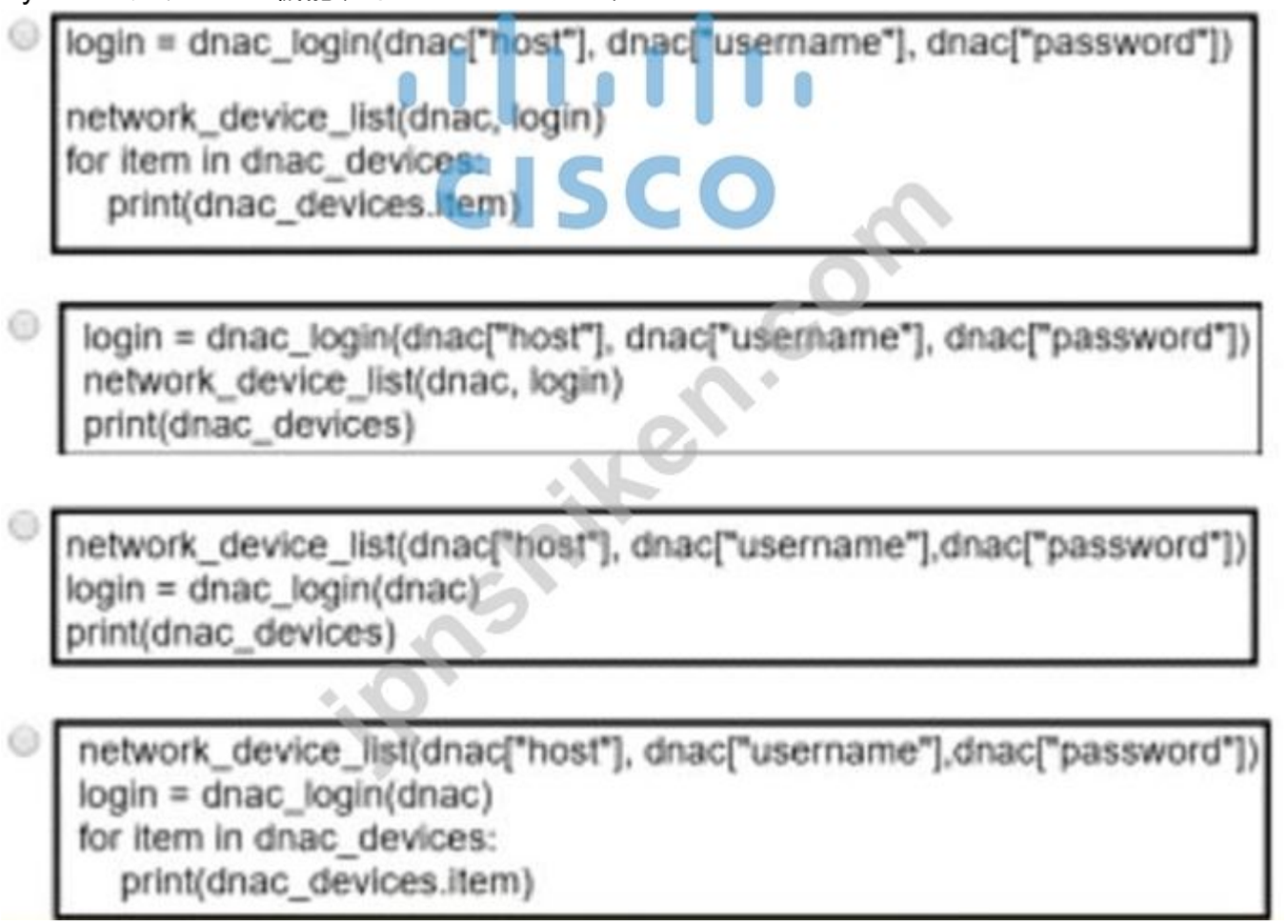
Cisco.350-401J.v2021-09-01.q42

試験コード：	350-401J
試験名称：	Implementing and Operating Cisco Enterprise Network Core Technologies (350-401日本語版)
認証ベンダー：	Cisco
無料問題の数：	42
バージョン：	v2021-09-01
ページの閲覧量：	883
問題集の閲覧量：	9367

https://www.jpnshiken.com/shiken/Cisco.350-401J.v2021-09-01.q42.html

質問: **1**

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



A. オプションA

B. オプションC

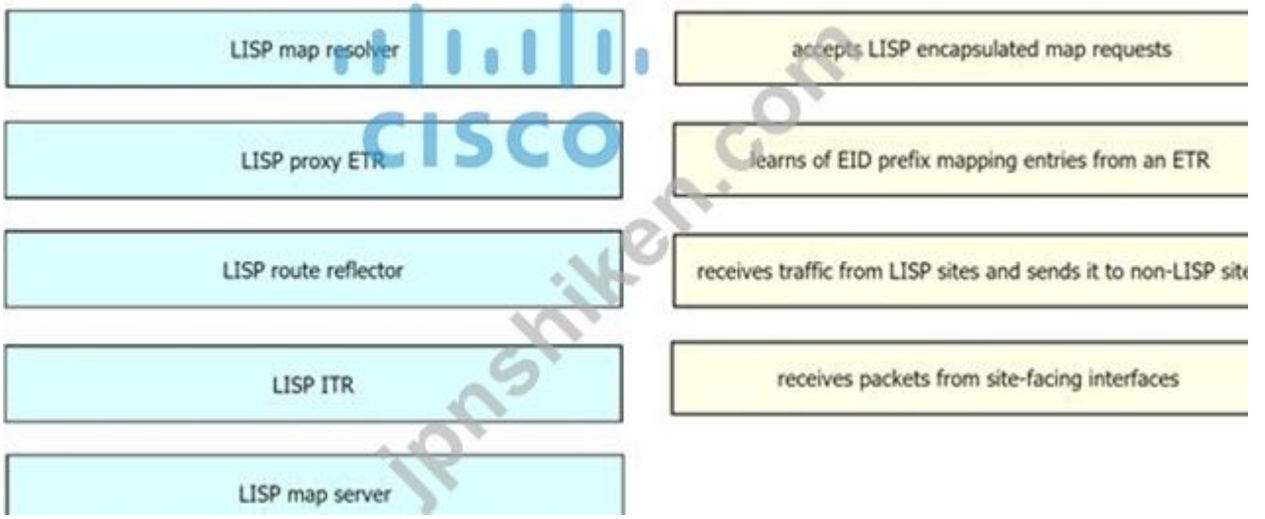
C. オプションD

D. オプションB

正解: (正解を表示します)

質問: **2**
エンジニアは、ランサムウェア攻撃から自社を保護する必要があります。エンジニアが実行段階をブロックしてファイルの暗号化を防ぐことができるソリューションはどれですか？
A. 侵入ポリシーとSMBの悪用をブロックするsnortルールでCisco Firepowerを使用します。
B. Exploit Preventionエンジンを有効にしてCisco AMP展開を使用します。
C. Cisco Firepowerを使用して、TORネットワークへのトラフィックをブロックします。
D. 悪意のあるアクティビティ保護エンジニアを有効にしてCisco AMP展開を使用します。
正解: **D** (コメントを発表する)

質問: **3**
LISPコンポーネントを左から右に実行する機能にドラッグアンドドロップします。すべてのオプションが使用されるわけではありません。



正解:

質問: **4**
Cisco SD-Accessソリューションでは、Identity Services Engineの役割は何ですか？

A. エンドポイントからアプリへのフローを分析し、ファブリックのステータスを監視するために使用されます。
B. コンテキストを共有するアプリを介してGUI管理と抽象化を提供します。
C. 動的エンドポイントからグループへのマッピングとポリシー定義に活用されます。
D. LISPEIDデータベースを管理します。
正解: **(**正解を表示します**)**

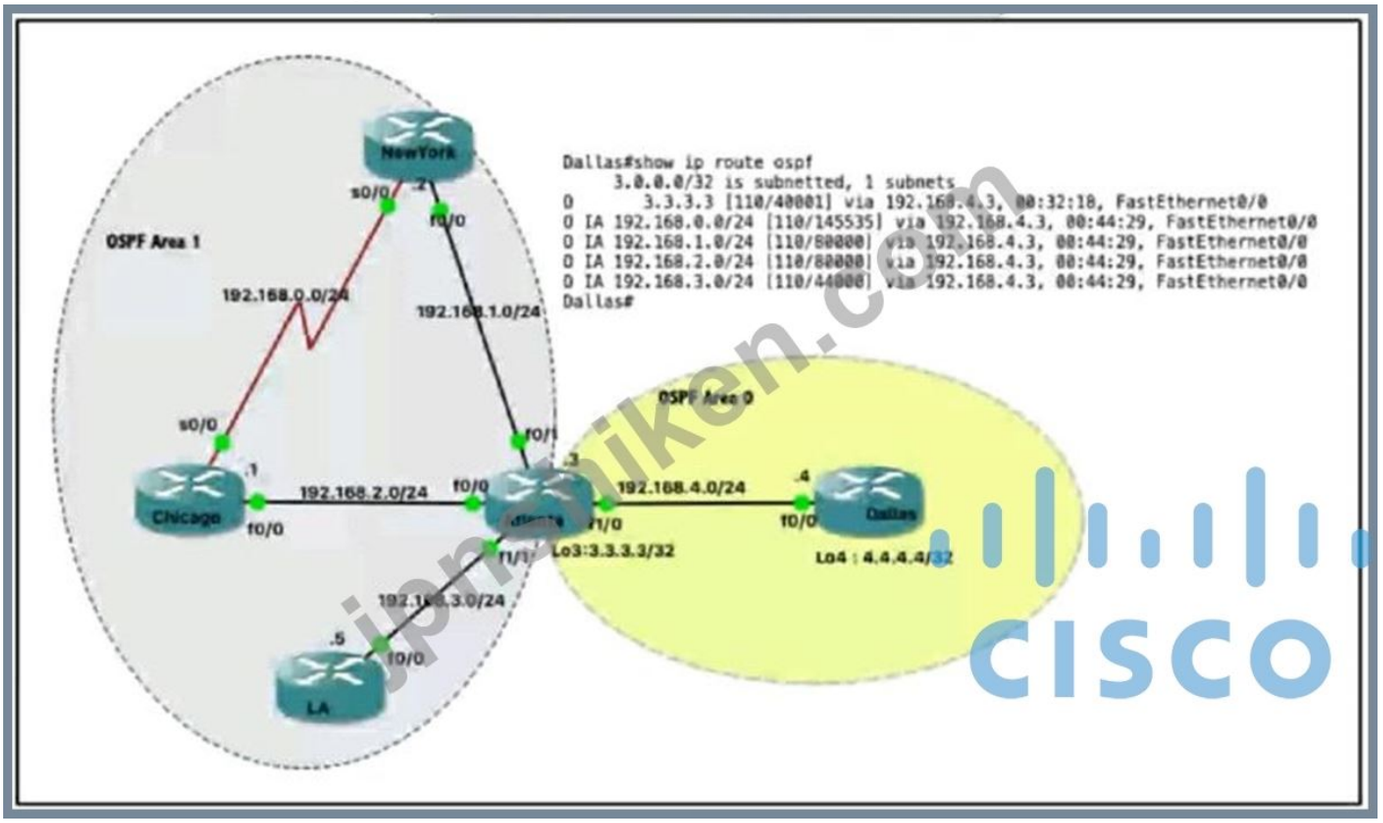
質問: **5**
ブルート攻撃からREST APIを保護し、影響を最小限に抑えるために使用されているアルゴリズムはどれですか？
A. SHA-512およびSHA-384
B. MD5アルゴリズム-128およびSHA-384
C. SHA-1、SHA-256、およびSHA-512
D. PBKDF2、BCrypt、およびSCrypt
正解: **(**正解を表示します**)**
One of the best practices to secure REST APIs is using password hash. Passwords must always be hashed to protect the system (or minimize the damage) even if it is compromised

質問: **6**
お客様は、すべてのAPを管理するためにSSOクラスタにCisco 5520WLCのペアを設定しています。ゲストトラフィックは、DMZにあるCisco 3504WLCに固定されています。SSOクラスターでフェイルオーバーが発生した場合にEoIPトンネルをUP状態のままにするために必要なアクションはどれですか。
A. モビリティピアが設定されている場合は、モビリティMACを使用します
B. すべてのWLCで同じモビリティドメインを使用する
C. デフォルトゲートウェイの到達可能性チェックを有効にする
D. RPポートで連続接続を構成します
正解: **(**正解を表示します**)**
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-5/High_Availability_DG.html

質問: **7**
Cisco SD-Accessワイヤレスネットワークの展開に関する1つの事実は何ですか？
A. アクセスポイントはファブリックアンダーレイの一部です
B. WLCはファブリックアンダーレイの一部です
C. アクセスポイントはファブリックオーバーレイの一部です
D. ワイヤレスクライアントはファブリックオーバーレイの一部です
正解: **(**正解を表示します**)**
Explanation
Access Points
+ AP is directly connected to FE (or to an extended node switch)

+ AP is part of Fabric overlay

質問: **8**
展示を参照してください。



Atlantaルーターにどのコマンドを適用すると、バックボーンエリアへのタイプ3 LSAフラッディングが減少し、ダラスルーターのエリア間ルートが要約されますか？
A. Atlanta ¢onfig-route⟩#area 1 range 192.168.0.0 255.255.248.0
B. Atlanta ¢onfig-route⟩#area 0 range 192.168.0.0 255.255.252.0
C. Atlanta ¢onfig-route⟩#area 0 range 192.168.0.0 255.255.248.0
D. Atlanta ¢onfig-route⟩#area 1 range 192.168.0.0 255.255.252.0
正解: **(**正解を表示します**)**

質問: **9**
NTP階層レベルの数値は何を表していますか？
A. デバイスクロックと実際の時間の間のオフセット量。
B. デバイスクロックと実際の時間の間のドリフト量。
C. 信頼できるタイムソースに到達するのにかかるホップ数。
D. マスタータイムサーバーに到達するのにかかるホップ数。
正解: **(**正解を表示します**)**

質問: **10**
EIGRPはOSPFとどのように異なりますか？
A. マスターコントローラーでの設定は、すべての無線LANコントローラーで実行されます。

B. マスターコントローラーは、他のコントローラーに接続しているすべてのクライアントの負荷分散を担当します。
C. WLANに参加するすべての新しいAPは、マスターコントローラに割り当てられます。
D. すべての無線LANコントローラーはマスターコントローラーによって管理されます。
正解: **(**正解を表示します**)**

質問: **11**
EIGRPでサポートされているが、OSPFではサポートされていない機能はどれですか。
A. ルートフィルタリング
B. ルートの要約
C. 不等コストの負荷分散
D. 等コストの負荷分散
正解: **C (**コメントを発表する**)**

質問: **12**
ネットワーク管理者がルーティング構成の変更を実装し、ルーティングデバッグを有効にして、変更中のルーティング動作を追跡します。端末のログ出力がコマンド入力プロセスを中断しています。コマンドを誤って入力する可能性を最小限に抑えるために、ネットワーク管理者が実行できる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. ロギング同期グローバル構成コマンドを構成します
B. terminal lengthコマンドを使用して画面の行数を増やします
C. ロギング区切り機能を構成する
D. TABキーを押して、コマンドを新しい行に再印刷します
E. vtyの下でlogging同期コマンドを構成します
正解: **(**正解を表示します**)**

質問: **13**
SSOはHSRPとどのように連携してネットワークの中断を最小限に抑えますか？
A. HSRPがグループ内の別のスイッチをアクティブなHSRPスイッチとして選出できるようにします。
B. リンク障害が発生した場合に高速フェイルオーバーを保証します。
C. スイッチオーバー後の既知のルートに沿ったデータ転送を可能にし、ルーティングプロトコルを再収束させます。
D. HSRPが同じデバイス上のスタンバイRPにフェイルオーバーできるようにします。
正解: **(**正解を表示します**)**
SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.
The SSO HSRP feature enables the Cisco IOS HSRP subsystem software to detect that a standby RP is installed and the system is configured in SSO redundancy mode. Further, if the

active RP fails, no change occurs to the HSRP group itself and traffic continues to be forwarded through the current active gateway device.

質問: **14**
どの方法
Cisco DNA Centerは、サウスバウンドプロトコルを介したシスコ以外のデバイスの管理を可能にするために使用しますか？
A. SDKを使用してデバイスパックを作成します
B. API呼び出しを使用してデバイスに問い合わせ、返されたデータを登録します。
C. 利用可能なAPIの詳細を示すMIBを各ベンダーから取得します。
D. シスコ以外のデバイスで使用可能なAPIをCSV形式でインポートします。
正解: (正解を表示します)
Cisco DNA Center allows customers to manage their non-Cisco devices through the use of a Software Development Kit (SDK) that can be used to create Device Packages for third-party devices.

質問: **15**
展示を参照してください。

```
interface Vlan10
 ip vrf forwarding Customer1
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
 ip vrf forwarding Customer2
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
 ip vrf forwarding Customer3
 ip address 10.1.1.1 255.255.255.0
```

Customer2ホストがIPアドレス192.168.1.200を持つCustomer1のFTPサーバーにアクセスできるようにする構成はどれですか？
A. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 Customerl ip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customer2
B. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 global
ip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 global
ip route 192.168.1.0 255.255.255.0 VlanlO
ip route 172.16.1.0 255.255.255.0 Vlan20
C. ip route vrf Customerl 172.16.1.0 255.255.255.0 172.16.1.1 Customer2 ip route vrf Customer 192.168.1.200 255.255.255.255 192.168.1.1 Customerl
D. ip route vrf Customerl 172.16.1.1 255.255.255.255 172.16.1.1 global
ip route vrf Customer 192.168.1.200 255.255.255.0 192.168.1.1 global
ip route 192.168.1.0 255.255.255.0 VlanlO
ip route 172.16.1.0 255.255.255.0 Vlan20
正解: (正解を表示します)

質問: **16**
Cisco SD-Accessワイヤレスネットワークの展開では、どの設計原則に従う必要がありますか。
A. WLCはファブリックアンダーレイの一部です
B. WLCはファブリックの外部に接続されています
C. アクセスポイントはファブリックの外部に接続されています。
D. WLCはファブリックオーバーレイの一部です。
正解: **(**正解を表示します**)**

質問: **17**
AnsibleとChefを区別する特徴はどれですか。
A. AnsibleはRubyを使用して構成を管理します。ChefはYAMLを使用して構成を管理します。
B. Ansibleサーバーは、Linux、Unix、またはWindowsで実行できます。Chefサーバーは Linuxまたはで実行する必要があります。
C. Ansibleは構成をクライアントにプッシュします。Chefクライアントはサーバーから構成をプルします。
D. マスターサーバーのAnsible lacs冗長性サポート。Chefはアクティブ/アクティブモードで2つのマスターを実行します。
正解: **C (**コメントを発表する**)**

質問: **18**
ルーターが100 kbpsを受け入れるSSHの量を制限する構成はどれですか。
A）

B）

C）

D）

A. オプションA
B. オプションB
C. オプションD
D. オプションC
正解: **D** (コメントを発表する)

質問: **19**
クライアントの信頼性を検証するために使用され、JSONオブジェクトとしてHTTPリクエストで送信されるものは何ですか？
A. SSH
B. HTTPS
C. JVVT
D. TLS

正解: (正解を表示します)
https://developer.atlassian.com/server/crowd/json-requests-and-responses/

質問: 20
展示を参照してください。
エンジニアは、ホスト間の他のすべての通信を許可しながら、ホストAからホストBへのHTTPトラフィックを拒否する必要があります。どのコマンドセットがこのタスクを実行しますか？

SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)#permit tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# permit ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# action forward

SW1(config)# vlan filter HOST-A-B vlan 10

SW1(config)# mac access-list extended HOST-A-B
SW1(config-ext-macl)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd

SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)#deny tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# vlan access-map DROP-MAC 10
SW1(config-access-map)# match mac address HOST-A-B
SW1(config-access-map)# action drop
SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop

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

正解: **A (**コメントを発表する**)**

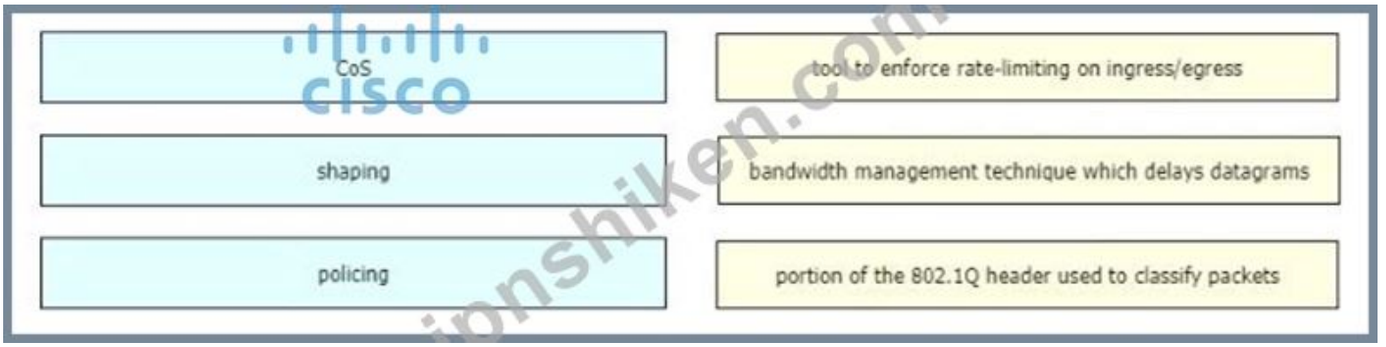
In this case we need to configure a VLAN access-map to deny HTTP traffic and apply it to VLAN 10. To do it, first create an access-list, by which interesting traffic will be matched. The principle of VLAN access-map config is similar to the route-map principle.

After this we'll create a vlan access-map, which has two main parameters: action and match. Match: by this parameter the interesting traffic is matched and here RACL or MAC ACL can be applied as well. Action: what to do with matched traffic. Two main parameters exist: Drop and Forward. In case of Drop, matched traffic will be dropped, and in case of forward, matched traffic will be allowed.

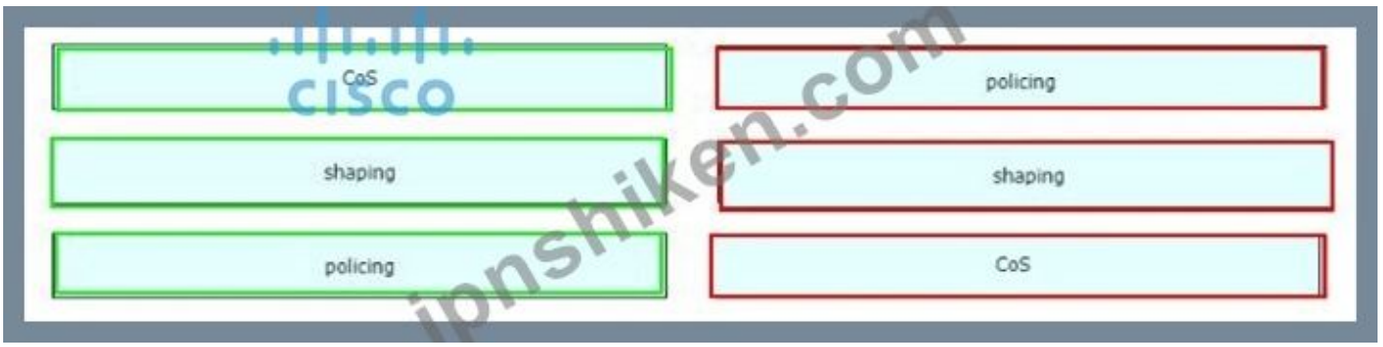
A good reference and example can be found at https://www.networkstraining.com/vlan-access-map-example-configuration/

質問: **21**

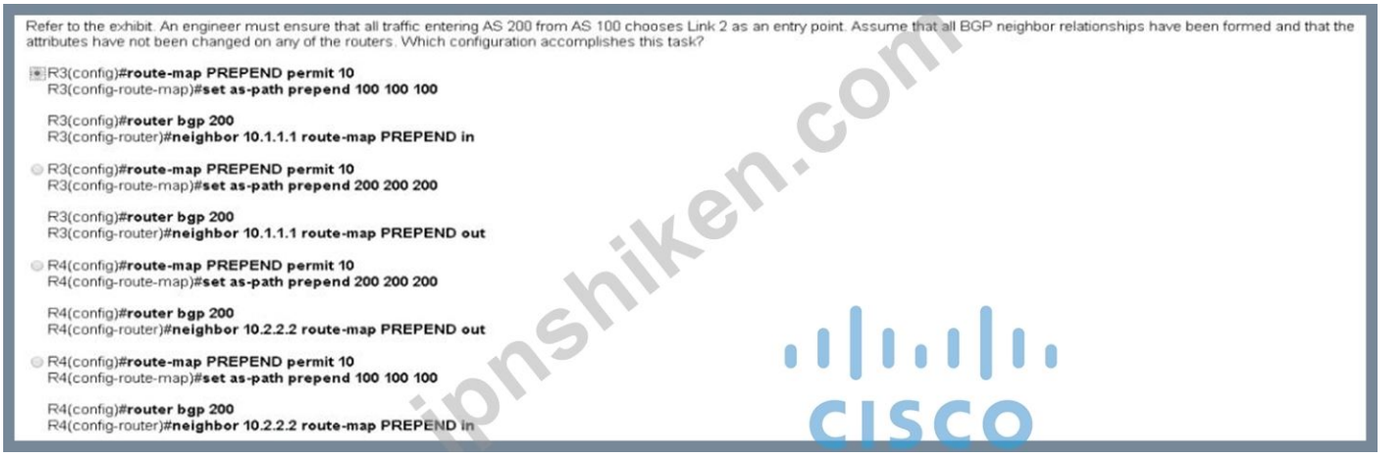
QoSメカニズムを左から右側の説明にドラッグアンドドロップします



正解:



質問: **22**
展示を参照してください。エンジニアは、AS100からAS200に入るすべてのトラフィックがリンク2を選択し、すべてのBGPネイバーに入る関係が形成されていること、およびどのルータでも属性が変更されていないことを確認する必要があります。



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
正解: **(**正解を表示します**)**

質問: **23**
データモデリング言語の使用方法
A. 変更できない有限で明確なネットワーク要素を表すため。
B. インフラストラクチャ内の非構造化データのフローをモデル化します。
C. データを簡単に構造化、グループ化、検証、および複製できるようにするため
D. スクリプト言語を人間が読みやすくするため
正解: **(**正解を表示します**)**

質問: **24**
PIMはマルチキャストトラフィックを転送するためにどのようなメカニズムを使用しますか？
A. PIM希薄モードは、プルモデルを使用してマルチキャストトラフィックを配信します。
B. PIMデンスモードは、プルモデルを使用してマルチキャストトラフィックを配信します。
C. PIMスパースモードは、レシーバーを使用してRPに登録します。

D. PIM希薄モードは、フラッドアンドプルーンモデルを使用してマルチキャストトラフィックを配信します。

正解: **A (**コメントを発表する**)**

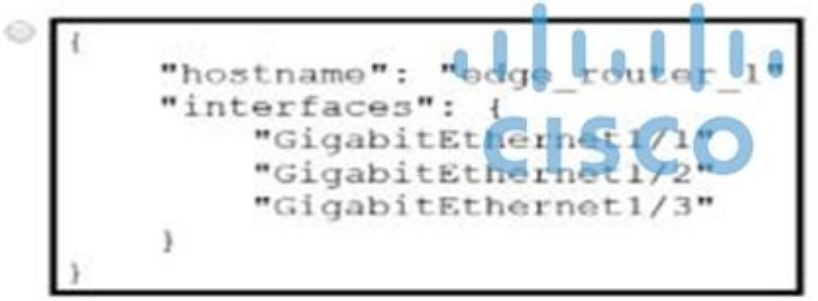
PIM dense mode (PIM-DM) uses a push model to flood multicast traffic to every corner of the network. This push model is a brute-force method of delivering data to the receivers. This method would be efficient in certain deployments in which there are active receivers on every subnet in the network. PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune the unwanted traffic. This process repeats every 3 minutes.

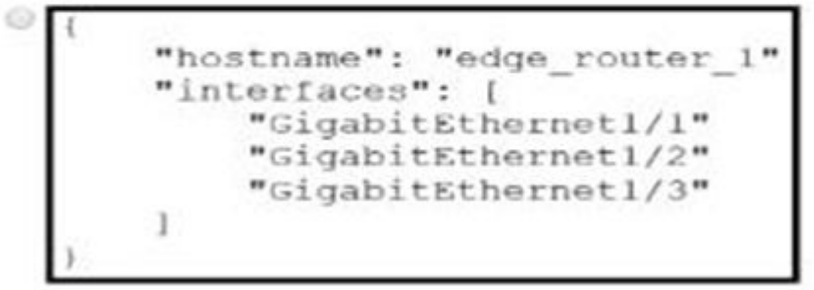
PIM Sparse Mode (PIM-SM) uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data receive the traffic. PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least initially), it requires the use of an RP. The RP must be administratively configured in the network.

Answer C seems to be correct but it is not, PIM spare mode uses sources (not receivers) to register with the RP. Sources register with the RP, and then data is forwarded down the shared tree to the receivers.

質問: **25**

有効なJSONファイルを表示する展示はどれですか？





A. オプションC
B. オプションA
C. オプションD
D. オプションB
正解: **(**正解を表示します**)**

質問: **26**
RIBとFIBの2つの違いは何ですか？ 2つ選択してください。）
A. FIBはデータプレーンから派生し、RIBはFIBから派生します。
B. RIBはルーティングプレフィックスのデータベースであり、FIBは各パケットの出力インターフェイスを選択するために使用される情報です。
C. FIBはルーティングプレフィックスのデータベースであり、RIBは各パケットの出力インターフェイスを選択するために使用される情報です。
D. FIBはコントロールプレーンから派生し、RIBはFIBから派生します。
E. RIBはコントロールプレーンから派生し、FIBはRIBから派生します。
正解: **B,E (**コメントを発表する**)**
The Forwarding Information Base (FIB) contains destination reachability information as well as next hop information. This information is then used by the router to make forwarding decisions. The FIB allows for very efficient and easy lookups

質問: **27**
ある会社には、SSOを使用する既存のCisco 5520HAクラスタがあります。エンジニアは、新しい単一のCisco Catalyst 9800 WLCを導入して、新しい機能をテストします。エンジニアは、5520クラスタと9800WLCの間にモビリティトンネルを正常に設定します。企業のWLANに接続されたクライアントは、5520と9800のWLCのアクセスポイント間をシームレスにローミングします。プライマリ5520WLCで障害が発生した後も、すべてのWLANサービスは機能し続けます。ただし、クライアントは接続を切断せずに5520コントローラーと9800コントローラーの間をローミングします。問題を解決するには、どの機能を構成する必要がありますか？
A. 9800WLCの新しいモビリティ
B. 5520クラスターのモビリティMAC
C. 5520クラスターの新しいモビリティ
D. 9800WLCのモビリティMAC
正解: **(**正解を表示します**)**

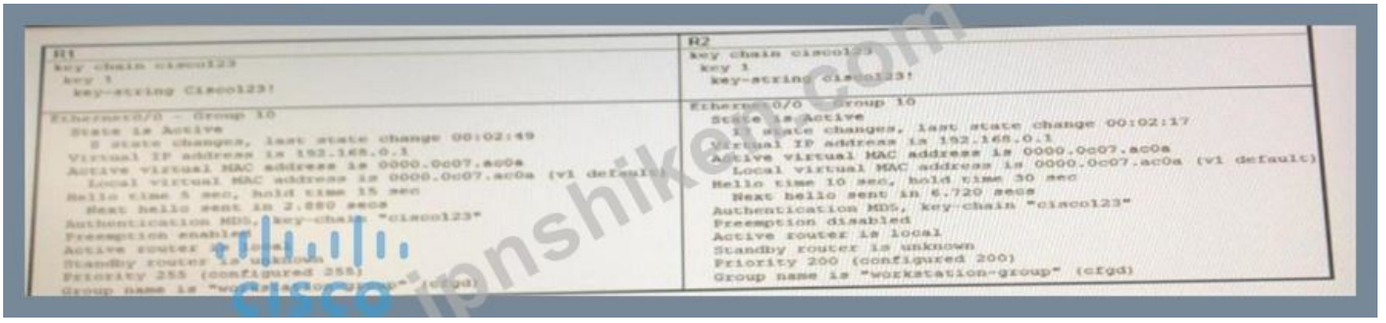
質問: **28**

展示を参照してください。拡張アクセスリスト100は、インターフェイスGigabitEthernet 0/0でインバウンド方向に設定されていますが、192.168.0.0 / 16との間のパケットのみを許可するという期待される動作はありません。どのコマンドセットがアクセスリストを適切に設定しますか？

A. オプションC
B. オプションD
C. オプションB
D. オプションA
正解: **(**正解を表示します**)**

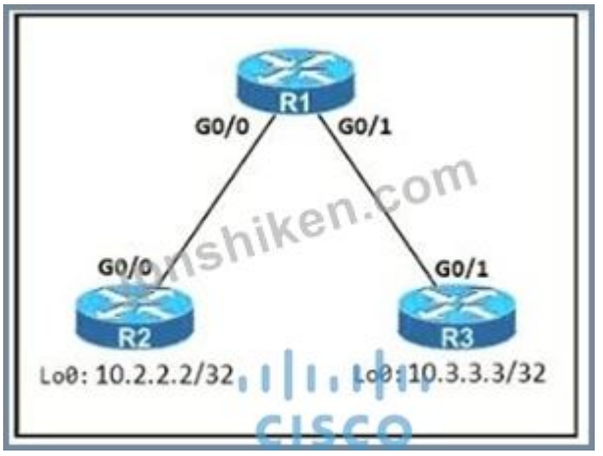
質問: **29**
エンジニアがWLANでローカルWeb認証を構成しています。エンジニアは、Webポリシーのレイヤー3セキュリティオプションの下にある[認証]ラジオボタンを選択します。
WLANのWeb認証を提示するのはどのデバイスですか？
A. RADIUSサーバー
B. ローカルWLC
C. ISEサーバー
D. アンカーWLC
正解: **(**正解を表示します**)**

質問: **30**
展示を参照してください。



エンジニアが冗長構成でルーターの新しいペアをインストールしています。各ルーターのスタンバイステータスを確認すると、エンジニアはルーターが期待どおりに機能していないことに気付きます。構成エラーを解決するアクションはどれですか？
A. 一致するホールドタイマーと遅延タイマーを設定します
B. 一致するキー文字列を構成します
C. 一致する優先度の値を設定します
D. 一意の仮想IPアドレスを構成します
正解**: (**正解を表示します**)**
From the output exhibit, we notice that the key-string of R1 is -Cisco123!|| (letter -C|| is in capital) while that of R2 is -cisco123!||. This causes a mismatch in the authentication so we have to fix their key-strings.
key-string [encryption-type] text-string: Configures the text string for the key. The text-string argument is alphanumeric, case-sensitive, and supports special characters.

質問**: 31**
展示を参照してください。



エンジニアは週末に、ルータR3のループバックインターフェイスからルータR2のループバックインターフェイスへのTelnetトラフィックを拒否する必要があります。ルータR3とR2のループバックインターフェイス間の他のすべてのトラフィックは、常に許可する必要があります。このコマンドを実行するのはどのコマンドですか？ A）

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

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

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

B）

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

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

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

C）

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

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

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

D）

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

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

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

A. オプションA

B. オプションB

C. オプションC

D. オプションD

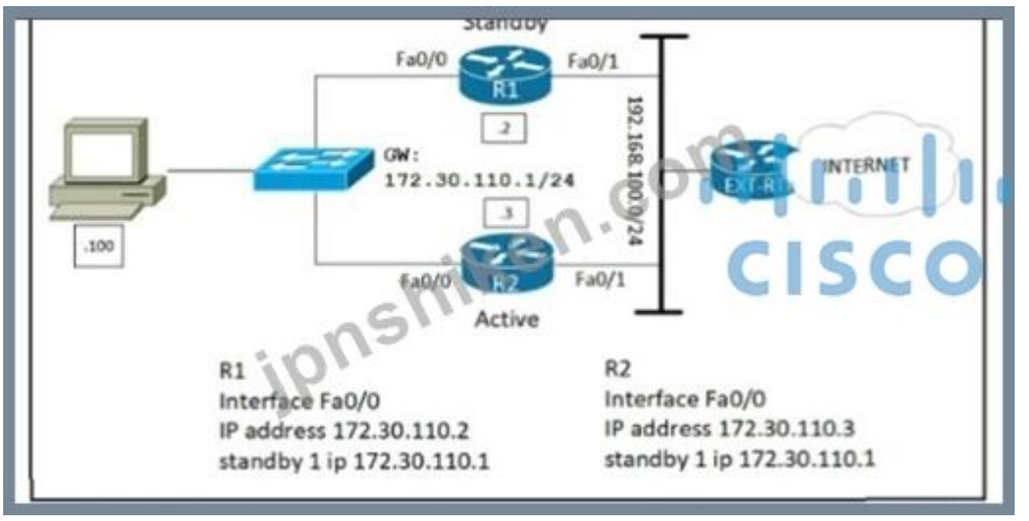
正解**: C (**コメントを発表する**)**

We cannot filter traffic that is originated from the local router (R3 in this case) so we can only configure the ACL on R1 or R2. "Weekend hours" means from Saturday morning through Sunday night so we have to configure: "periodic weekend 00:00 to 23:59".

Note: The time is specified in 24-hour time (hh:mm), where the hours range from 0 to 23 and the minutes range from 0 to 59.

質問**: 32**

展示を参照してください。



172.30.110.0/24ネットワークの機能状態にあるときはいつでもR1がアクティブゲートウェイであることを保証する構成変更はどれですか？

R2
standby 1 priority 90
standby 1 preempt

R1
standby 1 preempt
R2
standby 1 priority 90

R2
standby 1 priority 100
standby 1 preempt

R1
standby 1 preempt
R2
standby 1 priority 100

A. オプションC
B. オプションB
C. オプションD
D. オプションA
正解: **(**正解を表示します**)**

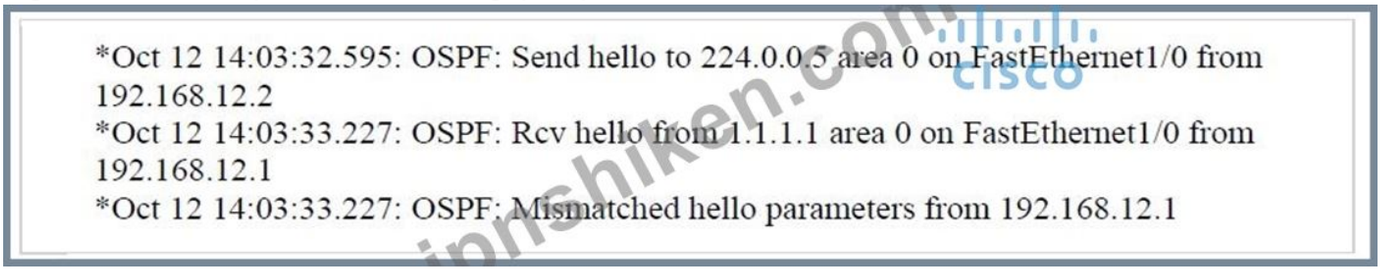
質問: **33**
YANGのようなデータモデリング言語の利点は何ですか？
A. プログラマがデバイスのオペレーティングシステム内で独自のアプリケーションを変更または作成できるようにします。

B. より安全で効率的なSNMP OIDを作成します。
C. CLIをシンプルかつ効率的にします。
D. 標準化されたデータ構造を提供し、構成のスケーラビリティと一貫性を実現します。
正解: **(**正解を表示します**)**
Yet Another Next Generation (YANG) is a language which is only used to describe data models (structure). It is not XML or JSON.

質問: **34**
展示を参照してください。

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

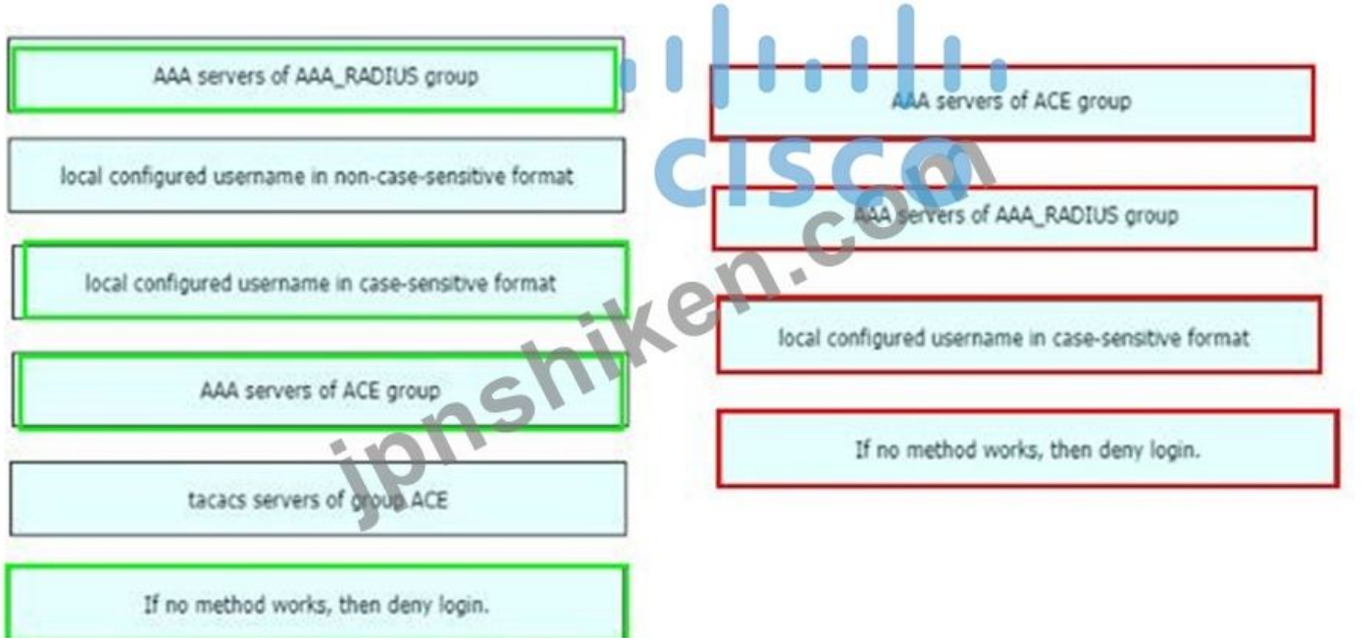
OPSFデバッグ出力について正しい説明はどれですか。
A. 出力には、ルーターR1が送信したすべてのOSPFメッセージがインターフェースFa0 / 1で受信されて表示されます。
B. 出力には、ルーターR1がすべてのインターフェースで送信または受信したすべてのOSPFメッセージが表示されます。
C. 出力には、ルーターR1がインターフェイスFa0 / 1で受信したOSPF helloメッセージが表示されます。
D. 出力には、ルーターR1が送信または受信したOSPF helloおよびLSACKメッセージが表示されます。
正解: **C (**コメントを発表する**)**
This combination of commands is known as "Conditional debug" and will filter the debug output based on your conditions. Each condition added, will behave like an 'And' operator in Boolean logic. Some examples of the "debug ip ospf hello" are shown below:



質問: **35**
エンジニアが以下の構成を作成します。認証方法を左から右の優先順位にドラッグアンドドロップします。すべてのオプションが使用されるわけではありません。

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

正解:



質問: **36**
陽は何に使われますか？
A. CLIを介してデータをスクレイピングする
B. データモデルの説明
C. SNMP読み取り専用ポーリングの処理
D. クライアントとサーバー間のネットワーク構成データのトランスポートを提供します
正解: **(**正解を表示します**)**

質問: **37**
Cisco SD-Access展開でのファブリックコントロールプレーンノードの機能は何ですか？
A. ファブリック内のポリシーアプリケーションとネットワークセグメンテーションを担当します。
B. ファブリックでトラフィックのカプセル化とセキュリティプロファイルの適用を実行します。
C. ファブリック内のエンドポイントとネットワークを追跡する包括的なデータベースを保持します。

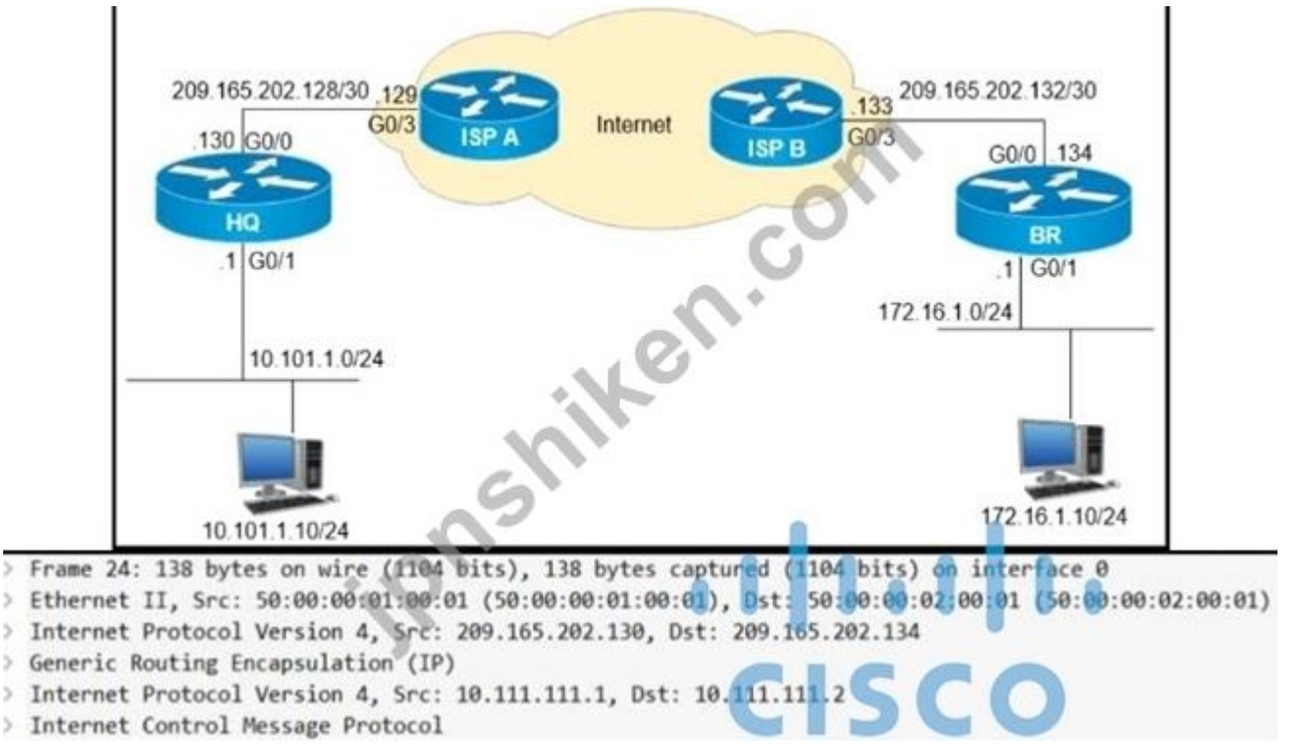
D. 従来の非ファブリック対応環境との統合を提供します。
正解: **(**正解を表示します**)**
Fabric control plane node (C): One or more network elements that implement the LISP Map-Server (MS) and Map-Resolver (MR) functionality. The control plane node's host tracking database keep track of all endpoints in a fabric site and associates the endpoints to fabric nodes in what is known as an EID-to-RLOC binding in LISP.

質問: **38**
どのエンティティ
VXLAN環境でセグメント間のレイヤー2分離を維持する責任がありますか？
A. スイッチファブリック
B. VTEP
C. VNID
D. ホストスイッチ
正解: **(**正解を表示します**)**

VXLAN uses an 8-byte VXLAN header that consists of a 24-bit VNID and a few reserved bits. The VXLAN header together with the original Ethernet frame goes in the UDP payload. The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.

質問: **39**
Cisco NQFWのどの展開オプションがスケーラビリティを提供しますか？
A. タップ
B. クラスタリング
C. 高可用性
D. インラインタップ
正解: **C (**コメントを発表する**)**

質問: **40**
展示を参照してください。



HOルーターとBRルーターの間にGREトンネルが作成されました。

HQルーターのトンネルIPとは何ですか？

A. 209.165.202.134

B. 10.111.111.2

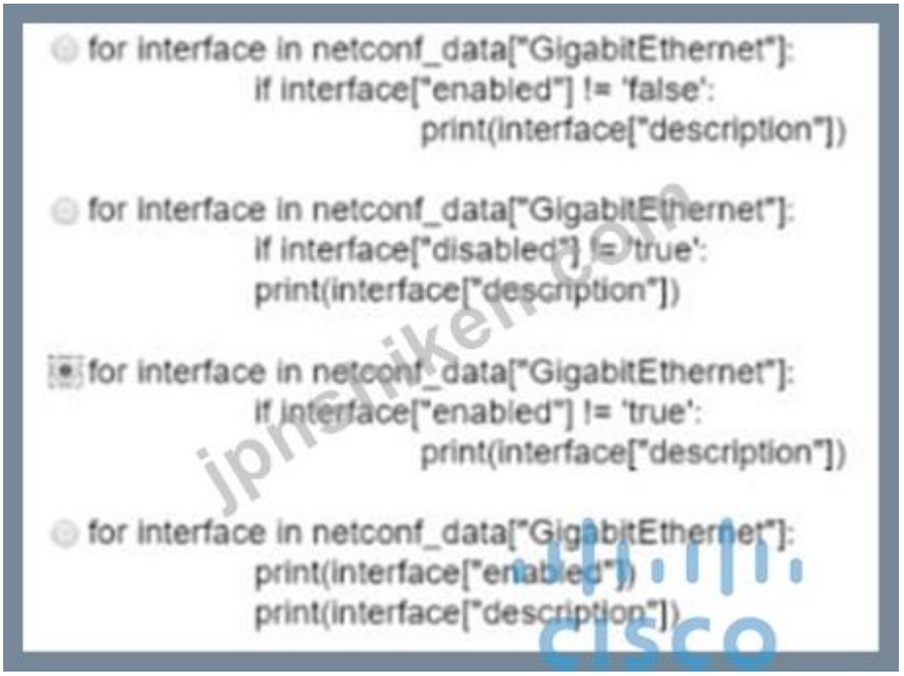
C. 209.165.202.130

D. 10.111.111.1

正解**: (**正解を表示します**)**

質問**: 41**

展示を参照してください。無効になっているインターフェースの説明のみを出力するPythonコードスニペットはどれですか？



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
正解: **B** (コメントを発表する)

質問: **42**
展示を参照してください。すべてのユーザーに対して動的な連続マップNATを実現するために、構成を完了するアクションはどれですか。
A. マッチホストタイプのNATプールを構成します
B. 1対1タイプのNATプールを構成します
C. 192.168 10アドレス範囲を使用するようにプールを再構成します
D. NATプールサイズを増やして、254個の使用可能なアドレスをサポートします
正解: (正解を表示します)