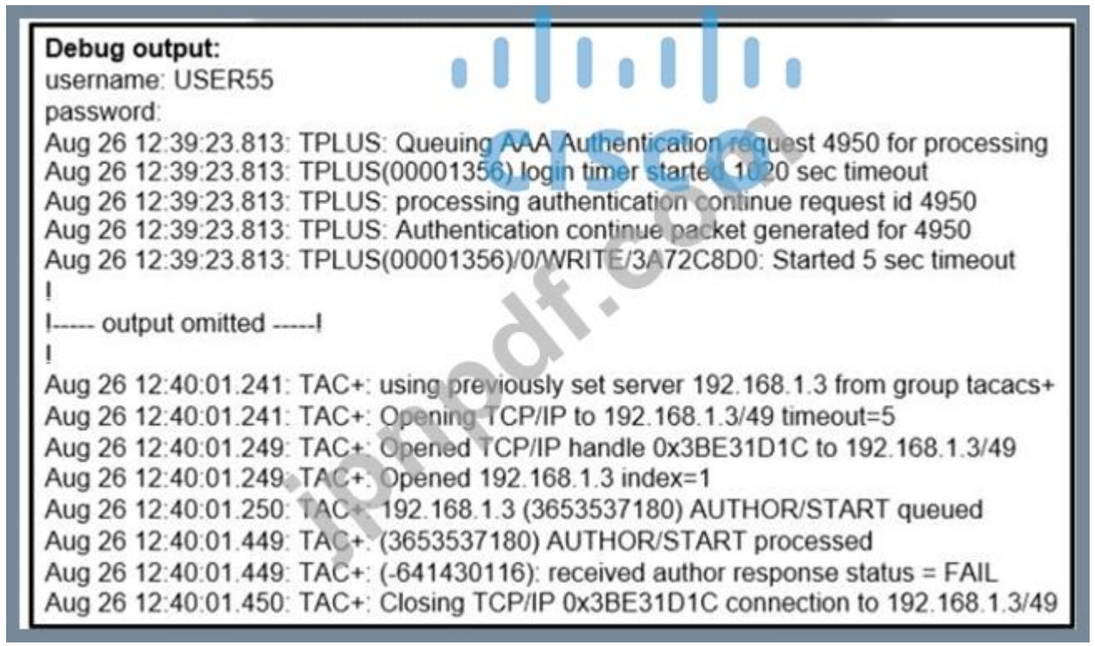
```
R1#show policy-map control-plane
 Control Plane

        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. アクセスリストを変更して2行目を追加し、udp any any eqsnmpを許可します。
B. 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。
C. 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。
D. snmptrapを含めるようにアクセスリストを変更します。
Answer: A (メーッセージを残す**)**

最新問題**: 13**
エンジニアは、デフォルトの属性で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ます。2番目のISPリンクがアップしている場合に、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. LOCAL_PREF
B. MED
C. 重量
D. AS-PATH
Answer: A (メーッセージを残す**)**

最新問題**: 14**
展示を参照してください。



ネットワーク管理者は、TACACS +ユーザー名とパスワードの資格情報を使用してルーターにログインしますが、管理者は特権コマンドを実行できません。問題を解決するアクションはどれですか。

A. TACACS +サーバーからのユーザー名のフルアクセスを構成します

B. このユーザーがこのルーターにアクセスするための承認済みIPアドレスを構成します

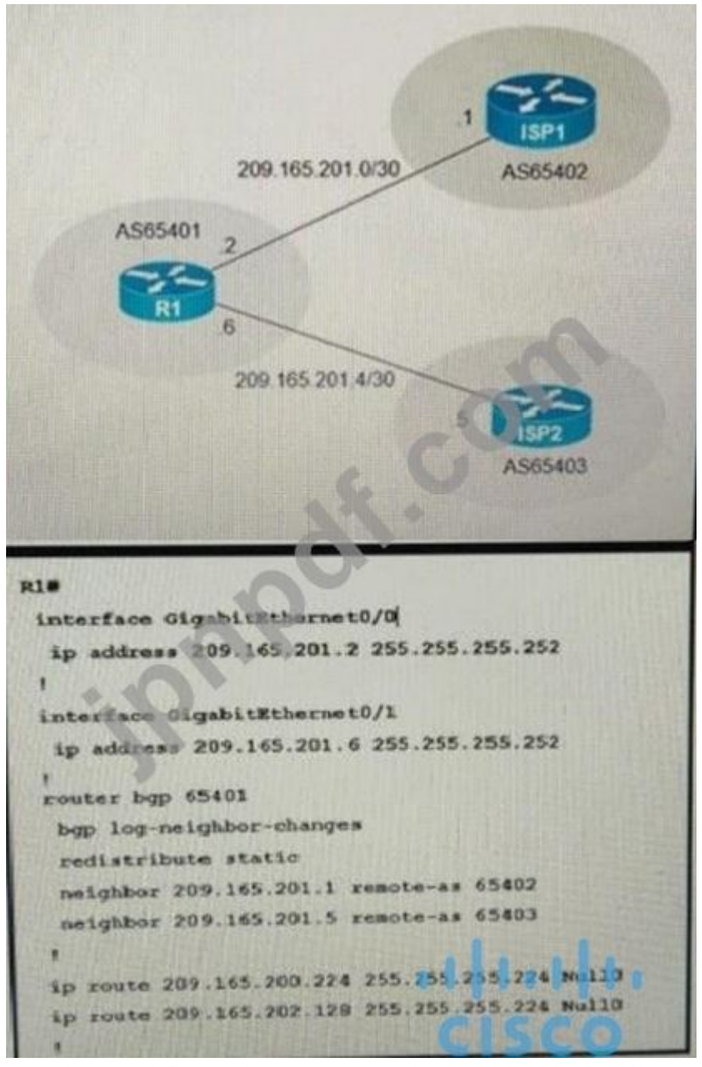
C. ローカルデータベースからユーザー名を構成します

D. ActiveDirectory管理者グループとのTACACS +同期を構成します

Answer: (解答を表示する**)**

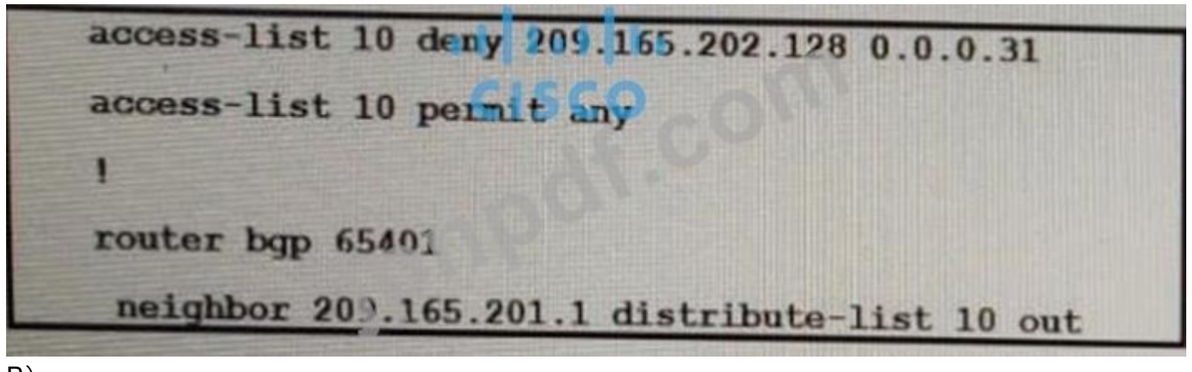
最新問題**: 15**

展示を参照してください。

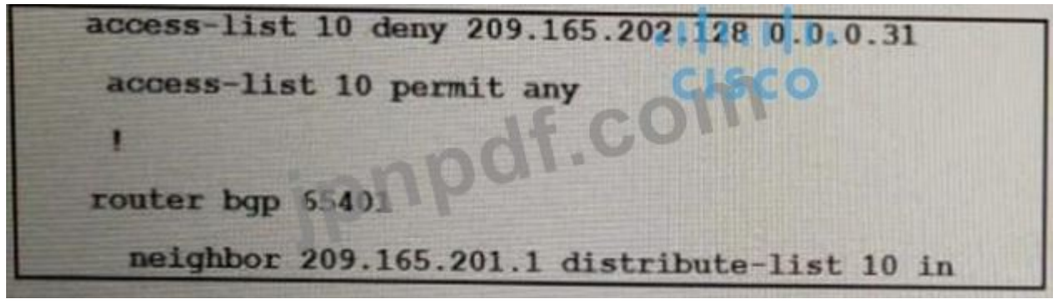


自律システム番号AS65401の会社は、ARINからIPアドレスブロック209.165.200.224/27を取得しました。会社はより多くのIPアドレスを必要とし、ISP2からブロック209.165.202.128/27を割り当てられました。エンジニアはISP1であり、AS65401からISP2ルートを受信していると報告しています。R1のどの構成で問題が解決しますか？

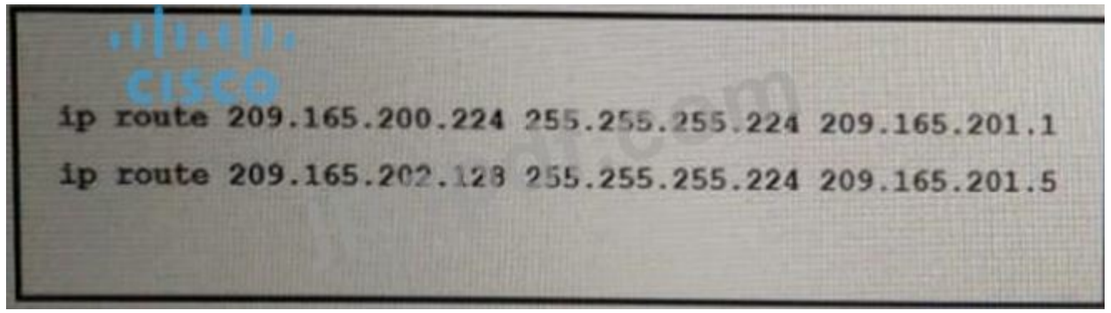
A）



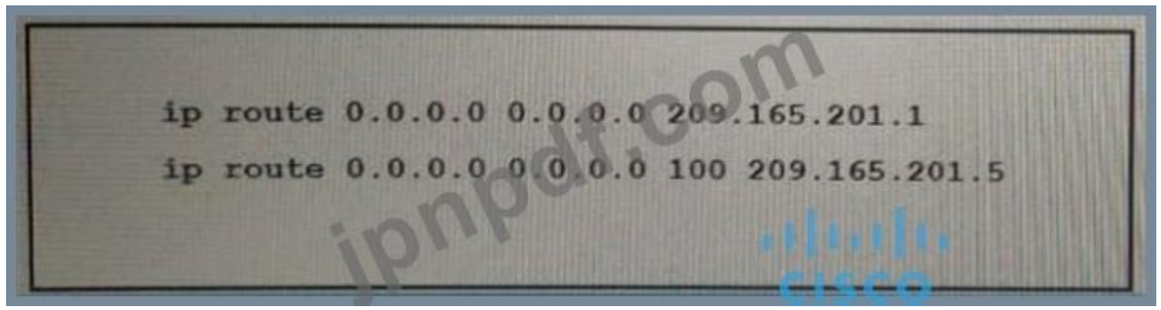
B）



C)

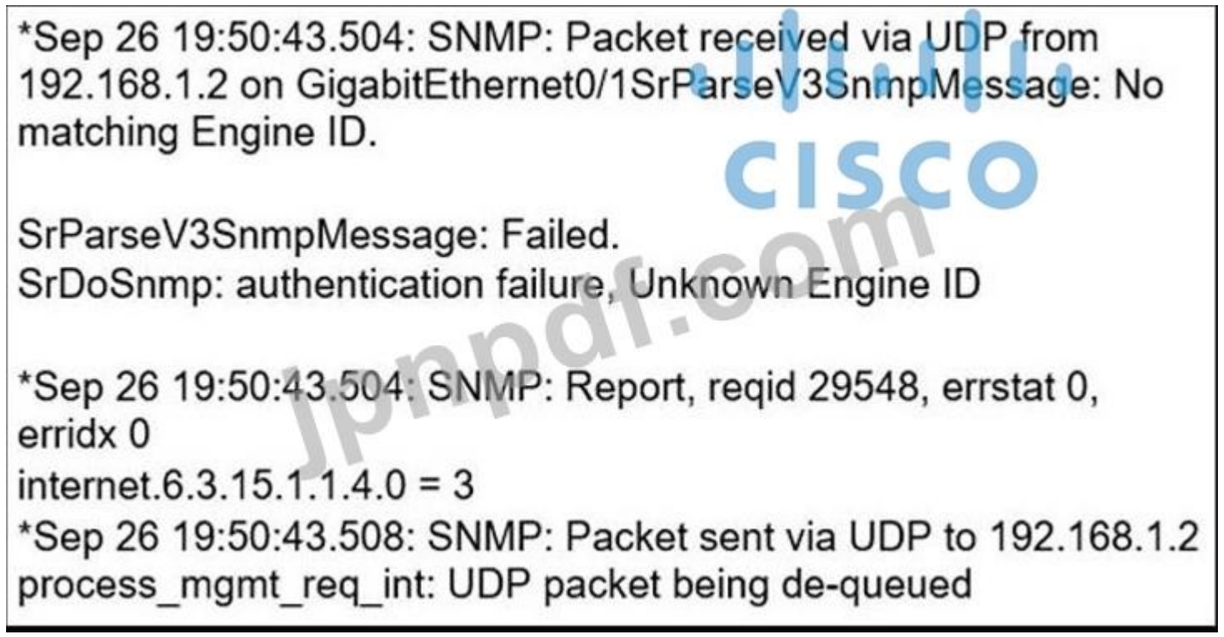


D)



A. オプションA
B. オプションB
C. オプションC
D. オプションD
Answer: A (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/23675-27.html

最新問題**: 16**
展示を参照してください。



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 snmp engine-id

C. debug snmpv3 engine-id

D. SNMPユーザーを表示

E. snmpパケットをデバッグします

Answer: D,E (メーッセージを残す**)**

最新問題**: 17**

展示を参照してください。

エンジニアは、ISP1およびISP2への構成済みのデフォルトルートの到達可能性を監視しています。可能であれば、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. 両方のデフォルトルートに同じADを使用します
C. trackおよびip slaコマンドの番号を照合してIP SLAを開始します
D. 頻度を定義してスケジュールすることにより、IP SLAを開始します。
Answer: D (メーッセージを残す)
Reference:
In the above configuration we have not had activated our IP SLA operation. We can start it with this command:
R1(config)#ip sla schedule 100 life forever start-time now
Also we should specific the rate of ICMP echo:
R1(config-ip-sla-echo)#frequency 5 // Send ICMP echo every 5 seconds

最新問題**: 18**
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. PEセッションとCEセッション間のeBGPパスの関連付け
B. 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
C. 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
D. IPとPEルータIDを組み合わせた48ビットルート
Answer: C (メーッセージを残す)

最新問題**: 19**

MPLSラベルの内容を定義するリストはどれですか。
A. 20-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL
B. 32-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL
C. 20-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit
D. 32-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit
Answer: A (メーッセージを残す)
The first 20 bits constitute a label, which can have 2^20 values. Next comes 3 bit value called Traffic Class. It was formerly called as experimental (EXP) field. Now it has been renamed to Traffic Class (TC). This field is used for QoS related functions. Ingress router can classify the packet according to some criterion and assign a 3 bit value to this filed. If an incoming packet is marked with some IP Precedence or DSCP value and the ingress router may use such a field to assign an FEC to the packet. Next bit is Stack bit which is called bottom-of-stack bit. This field is used when more than one label is assigned to a packet, as in the case of MPLS VPNs or MPLS TE. Next byte is MPLS TTL field which serves the same purpose as that of IP TTL byte in the IP header

最新問題**: 20**
エンジニアは、EIGRPルートを要約し、特にループバックをアドバタイズするようにリークマップコマンドを設定しました
0、IPが10.1.1.1.255.255.255.252、サマリールート。設定が完了した後、特定のループバックアドレスを持つサマリールートを受信しないとお客様から苦情がありました。どの2つの構成がそれを修正しますか？　2つ選択してください。）

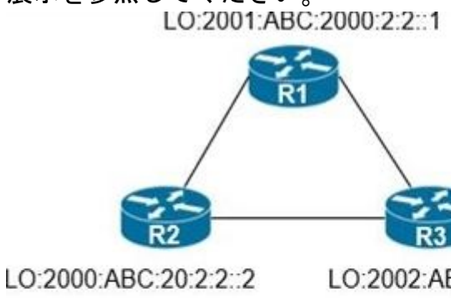
```
router eigrp 1
!
route-map Leak-Route deny 10
!
interface Serial 0/0
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 leak-map Leak-Route
```

A. アクセスリスト1許可10.1.1.1.0.0.0.3を構成します。
B. アクセスリスト1許可10.1.1.1.0.0.0.252を構成します。
C. アクセスリスト1を構成し、ルートマップLeak-Routeで照合します。
D. ルートマップLeak-Route許可10を構成し、アクセスリスト1に一致させます。
E. ルートマップLeak-Route permit 20を構成します。
Answer: (解答を表示する)
When you configure an EIGRP summary route, all networks that fall within the range of your summary are suppressed and no longer advertised on the interface. Only the summary route is advertised. But if we want to advertise a network that has been suppressed along with the summary route then we can use leak-map feature. The below commands will fix the configuration in this question:
R1(
config)#access-list 1 permit 10.1.1.0 0.0.0.3
R1(config)#route-map Leak-Route permit 10 // this command will also remove the "route_map Leak-Route deny 10" command.
R1(config-route-map)#match ip address 1

最新問題**: 21**
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. R2設定からpassive-interfaceコマンドを削除して、R1設定と一致させます。
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. 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。
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: (解答を表示する)

最新問題: **22**
展示を参照してください。ネットワーク管理者は、インターネットに到達するために、デフォルトの静的ルートをすべての内部ルーターに向けてOSPFに再配布しました。内部ルーターによるインターネットへの到達可能性を復元するコマンドのセットはどれですか？
A. router ospf 1
デフォルト情報の発信
B. ルータospf 1
接続された0.0.0.0を再配布します
C. ルーターospf 1
静的サブネットを再配布する
D. ルーターospf 1
ネットワーク0.0.0.00.0.0.0エリア0
Answer: A (メーッセージを残す**)**

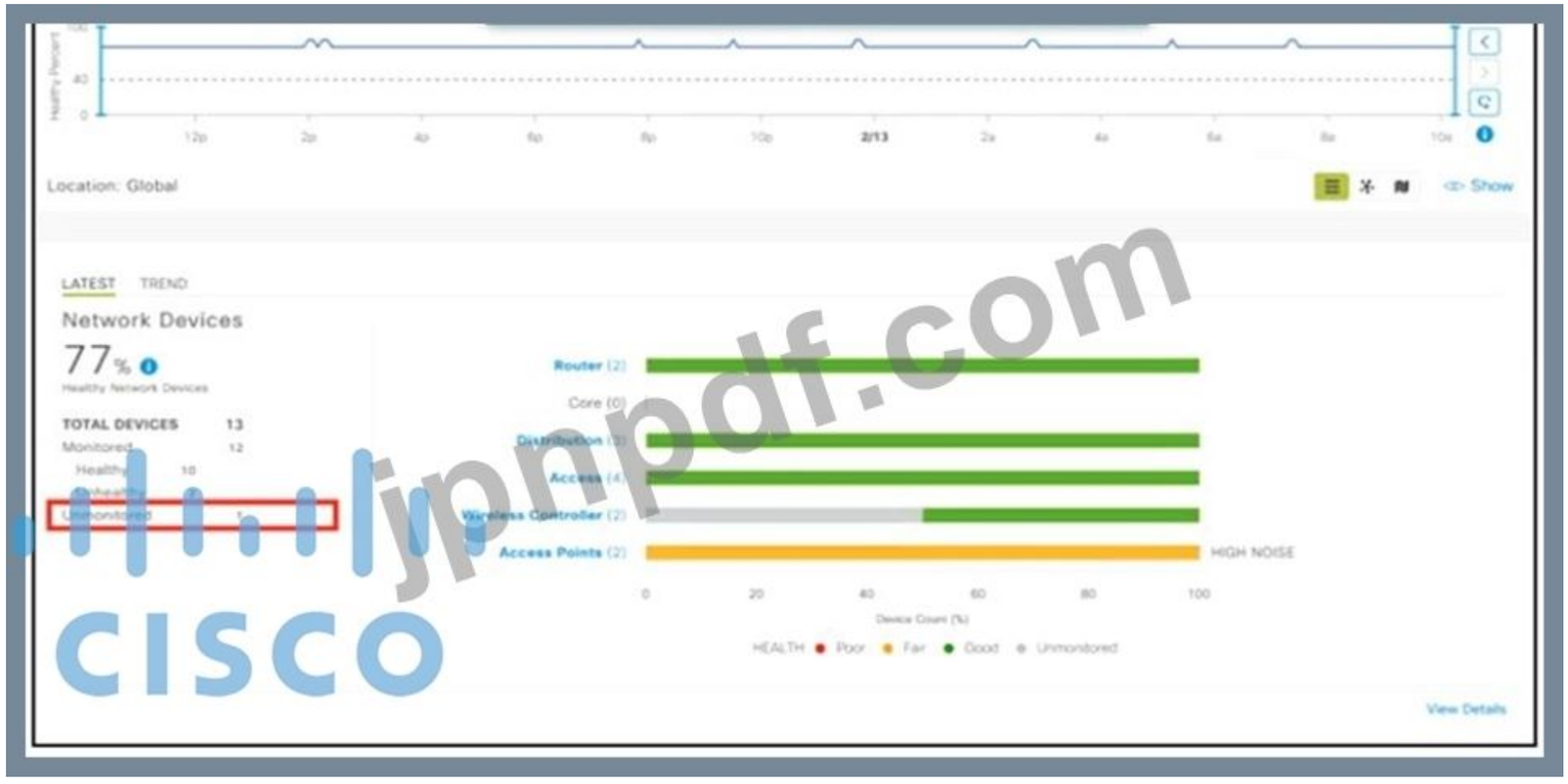
最新問題: **23**
展示を参照してください。




```
IPv6 access list PERMIT_SSH
 10 deny tcp 2001:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
 20 permit tcp 2001:ABC:2000:2:2::/64 host 2000:ABC:20:2:2::2 eq 22
 30 deny tcp 2002:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
 40 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
 50 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
 60 permit tcp host 2002:ABC:2000:2:2::2 host 2000:ABC:20:2:2::2 eq 22
 70 deny ipv6 any any
```

IPv6ネットワークが環境に新たに導入され、ヘルプデスクは、R3がR2のループバックインターフェイスにSSHで接続できないことを報告しています。どのアクションが問題を解決しますか？
A. アクセスリストの10行目を変更して、拒否ではなく許可します。
B. アクセスリストの30行目を変更して、拒否ではなく許可します。
C. アクセスリストから60行目を削除します。
D. アクセスリストから70行目を削除します。
Answer: (解答を表示する**)**

最新問題: **24**
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、ルータで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. Cisco DNACenterに到達するように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**)**

Unmonitored: Unmonitored devices are devices for which Assurance did not receive any telemetry data during the specified time range.

最新問題**: 25**

展示を参照してください。エンジニアは、HQ_R1をプライマリデフォルトゲートウェイとして使用して、BRANCHルーターからHQネットワークへのフローティング静的ルートを正常に設定しました。g0/ 0がHQ_R1でダウンすると、ブランチネットワークはHQネットワーク192.168.20.0/24に到達できなくなります。どの構成セットが問題を解決しますか？

A. BRANCH（config）#p sla 1
BRANCH（config-ip-sta）#cmp-echo 192.168.100.1

B. HQ_R3（config）#pslaレスポンダー
HQ_R3（config）#p sla responseer icmp-echo 172.16.35.1

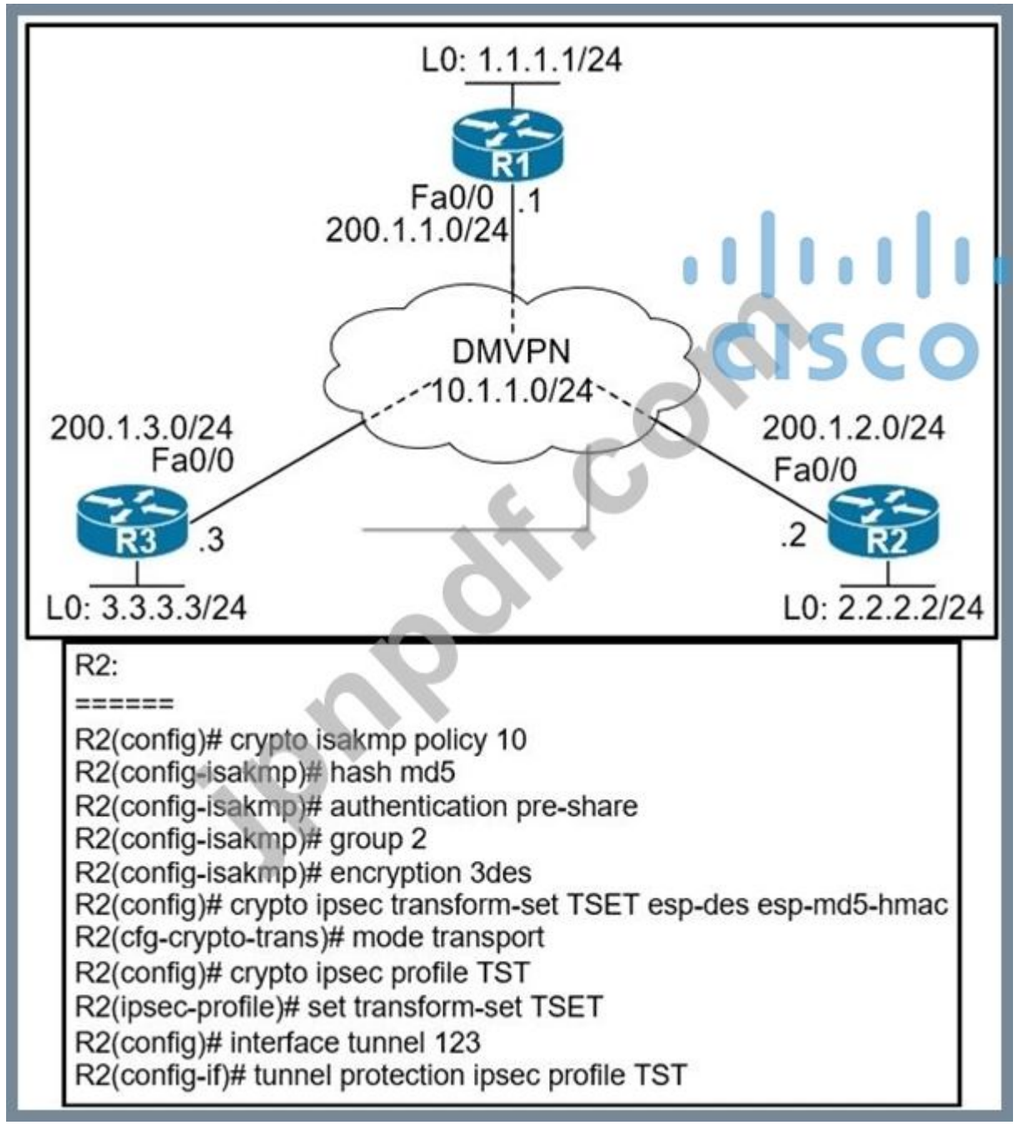
C. HQ R3（config）#pslaレスポンダー
HQ R3（config）#pslaレスポンダーIcmp-echo172.16.35.5

D. BRANCH（config）#p sla 1
BRANCH（config-ip-sla）#cmp-echo 192.168.100.2

Answer: A (メーッセージを残す**)**

最新問題: **26**

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 isakmp keycisco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 isakmp keyciscoアドレス200.1.0.0255.255.0.0を設定します。

D. スポークにcrypto isakmp keyciscoアドレス0.0.0.0を設定します。

Answer: D (メーッセージを残す**)**

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

最新問題: **27**

エンジニアがルータのコンソールセッションのトラブルシューティングを行っており、複数のデバッグコマンドをオンにしています。コンソール画面には、コマンドが正しく入力されているか、出力が表示されているかどうかを確認できないという、スクロールするデバッグメッセージが表示されます。エンジニアがデバッグメッセージの分析を続行しながら、入力されたコンソールコマンドを確認できるようにするアクションはどれですか？

A. loggingsynchronizationコマンドを設定します

B. no loggingconsoleデバッグコマンドをグローバルに設定します

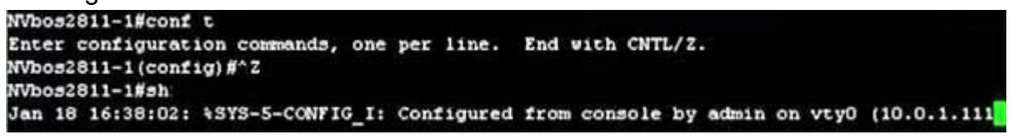
C. logging synchronized levelallコマンドを設定します

D. term nomonコマンドをグローバルに設定します

Answer: A (メーッセージを残す**)**

Let's see how the "logging synchronous" command affect the typing command:

Without this command, a message may pop up and you may not know what you typed if that message is too long. When trying to erase (backspace) your command, you realize you are erasing the message instead.



With this command enabled, when a message pops up you will be put to a new line with your typing command which is very

最新問題: **28**

MPLS LDP自動設定機能でサポートされているIGPはどれですか？

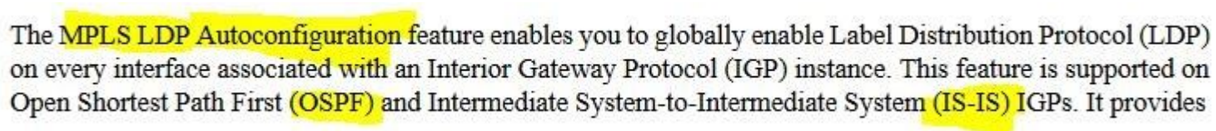
A. RIPv2とOSPF

B. OSPFおよびEIGRP

C. OSPFおよびISIS

D. ISISとRIPv2

Answer: C (メーッセージを残す**)**


The MPLS LDP Autoconfiguration feature enables you to globally enable Label Distribution Protocol (LDP) on every interface associated with an Interior Gateway Protocol (IGP) instance. This feature is supported on Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) IGPs. It provides

最新問題: **29**

展示を参照してください。

ITスタッフが通常の営業時間中にオフィスに来て、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

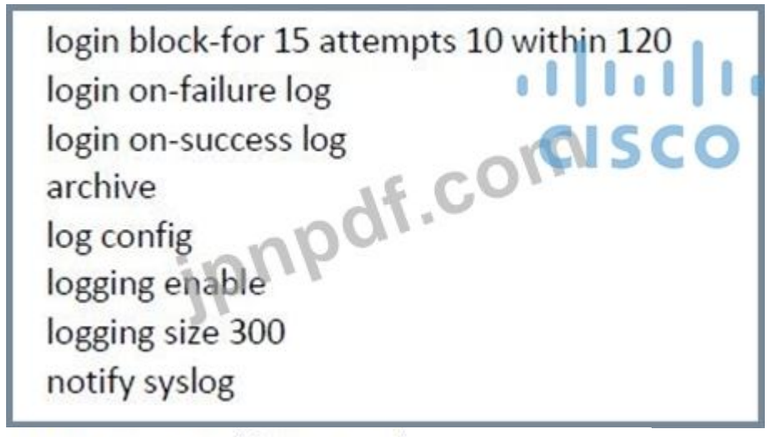
D. アウトバウンド方向のアクセスリストを設定します。

Answer: A (メーッセージを残す**)**

To ACL should be permit tcp 101 10.1.1.1 0.0.0.0

最新問題**: 30**

展示を参照してください。



管理者は、失敗したログイン試行のトラップを確認できますが、成功したログイン試行のトラップを確認することはできません。問題を解決するにはどのコマンドが必要ですか？

A. ログ履歴の構成2

B. ログ履歴の構成3

C. ログ履歴の構成4

D. ログ履歴の構成5

Answer: (解答を表示する**)**

By default, the maximum severity sent as a syslog trap is warning. That is why you see syslog traps for login failures. Since a login success is severity 5 (notifications), those syslog messages will not be converted to traps. To fix this, configure:

logging history 5

Syslog levels are listed below

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

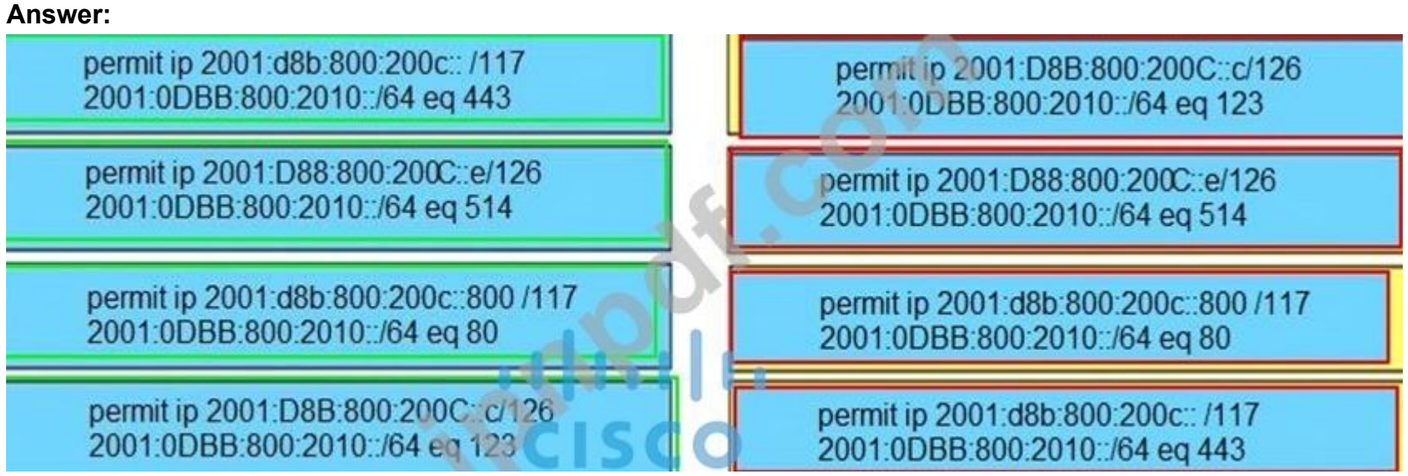
Note:
The syntax of login block is:
login block-for seconds attempts tries within seconds

最新問題**: 31**
複数のスポークデバイスからの複数の接続をサポートするために、マルチポイントトンネルを使用してハブ上に単一のGREトンネルインターフェイスを生成できるCisco VPNテクノロジーはどれですか。
A. FlexVPN
B. DMVPN
C. Cisco Easy VPN
D. GETVPN
Answer: B (メーッセージを残す**)**

最新問題: **32**
展示を参照してください。リモートサーバーがNetFlowデータの受信に失敗しています問題を解決するアクションはどれですか？
A. フロートランスポートコマンドtransport udp 2055を変更して、フローモニタープロファイルの下に移動します。
B. インターレースコマンドをIpフローモニターFLOW-MONITOR-1入力に変更します。
C. フローエクスポータプロファイルの下のudpポートをIpトランスポートudp4739に変更します。
D. フローレコードコマンドレコードv4_r1を変更して、フローエクスポータープロファイルの下に移動します。
Answer: B (メーッセージを残す**)**
From the exhibit we see there are two flow monitors: the first one "FLOW-MONITOR-1" has been configured correctly but the second one "v4_r1" was left empty andinterface E0/0.1 is using it. So the remote server does not receive any NetFlow data.

最新問題: **33**
左側のアドレスを右側の正しいIPv6フィルターの目的にドラッグアンドドロップします。

Answer:



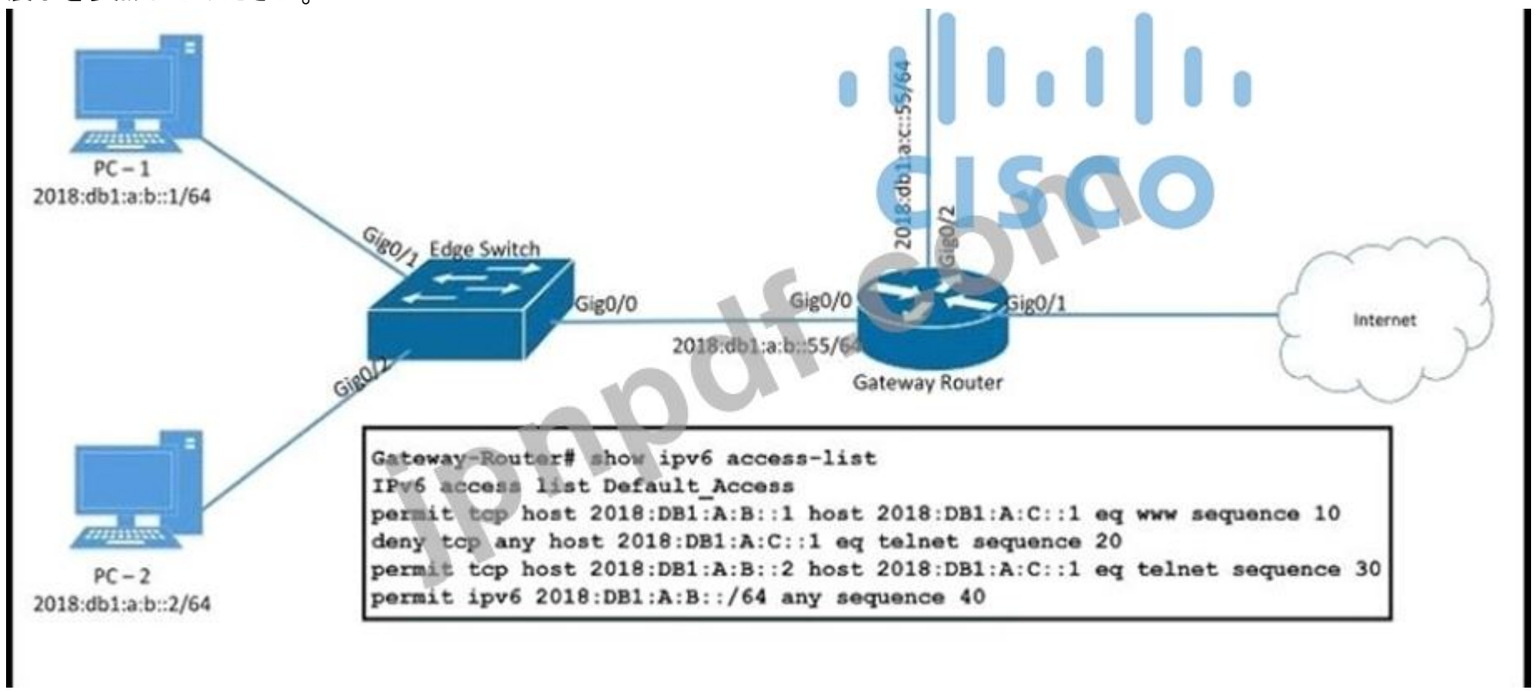
最新問題: **34**
展示を参照してください。

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

A. オプションA
B. オプションB
C. オプションC
D. オプションD
Answer: D (メーッセージを残す**)**
https://community.cisco.com/t5/other-network-architecture/out-of-band-router-access/td-p/333295 The "transport output none" command prevents any protocol connection made from R1.

Therefore our SSH connection to 192.168.12.2 was refused. In order to fix this problem we can configure "transport output ssh" under "line console 0" of R1.
Note: The parameter "-l" specifies the username to log in as on the remote machine.

最新問題**: 35**
展示を参照してください。



PC-2はターミナルサーバーへのTelnet接続の確立に失敗しましたどの構成が問題を解決しますか？

Gateway-Router(config)#**ipv6 access-list Default_Access**
Gateway-Router(config-ipv6-acl)#**sequence 15 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**

Gateway-Router(config)#**ipv6 access-list Default_Access**
Gateway-Router(config-ipv6-acl)#**permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**

Gateway-Router(config)#**ipv6 access-list Default_Access**
Gateway-Router(config-ipv6-acl)#**no sequence 20**
Gateway-Router(config-ipv6-acl)#**sequence 5 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**

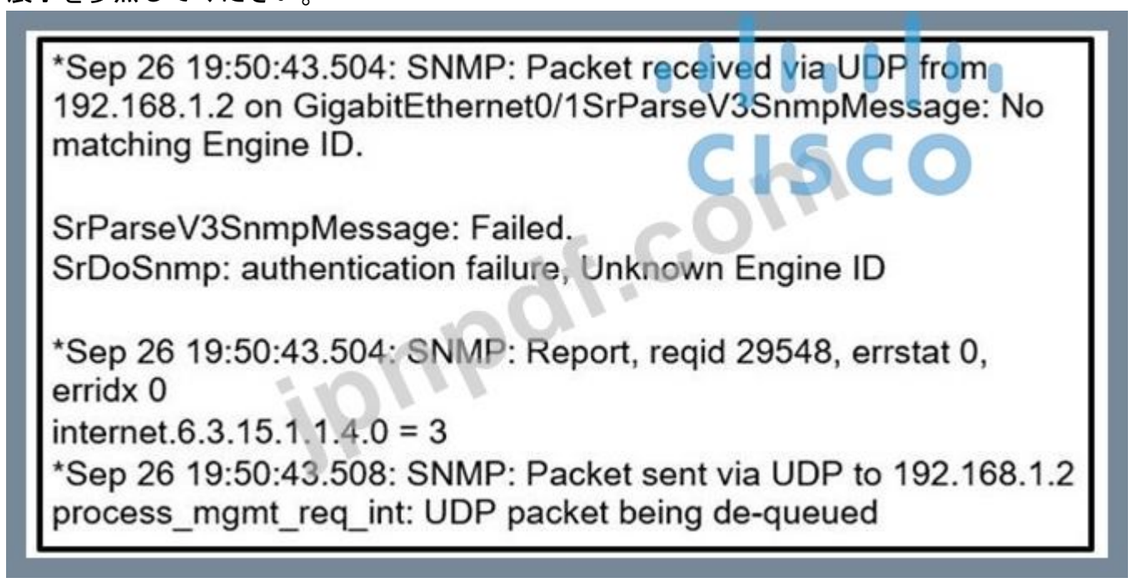
Gateway-Router(config)#**ipv6 access-list Default_Access**
Gateway-Router(config-ipv6-acl)#**sequence 25 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**

A. オプションA
B. オプションB
C. オプションC
D. オプションD
Answer: A (メーッセージを残す**)**
In fact in this question both answer A and answer C are correct but we believe answer A is the better choice as it only allows PC-2 to telnet to terminal server. All other hosts are refused to telnet to terminal server via sequence 20.

最新問題**: 36**

次のコマンドの出力は何ですか。
show ip vrf
A. 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
B. 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。
C. 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
D. ショーのデフォルトのRD値
Answer: D (メーッセージを残す)

最新問題**: 37**
展示を参照してください。



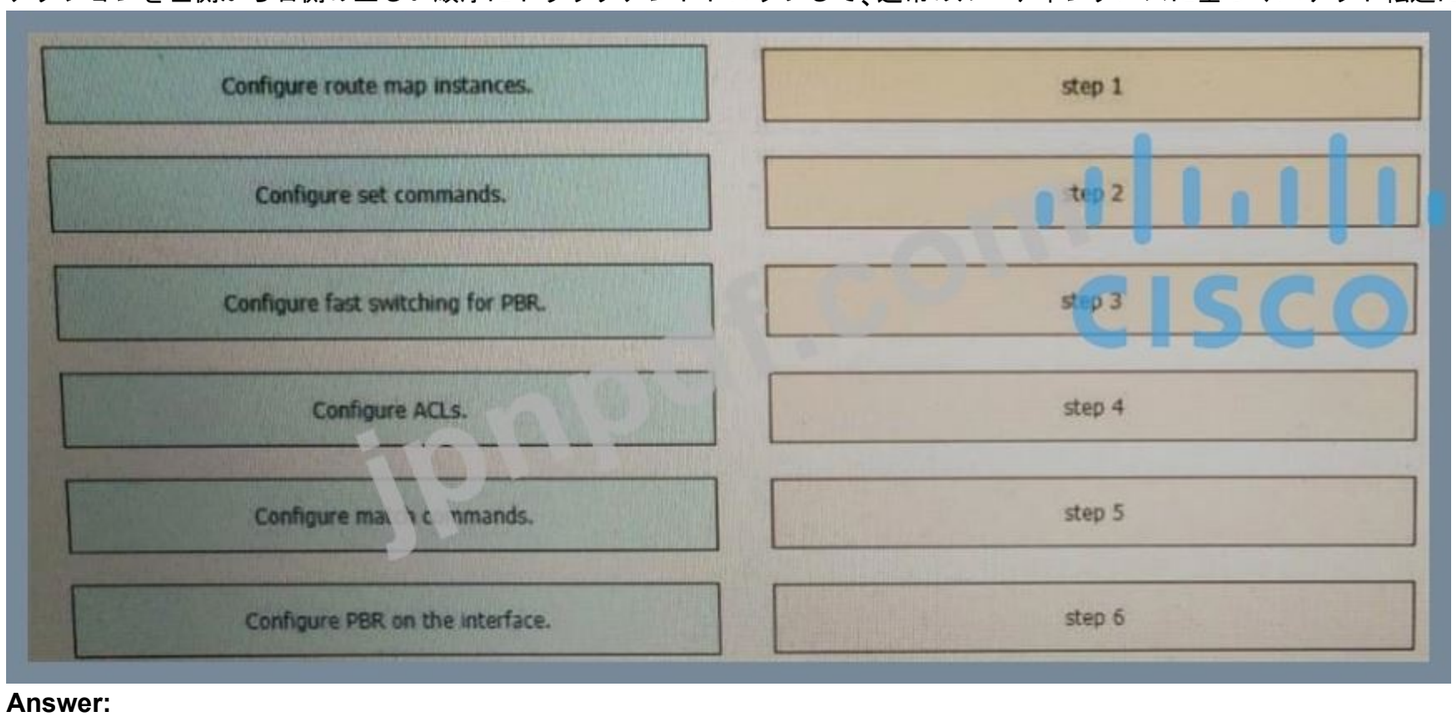
問題を解決するために必要な情報を管理者に提供する2つのコマンドはどれですか？　2つ選択してください。）
A. snmpパケットをデバッグします
B. debug snmp engine-id
C. snmpユーザー
D. showsnmpv3ユーザー
E. debug snmpv3 engine-id
Answer: C,D (メーッセージを残す)

最新問題**: 38**
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。

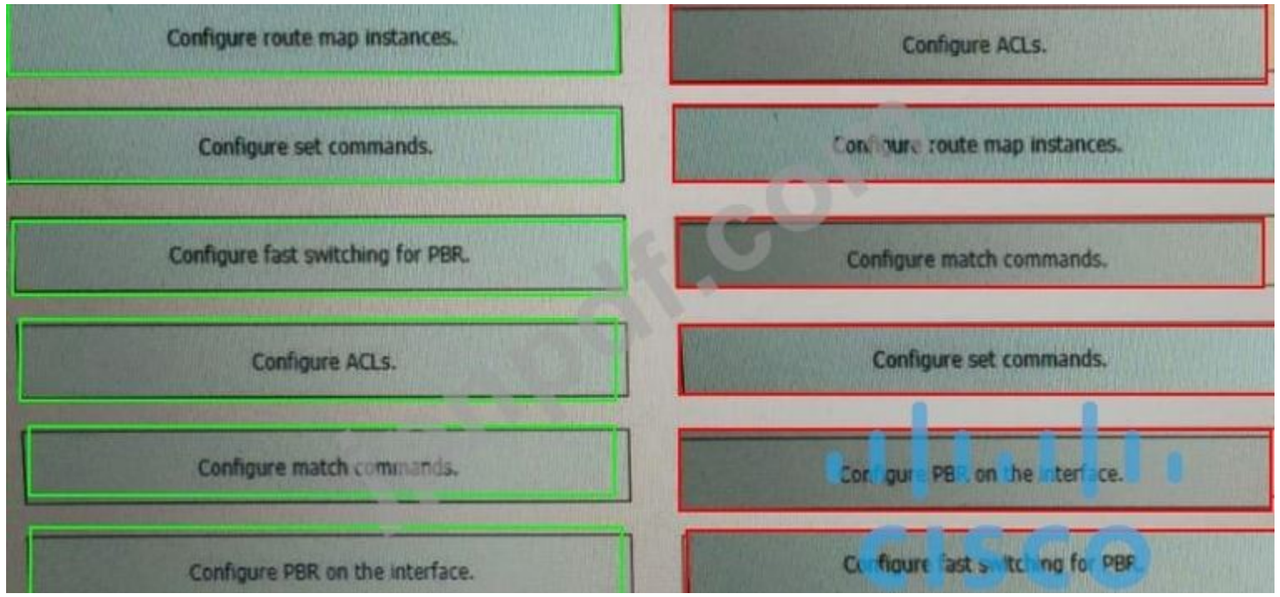
Answer:

最新問題**: 39**

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。

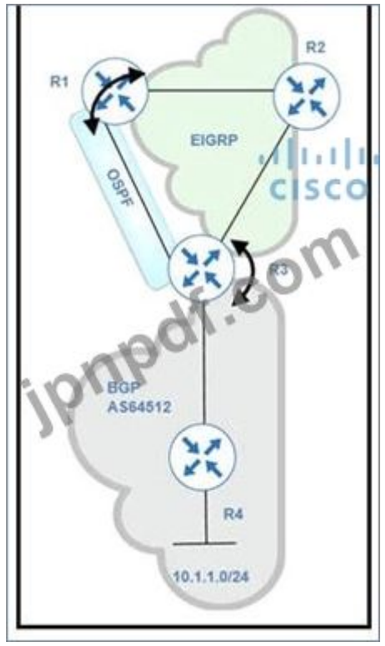


Answer:



最新問題: **40**

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、10.1.1.0724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、debug ip route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付きました。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. 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OSPFSPF計算を減らします。

C. OSPF配布リストアウトバウンドをR3に配置して、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。

D. 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。

Answer: A (メーッセージを残す)

最新問題**: 41**
VRF-Lite構成に関する説明として正しいものはどれですか。 2つ選択してください。）
A. MPLSラベルの交換をサポートします
B. IS-ISをサポートします
C. 最大512.000ルートをサポートします
D. 異なる顧客が異なるVPNでIPアドレスを重複させることができます
E. 各顧客は独自のプライベートルーティングテーブルを持っています。
F. 顧客ごとに専用のTCAMリソースがあります
Answer: D,E (メーッセージを残す)

最新問題**: 42**
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: (解答を表示する**)**
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**: 43**
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 conformed 4000 bps, exceed 0 bps
R1#
```

企業は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付きました。グラフのギャップを解決するものは何ですか？

A. クラスマップから超過レートコマンドを削除します。

B. コントロールプレーンポリシングの一部からクラスマップNMSを削除します。

C. すべてのNMSツールに対応する低い値にCIRレートを構成します

D. NMSクラスマップを、適切なCoPPアクションを持つ特定のプロトコルに基づいて複数のクラスマップに分離します

Answer: (解答を表示する)

Reference:

https://tools.cisco.com/security/center/resources/copp_best_practices

The class-map NMS in the exhibit did not classify traffic into specific protocols so many packets were dropped. We should create some class-map to classify the receiving traffic. It is also a recommendation of CoPP/CPP policy:

"Developing a CPP policy starts with the classification of the control plane traffic. To that end, the control plane traffic needs to be first identified and separated into different class maps."

最新問題: 44

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.(
!
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 (
 !
end
```

ネットワーク管理者は、顧客A用にVRFlite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

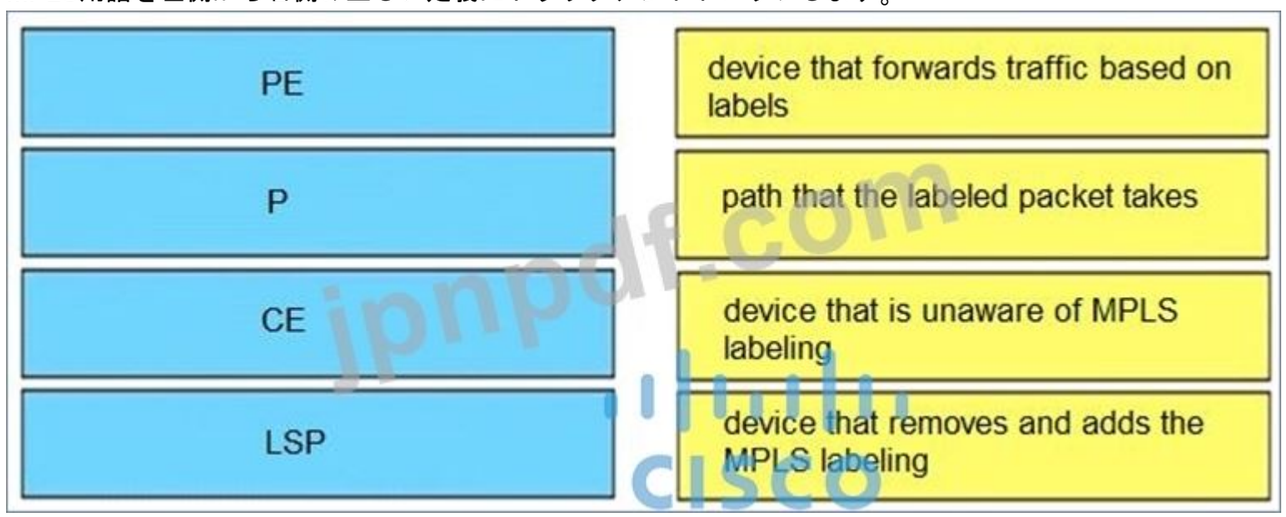
A. オプションA
B. オプションB
C. オプションC
D. オプションD

Answer: (解答を表示する**)**

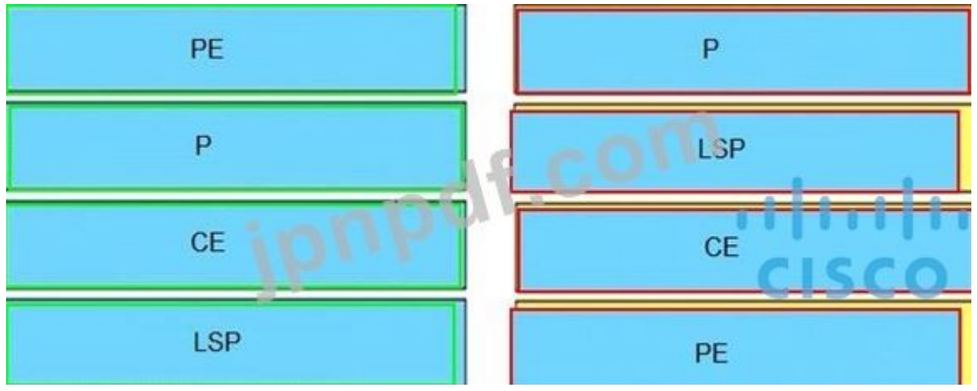
From the exhibit, we learned:

+ VRF customer_a was exported with Route target (RT) of 1:1 so at the remote site it must be imported with the same RT 1:1.
+ VRF customer_a was imported with Route target (RT) of 1:1 so at the remote site it must be exported with the same RT 1:1.
Therefore at the remote site we must configure the command "route-target both 1:1" (which is equivalent to two commands "route-target import 1:1" & "route-target export 1:1".

最新問題**: 45**
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**: 46**
インフラストラクチャでIPv6が有効になっているため、WANを介したIPv6ネットワークで顧客をサポートし、本社をローカルネットワークのブランチオフィスに接続できます。顧客の1人はすでにIPv6を実行しており、ヘッドエンドサイトとブランチサイトの間のDMVPNネットワークインフラストラクチャを介してIPv6を有効にしたいと考えています。mGRE IPv6トンネルネイバーシップを確立するには、どの設定コマンドを適用する必要がありますか？
A. トンネル保護モードipv6
B. ipv6 nhrp holdtime 30
C. ipv6ユニキャストルーティング
D. トンネルモードgreマルチポイントipv6
Answer: D (メーッセージを残す**)**

最新問題: **47**
エンジニアがCiscoIP PhoneのDHCPサーバを設定してTFTPサーバから設定をダウンロードしましたが、IP Phoneが設定を送信できませんでした。問題を解決するには、何を設定する必要がありますか。
A. BOOTPポート67
B. DHCPオプション66
C. BOOTPポート68
D. DHCPオプション69
Answer: (解答を表示する**)**

Command	Purpose
`dhcpd option 66 ascii server_name`	Provides the IP address or name of a TFTP server for option 66.

Example:

```
hostname(config)# dhcpd option 66 ascii
exampleserver
```

DHCP options 3, 66, and 150 are used to configure Cisco IP Phones. Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, ifit does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.+ DHCP option 150 provides the IP addresses of a list of TFTP servers.+ DHCP option 66 gives the IP address or the hostname of a single TFTP server.

最新問題: **48**
展示を参照してください。

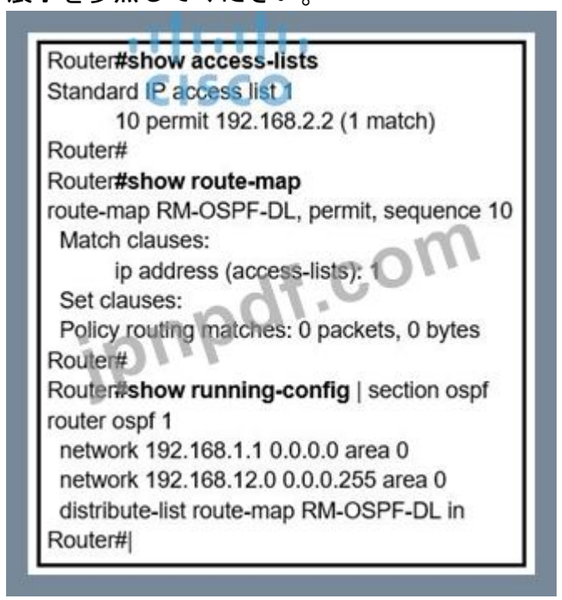
```
R1#show policy-map control-plane
 Control Plane
        Service-policy input: CoPP-BGP
          Class-map: BGP (match all)
            2716 packets, 172071 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: access-group name BGP
            drop

          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. ルータは、指定された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. ルータは、指定された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」。
Answer: (解答を表示する**)**
after bgp session are UP.I configured the CoPP to drop 10.3.3.3 bgp traffic (R3).
R3 bgp traffic that matched the ACL 100 is dropped and the state is in IDLE
---
access-list 100 permit tcp host 10.3.3.3 any eq bgp
access-list 100 permit tcp host 10.3.3.3 eq bgp any
!
class-map match-all class-bgp
match access-group 100
!
policy-map policy-bgp
class class-bgp
drop
!
control-plane
service-policy input policy-bgp
!
The 10.3.3.3 neighbor goes to IDLE

最新問題**: 49**
IPv6ファーストホップセキュリティバインディングテーブルはどの2つの方法で動作しますか？ （2つ選択してください。）
A. 認証を必要とせずにネイバーシップを安全に構築するためのIPv6ルーティングプロトコルによる
B. デバイスの再起動時にバインディングテーブルを回復する回復メカニズムによる
C. IPv6 HSRPにより、ゲートウェイとして使用される前にネイバーが認証されていることを確認します
D. データリンク層アドレスを検証するためのさまざまなIPv6ガード機能による
E. 組み込みIPsec機能のIPsecトンネルのハッシュキーを保存する
Answer: B,D (メーッセージを残す**)**
Overview of the IPv6 First-Hop Security Binding Table
A database table of IPv6 neighbors connected to the device is created from information sources such as NDP snooping. This database, or binding table, is used by variousIPv6 guard features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and the prefix binding of the neighbors to prevent spoofing and redirect attacks.
IPv6 First-Hop Security Binding Table Recovery MechanismThe IPv6 first-hop security binding table recovery mechanism enables the binding table to recover in the event of a device reboot.

最新問題**: 50**

展示を参照してください。



エンジニアは、表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。ルートはまだOSPFルートとしてルーティングテーブルに存在しています。ルートをブロックするアクションはどれですか？

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-DL deny 20。

B. 標準アクセスリストの代わりに拡張アクセスリストを使用します。

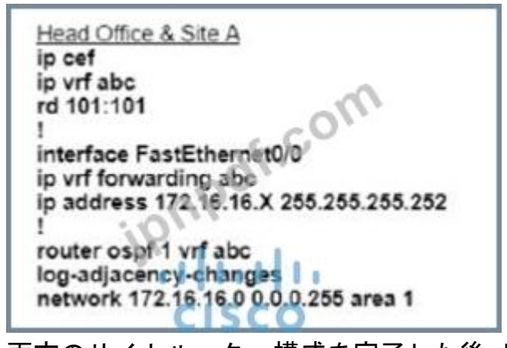
C. ルートマップでアクセスリストの代わりにプレフィックスリストを使用します。

D. route-mapコマンドのシーケンス10を許可から拒否に変更します。

Answer: (解答を表示する)

最新問題**: 51**

エンジニアは、会社の複数エリアのOSPF本社ルーターとサイトA ciscoルーターをVRF liteで構成しました。各サイトルータは、MPLSバックボーンのPEルータに接続されています。



両方のサイトルーター構成を完了した後、LSA 3、4、5、7のいずれもサイト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. 本社の機能vrf-liteとルーターospf 1 vrf abcに接続されたPEルーターを構成します

B. サイトAに機能vrf-liteを構成し、ルーターospf 1 vrf abcの下に接続されたPEルーターを構成します。

C. router ospf 1 vrf abcの下にある本社とサイトAのルーターで機能vrf-liteを構成する

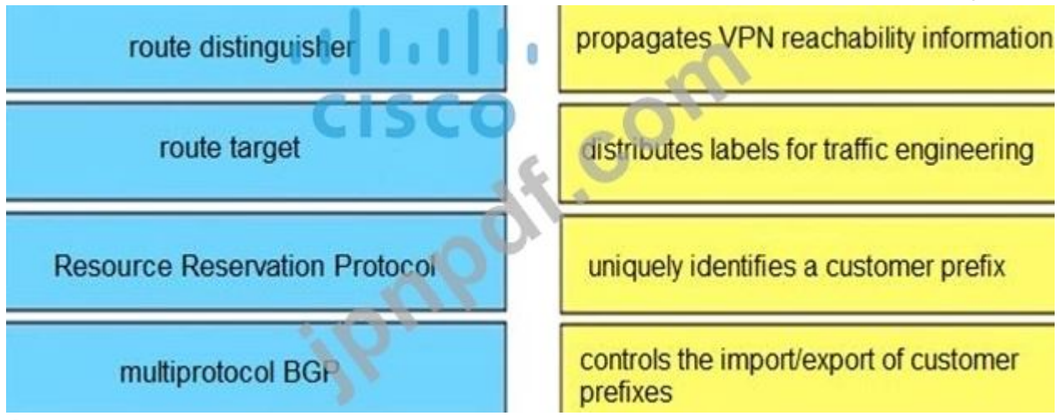
D. routtr ospf 1 vrf abcの下で本社とサイトAルーターに接続されている両方のPEルーターで機能vrf-liteを構成する

Answer: D (メーッセージを残す)

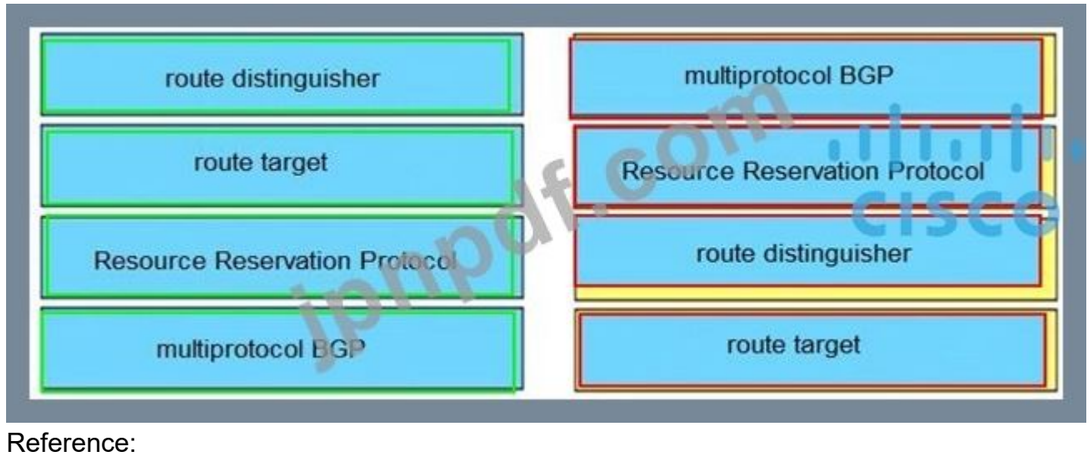
最新問題: **52**
PEルータはIpv4プレフィックスをMPLSVPN内で何に変換しますか？
A. 64ビットルート識別子と組み合わせたVPN-IPv4プレフィックス
B. IPとPEのrouter-idを組み合わせた48ビットルート
C. ASN、PEルータID、およびIPプレフィックスを組み合わせたプレフィックス
D. PEセッションとCEセッション間のeBGPパスの関連付け
Answer: A (メーッセージを残す)

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

最新問題: **53**
MPLS VPNの概念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。



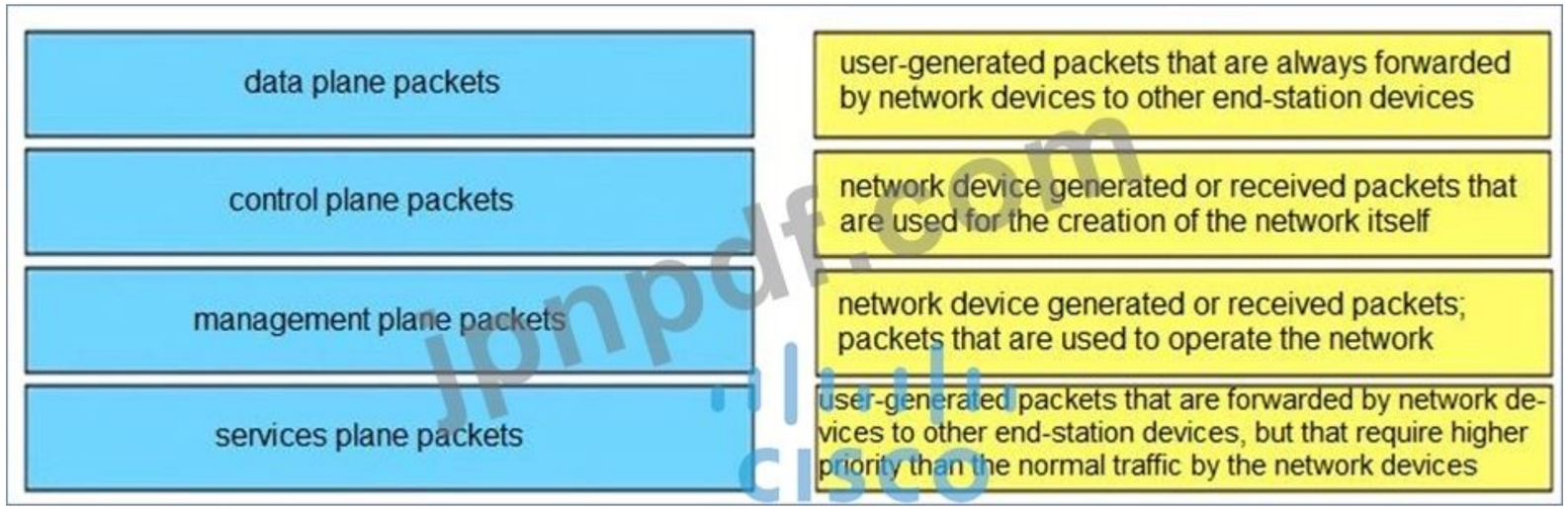
Answer:



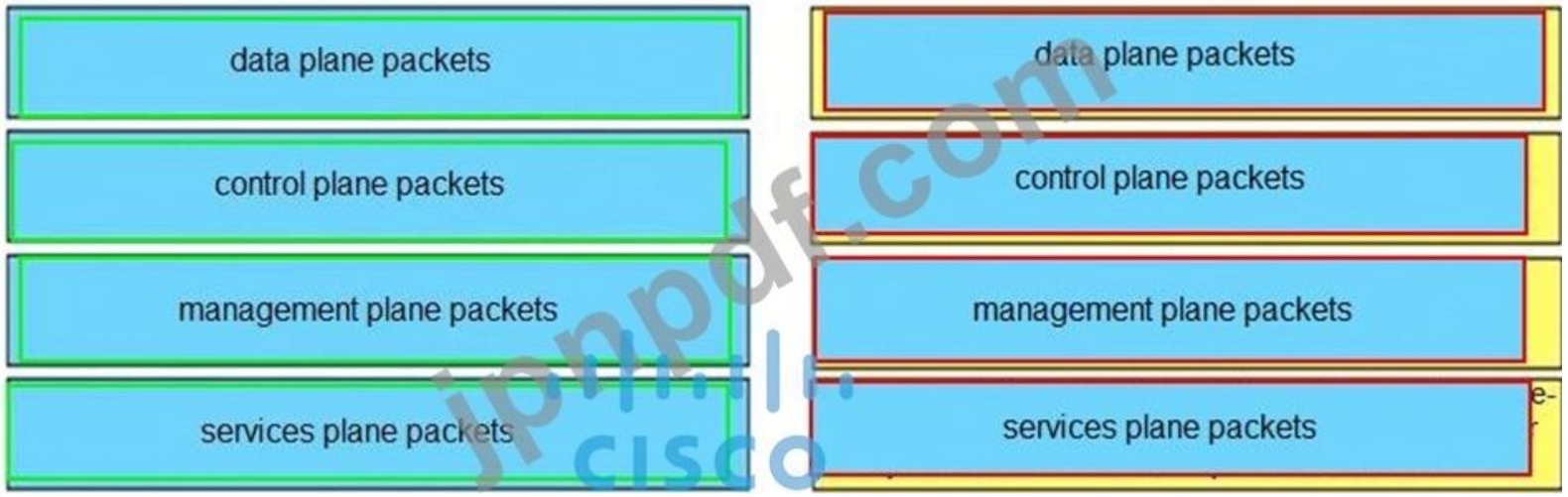
Reference:
https://www.rogerperkin.co.uk/featured/route-distinguisher-vs-route-target/

最新問題: **54**
IPv6 RAガードの制限は何ですか？
A. TCAMがプログラムされている場合、ハードウェアではサポートされません。
B. IPv6トラフィックがトンネリングされる環境では保護されません。
C. 入力方向のスイッチポートインターフェイスでは構成できません
D. IPv6 RAガードによってドロップされたパケットはスパニングできません
Answer: B (メーッセージを残す)
Restrictions for IPv6 RA Guard
The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
This feature can be configured on a switch port interface in the ingress direction.
This feature supports host mode and router mode.
This feature is supported only in the ingress direction; it is not supported in the egress direction.
This feature is not supported on EtherChannel and EtherChannel port members.
This feature is not supported on trunk ports with merge mode.
This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
Packets dropped by the IPv6 RA Guard feature can be spanned.
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16-10/ip6f-xe-16-10-book/ip6-ra-guard.html#GUID-589AF00C-7499-439F-AD23-51005D61CAB7

最新問題: **55**
パケットタイプを左から右側の正しい説明にドラッグアンドドロップします。

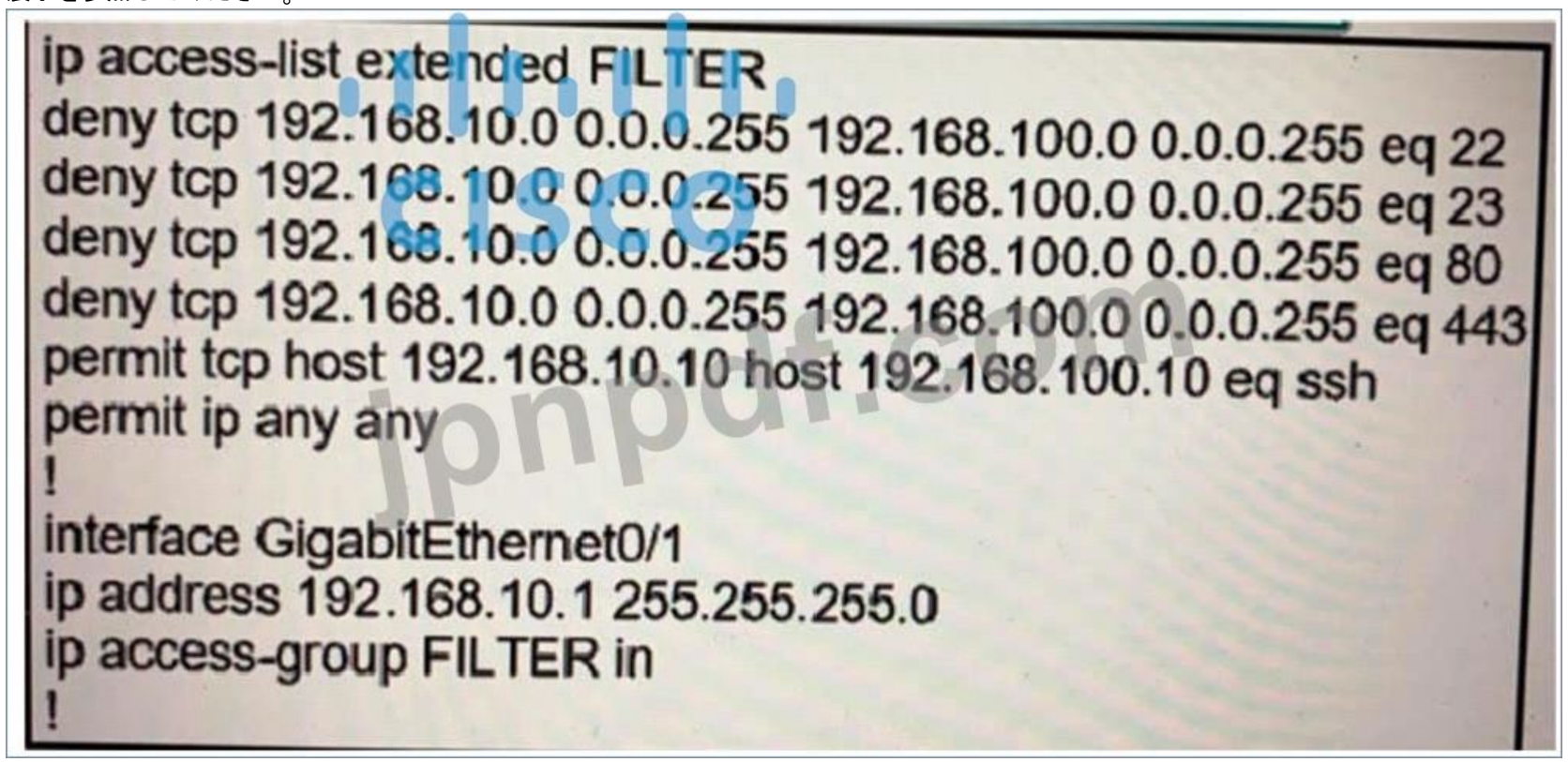


Answer:



最新問題: **56**

展示を参照してください。



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

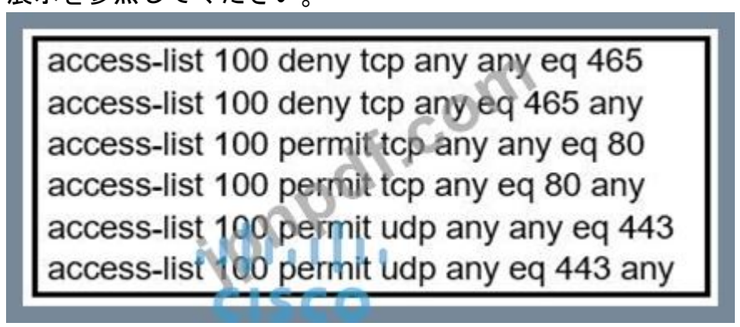
A. インターフェースから一時的にACLを削除して、フローが機能するかどうかを確認します

B. 一時的にpermit ip any any行をACLの先頭に移動して、フローが機能するかどうかを確認します

C. SSHエントリをACLの先頭に移動します

D. show access-list FILTERコマンドを実行して、SSHエントリにヒット統計が関連付けられているかどうかを確認します
Answer: C (メーッセージを残す)

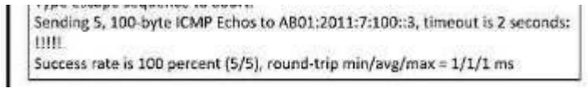
最新問題**: 57**
展示を参照してください。



トラブルシューティング中に、安全なWebブラウザーを使用してデバイスに到達できないことが発見されました。問題を解決するには何が必要ですか？
A. tcpポート22を許可します
B. UDPポート465を許可します
C. tcpポート465を許可します
D. tcpポート443を許可します
Answer: D (メーッセージを残す)

最新問題**: 58**
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 elgrp 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 (メーッセージを残す)
In this topology, Chicago router (Hub) will receive advertisements from Los Angeles (Spoke1) router on its tunnel interface. The problem here is that it also has a connection with New York (Spoke2) on that same tunnel interface. If we don't disable EIGRP split-horizon, then the Hub will not relay routes from Spoke1 to Spoke2 and the other way around. That is because it received those routes on interface Tunnel1 and therefore it cannot advertise back out that same interface (splithorizon rule). Therefore we must disable split-horizon on the Hub router to make sure the Spokes know about each other.

最新問題**: 59**
展示を参照してください。



エンジニアがルータR1とR3の間にBGPを設定しました。BOP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。どの構成がこの問題を解決しますか？

A. R1
router bgp 6501
address-family ipv6
neighbor AB01:2011:7:100;:3 activate
B. R3
router bgp 6502
neighbor AB01:2011:7:100::1 ebgp-muttlhop 255
C. R3
router bgp 6502
address-family ipv6
neighbor AB01:2011:7:100::1 activate
D. R1
router bgp 6501 neighborAB01:2011:7:100::3ebgp-multihop255
Answer: (解答を表示する**)**

最新問題**: 60**
展示を参照してください。

198A :0 :200C :: 1/64からルーター2へのTelnetトラフィックを拒否する構成はどれですか？
NS）

```
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
!
```

NS）

```
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
!
```

NS）

```
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
!
```

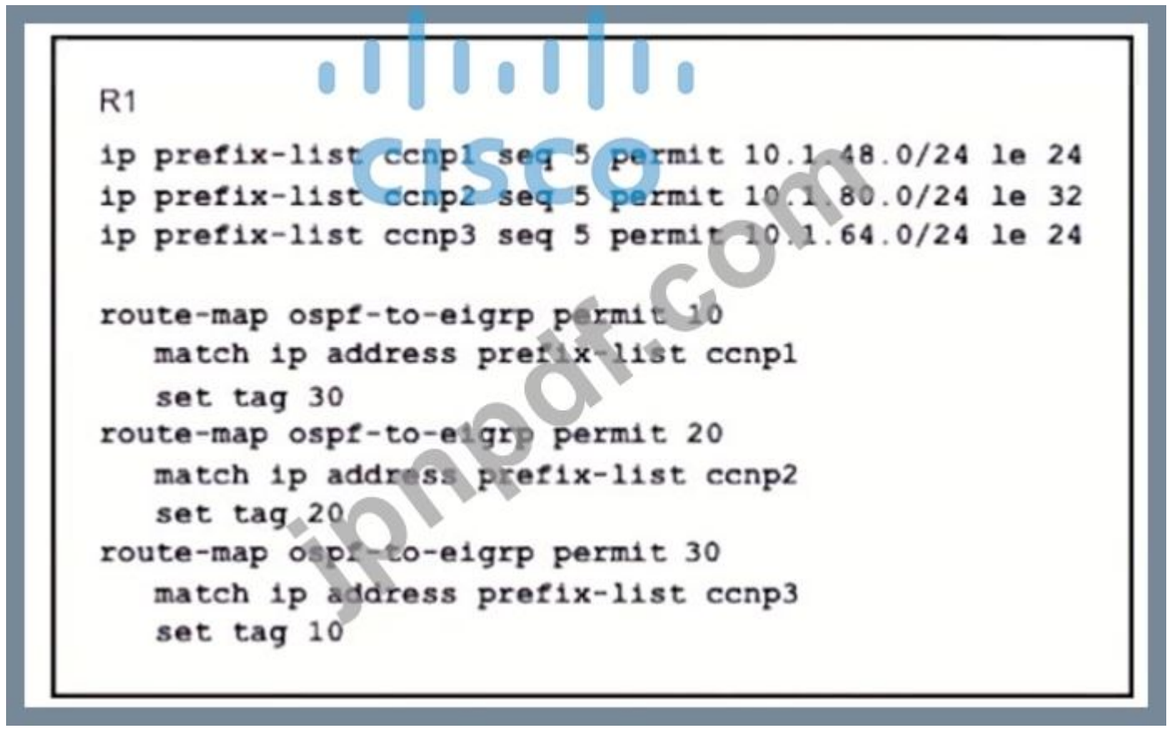
NS）

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

最新問題**: 61**
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. パケットはルーティングテーブルに基づいて転送されます。
C. パケットは静的ルート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: D (メーッセージを残す**)**
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**: 62**
展示を参照してください。



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. route-map ospf-to-eigrp permit 10を変更し、prefix-listccnp2と一致させます。

B. プレフィックスリストccnp3を変更して、10.1.64.0 / 20 le24を追加します。

C. route-map ospf-to-eigrp permit 30を変更し、prefix-listccnp2と一致させます。

D. プレフィックスリストccnp3を変更して、10.1.64.0 / 20 ge32を追加します。

Answer: A (メーッセージを残す**)**

最新問題**: 63**

悪意のあるトラフィックからルーターを保護するためにルーターでコントロールプレーンポリシングを構成する場合、エンジニアは、構成されたルーティングプロトコルがそのデバイスでフラッピングを開始することを確認します。コントロールプレーンポリシーのどのアクションが、セキュリティ目標を達成しながら本番環境でこの問題を防止しますか？

A. ACLと送信レートをテストし、出力方向にコントロールプレーンポリシーを適用するために最初に送信するconform-actionとexceed-actionを設定します

B. ACLと送信レートをテストし、入力方向にコントロールプレーンポリシーを適用するために、conform-actionを送信し、exceed-actionをドロップするように設定します

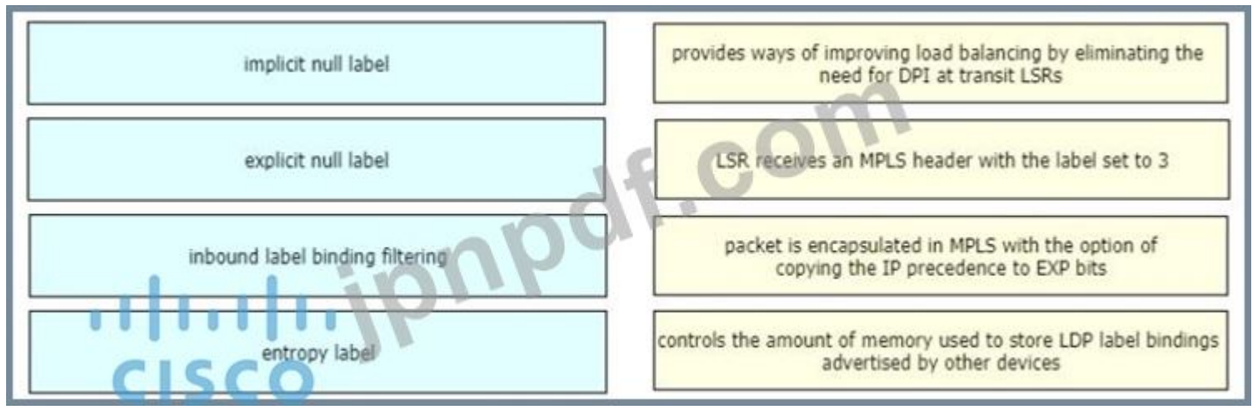
C. ACLと送信レートをテストし、入力方向にコントロールプレーンポリシーを適用するために最初に送信するconform-actionとexceed-actionを設定します

D. ACLと送信レートをテストし、出力方向にコントロールプレーンポリシーを適用するために、conform-actionを送信し、exceed-actionをdropに設定します。

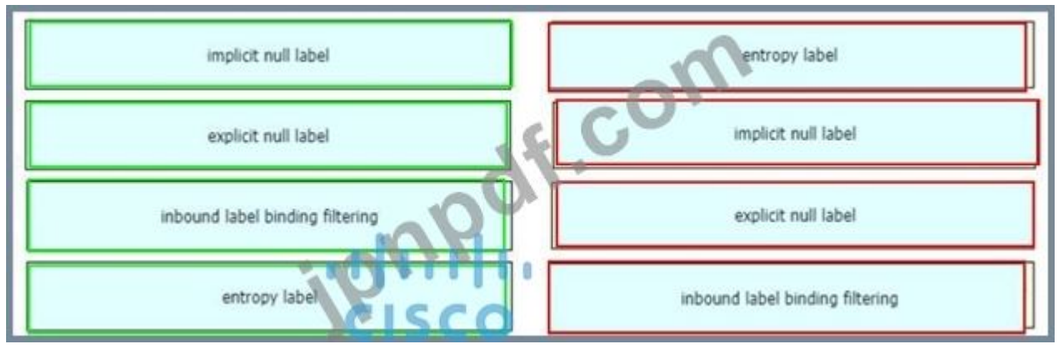
Answer: (解答を表示する**)**

最新問題**: 64**

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:



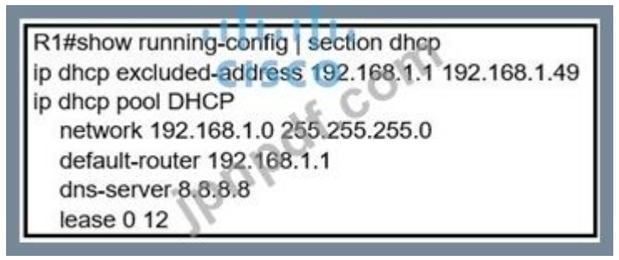
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/15-sy/mp-ldp-15-sy-boo k/mp-ldp-inbound-filtr.html

最新問題: **65**
MPLS VPNのどのコンポーネントを使用してIPアドレスを拡張すると、エンジニアはそれがどのVPNに属しているかを識別できますか？
A. VPNv4 address family
B. RD
C. RT
D. LDP
Answer: B (メーッセージを残す**)**

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

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

最新問題: **66**
展示を参照してください。



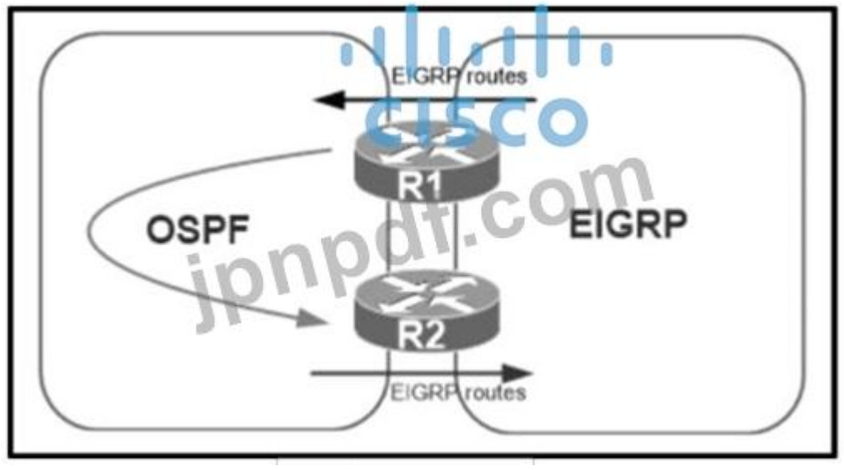
ユーザーから、DHCPサーバーからIPアドレスを取得できないことが報告されています。DHCPサーバーは、次のように構成されています。合計約300人の非同時ユーザーがこのDHCPサーバーを使用していますが、1日あたり2時間を超えてアクティブになるユーザーはいません。現在のリソース内の問題を修正するアクションはどれですか？

A. network 192.168.2.0 255.255.255.0コマンドをDHCPプールに追加します
B. DHCPリース時間をより小さい値に設定します
C. DHCPリース時間をより大きな値に設定します
D. DHCPプールでサブネットマスクをnetwork 192.168.1.0 255.255.254.0コマンドに変更します。
Answer: B (メーッセージを残す)

最新問題**: 67**
エンジニアは、ルータからネットワーク内の他のデバイスへの安全な接続を開始するようにCiscoルータを設定する必要がありますが、失敗し続けます。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. 開始するSSH接続の送信元ポートを構成します
B. TACACS +サーバーを構成して有効にします
C. コンソールでtransport inputsshコマンドを設定します
D. ドメイン名を設定します
E. 生成する暗号鍵を構成します
Answer: D,E (メーッセージを残す)
Follow these guidelines when configuring the switch as an SSH server or SSH client:
+ An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.+ If the SSH server is running on a stack master and the stack master fails, the new stack master uses the RSA key pair generated by the previous stack master
+ If you get CLI error messages after entering the crypto key generate rsa global configuration command, an RSA key pair has not been generated. Reconfigure thehostname and domain, and then enter the crypto key generate rsa command.+ When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the hostname globalconfiguration command.+ When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the ip domain-nameglobal configuration command.+ When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

最新問題**: 68**
展示を参照してください。



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

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. 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でEIGRPをOSPFに再配布するときにルートマップにタグを設定し、R2で同じタグを一致させてOSPFをEIGRPに再配布するときに拒否します。

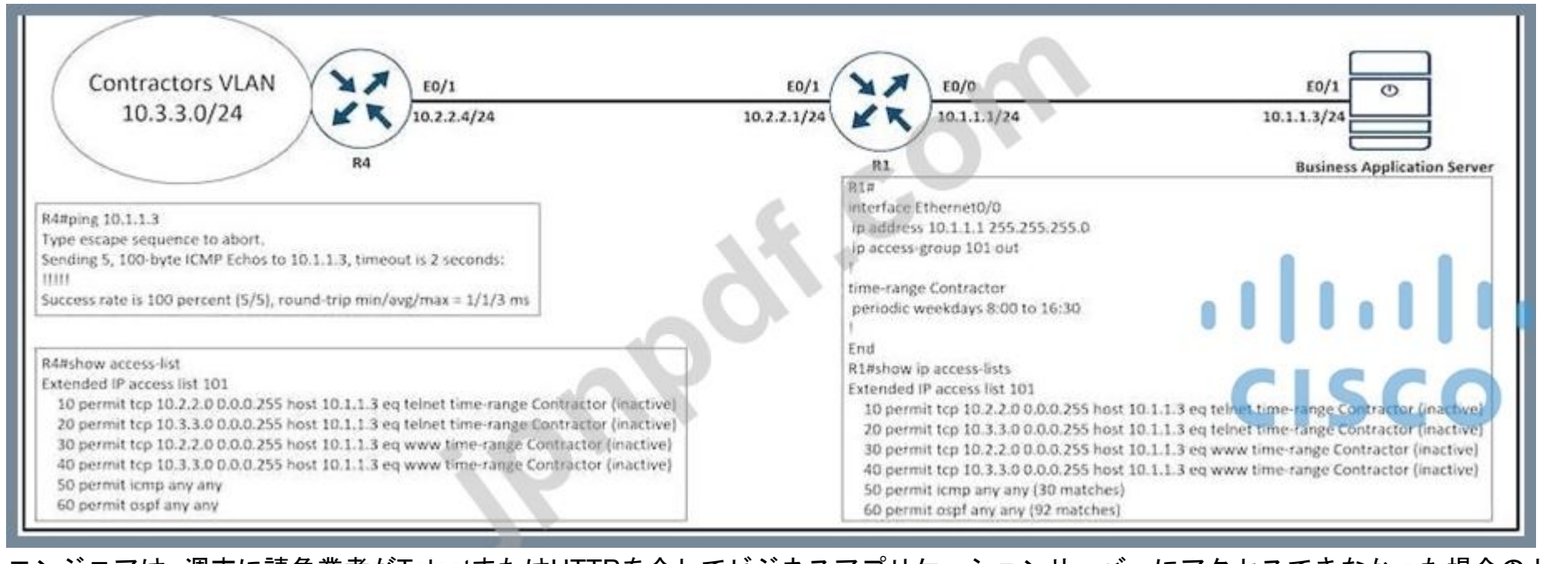
D. EIGRPのサマリールートをOSPFにアドバタイズし、OSPFに再配布するときに特定のEIGRPルートを拒否します。

Answer: C (メーッセージを残す)

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

最新問題**: 69**

展示を参照してください。



エンジニアは、週末に請負業者がTelnetまたはHTTPを介してビジネスアプリケーションサーバーにアクセスできなかった場合のトラブルシューティングを行っています。どの構成で問題が解決しますか？

NS）

R1
time-range Contractor
 no periodic weekdays 8:00 to 16:30
 periodic daily 8:00 to 16:30

NS）

R4
time-range Contractor
 no periodic weekdays 17:00 to 23:59
 periodic daily 8:00 to 16:30

NS）

R4
 no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor

NS）

R1
 no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor

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

最新問題**: 70**
サービスプロバイダーがLVPNMPLSアプリケーションを利用するために必要な2つのコンポーネントはどれですか。 2つ選択してください。）
A. Pルーターは、PEルーターに向けてMP-iBGP用に構成する必要があります
B. PルーターはRSVPで構成する必要があります。
C. PEルータは、他のPEルータとのMP-iBGP用に設定する必要があります
D. PEルータは、MP-eBGPがCEに接続するように設定する必要があります
E. PおよびPEルーターはLDPまたはRSVPで構成する必要があります
Answer: C,E (メーッセージを残す)
MPLS Network Protocols
+ IGP: OSPF, EIGRP, IS-IS on core facing and core links+ RSVP and/or LDP on core and/or core facing links ->
+ MP-iBGP on PE devices (for MPLS services), MP-BGP: Multiprotocol Border Gateway Protocol, used for MPLS L3 VPN -> .

最新問題**: 71**
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: (解答を表示する**)**

If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default.

You can redistribute both internal and external (type-1 & type-2) OSPF routes via this command: -Router(config-router)#redistribute ospf 1 match internal external 1 external 2

最新問題**: 72**

展示を参照してください。

```
Router# show ip route

     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Ethernet0/0
C    3.0.0.0/8 is directly connected, Serial1/0
O E2 200.1.1.0/24 [110/20] via 2.2.2.2, 00:16:17, Ethernet0/0
O E1 200.2.2.0/24 [110/104] via 2.2.2.2, 00:00:41, Ethernet0/0
     131.108.0.0/24 is subnetted, 2 subnets
O       131.108.2.0 [110/74] via 2.2.2.2, 00:16:17, Ethernet0/0
O IA    131.108.1.0 [110/84] via 2.2.2.2, 00:16:17, Ethernet0/0

Router# show ip bgp

  Network          Next Hop            Metric LocPrf Weight Path
*> 2.2.2.0/24      0.0.0.0                  0         32768 ?
*> 131.108.1.0/24  2.2.2.2                 84         32768 ?
*> 131.108.2.0/24  2.2.2.2                 74         32768 ?
```

OSPFルーティングプロトコルはBGPルーティングプロトコルに再配布されますが、すべてのOSPFルートがBGPに配布されるわけではありません。問題を解決するアクションはどれですか。

A. redistributeコマンドにexternalという単語を含めます

B. route-mapコマンドを使用して、アクセスリストで定義されたOSPF外部ルートを再配布します。

C. redistributeコマンドにinternalexternalという単語を含めます

D. route-mapコマンドを使用して、プレフィックスリストで定義されたOSPF外部ルートを再配布します。

Answer: C (メーッセージを残す)

If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default. You can use the internal keyword along with the redistribute command under router bgp to redistribute OSPF intra- and inter-area routes.

Use the external keyword along with the redistribute command under router bgp to redistribute OSPF external routes into BGP.

-> In order to redistribute all OSPF routes into BGP, we must use both internal and external keywords. The full command would be (suppose we are using OSPF 1):

redistribute ospf 1 match internal external

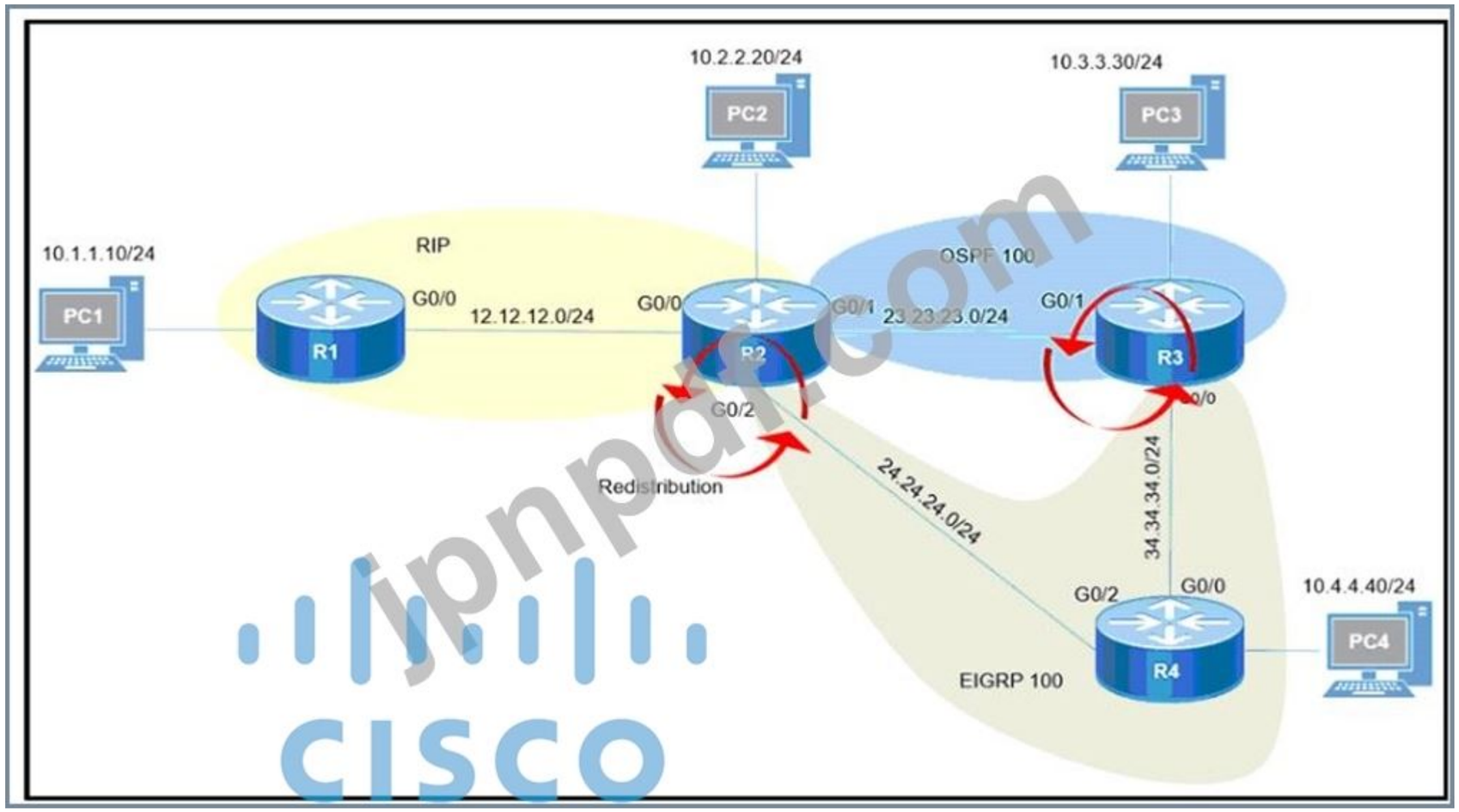
Note: The configuration shows match internal external 1 external 2. This is normal because OSPF automatically appends "external 1 external 2" in the configuration. In other words, keyword external = external 1 external 2. External 1 = O E1 and External 2 = O E2.

Reference:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5242-bgp-ospf-redi s.html

最新問題: 73

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、およびPC4がPC1に到達できない。問題を解決する2つの解決策は何ですか？　2つ選択してください。）

A. R2のRIPに再配布するときにRIPルートをフィルターしてRIPに戻す

B. R2のRIPに再配布するときに、OSPFルートをRIP FROM EIGRPにフィルターします。

C. R2のEIGRPに再配布するときに、RIPルートを除くすべてのルートをフィルタリングします。

D. R2でOSPFに再配布するときに、RIPおよびOSPFルートをフィルターしてEIGRPからOSPFに戻します

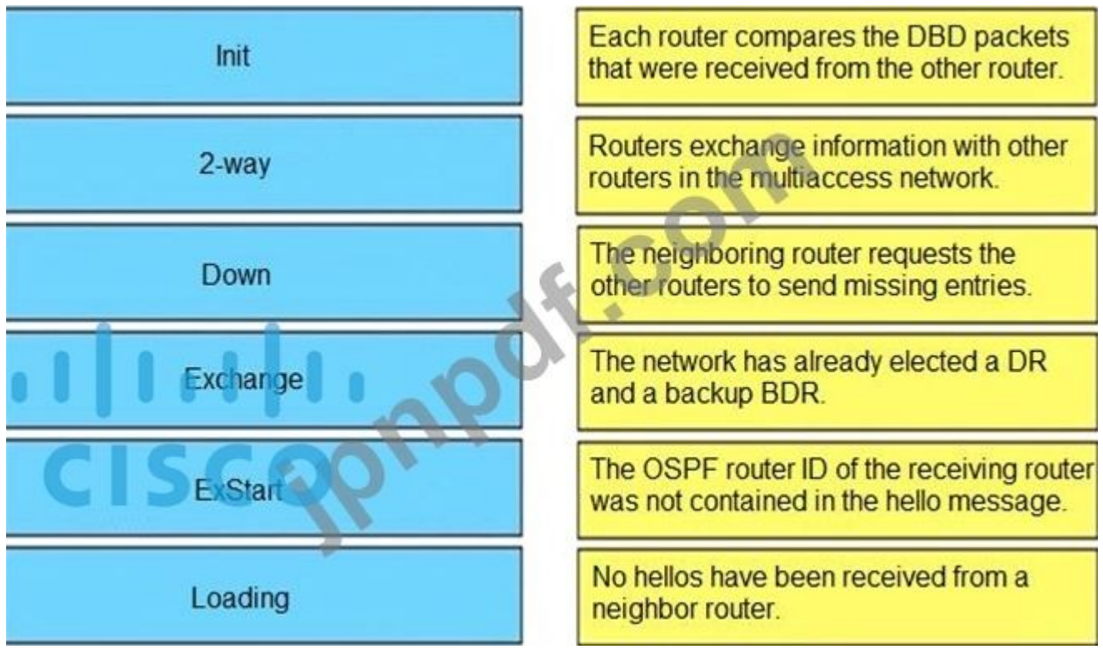
E. R3でOSPFに再配布するときに、EIGRPルートを除くすべてのルートをフィルタリングします。

Answer: (解答を表示する**)**

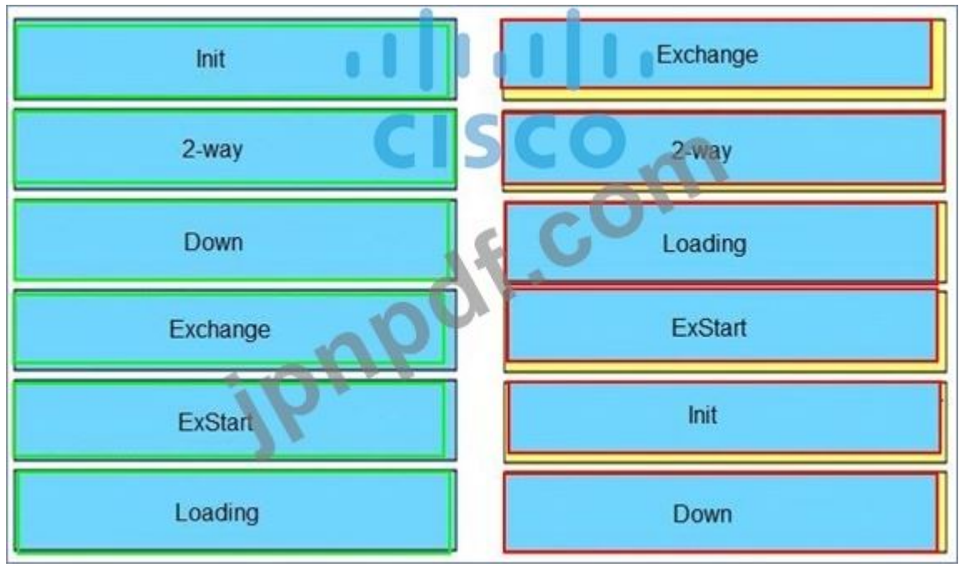
Even PC2 cannot reach PC1 so there is something wrong with RIP redistribution in R2. Because RIP has higher Administrative Distance (AD) value than OSPF and EIGRP so it will be looped when doing mutual redistribution.

最新問題**: 74**

OSPF隣接状態を左側から右側の正しい説明にドラッグアンドドロップします。



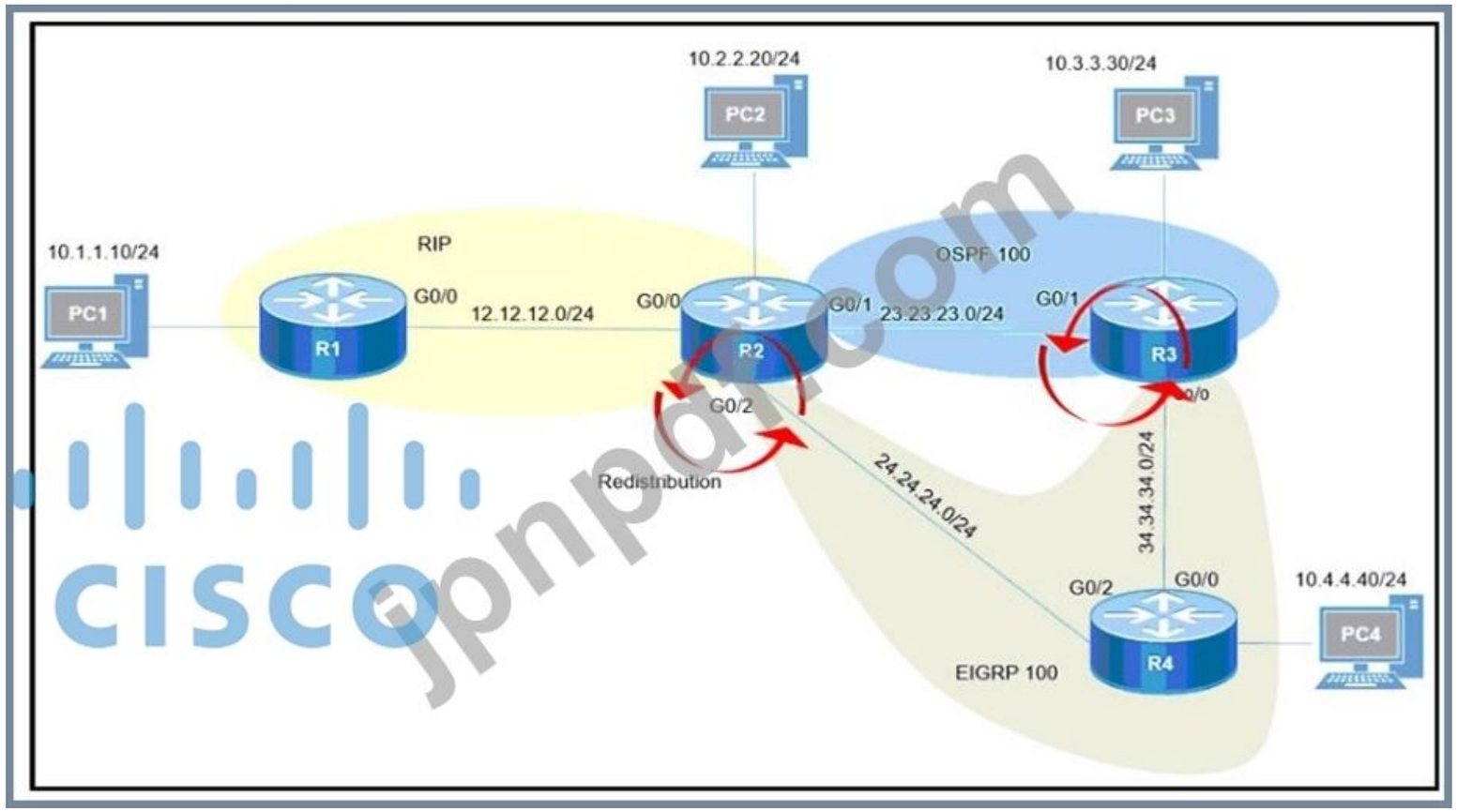
Answer:



最新問題: **75**
展示を参照してください。OSPFネイバー関係が確立されていませんOSPFネイバー隣接関係を復元するには何を設定する必要がありますか？
A. 一致するMTU値
B. ルーターIDを使用
C. ハロータイマーのマッチング
D. リモートルーターのOSPF
Answer: A (メーッセージを残す**)**

最新問題: **76**

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がPC1に到達できません。すべてのPCに到達できるように、エンジニアが問題を解決するために実行できるアクションはどれですか？

A. OSPFからEIGRPに再配布されるときに、プレフィックス10.1.1.0/24をフィルタリングします。
B. R2のRIPプロセスでアドミニストレーティブディスタンス100を設定します。
C. RIPからEIGRPに再配布されるときに、プレフィックス10.1.1.0/24をフィルタリングします。
D. 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 (メーッセージを残す**)**

最新問題: **77**
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. The TACACS+ server expects "user" but the NT client sends "domain\user"

B. The TACACS+ server is down and the user is not in the local database

C. The TACACS+ server refuses the user because the user is set up for CHAP

D. The TACACS+ server is down and the user is in the local database

Answer: B (メーッセージを残す)

最新問題**: 78**

インストール中に、エンジニアがCisco DNA Centerエンタープライズインターフェイスに間違ったデフォルトゲートウェイを設定しました。エンジニアが構成を修正するには、どのコマンドを実行する必要がありますか？

A. sudo maglev-config update

B. sudo maglevの再インストール

C. sudo maglev install config update

D. sudo update config install

Answer: A (メーッセージを残す)

最新問題**: 79**

ネットワークエンジニアが、NTPサーバーと同期し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。ログ出力は現在フラップの時間を示していません。スイッチのロギングでデバイスのクロック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. サービスのタイムスタンプログの稼働時間

B. 夏時間の時計mst繰り返し2月3日日曜日2:00 1日曜日11月11日2:00

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

D. 時計カレンダー有効

Answer: C (メーッセージを残す)

By default, Catalyst switches add a simple uptime timestamp to logging messages. This is a cumulative counter that shows the hours, minutes, and seconds since the switch has been booted up

最新問題**: 80**

IPv6 ND検査の機能とは？

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. レイヤー2ネイバーテーブルのステートフル自動構成アドレスのバインディングを学習して保護します。

C. レイヤー3ネイバーテーブルのステートフル自動構成アドレスのバインディングを学習して保護します。

D. 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

Answer: D (メーッセージを残す)

最新問題: **81**
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データを受信できないのはなぜですか？
A. フローモニターが間違った方向に適用されています。
B. フローエクスポーターは設定されていますが、使用されていません。
C. フローモニターが間違ったインターフェイスに適用されています。
D. フローエクスポーターの宛先に到達できません。
Answer: (解答を表示する**)**

最新問題: **82**
展示を参照してください。

隣接の問題を解決するアクションはどれですか？

A. helloインターバルタイマーを一致させます。

B. 認証キーを照合します。

C. 同じEIGRPプロセスIDを設定します。

D. 同じ自律システム番号を構成します。

Answer: D (メーッセージを残す)

最新問題**: 83**

エンジニアは、認証を使用して管理サーバーに送信されるSNMP通知を構成し、DESでデータを暗号化しました。応答PDUのエラーは、「UNKNOWNUSERNAME.WRONGDIGEST」として受信されます。どのアクションが問題を解決しますか？

A. SNMPv3authPrivを使用して正しい認証パスワードを構成します。

B. SNMPv3authNoPrivを使用して正しい認証パスワードを構成します。

C. SNMPv3 authNoPrivを使用して、正しい認証パスワードとプライバシーパスワードを構成します。

D. SNMPv3 authPrivを使用して、正しい認証パスワードとプライバシーパスワードを構成します。

Answer: D (メーッセージを残す)

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html

最新問題**: 84**

EIGRPをOSPFに再配布することについて正しい2つのステートメントはどれですか。 2つ選択してください）

A. 再配布されたEIGRPルートは、OSPFデータベースでタイプ5 LSAとして表示されます

B. 再配布されたEIGRPルートは、OSPFデータベースでタイプ3 LSAとして表示されます

C. エリアIDがEIGRP自律システム番号と一致するOSPFエリアに配置された、再配布されたEIGRPルート

D. 再配布されたEIGRPルートは、ルーティングテーブルにOSPF外部タイプ2ルートとして表示されます

E. 再配布されたEIGRPルートはOSPF外部タイプ1として表示されます
F. 再配布されたルートのアドミニストレーティブディスタンスは170です
Answer: A,D (メーッセージを残す)

最新問題**: 85**
デバイスのCPU使用率を保護するには、どのオプションが最適ですか？
A. COPP
B. 断片化
C. ICMPリダイレクト
D. ICMP到達不能メッセージ
Answer: (解答を表示する)