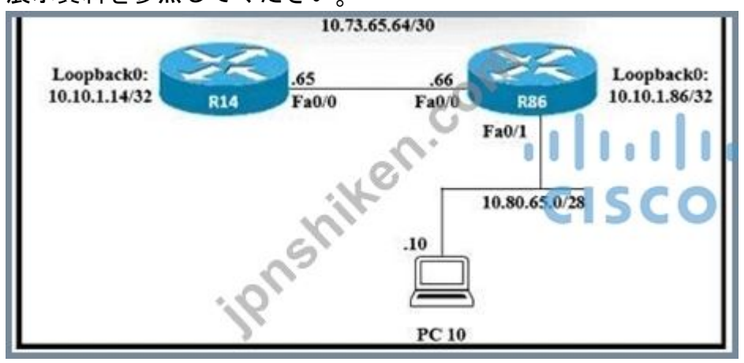
Cisco.200-301J.v2026-09-26.q525

試験コード：	200-301J
試験名称：	Cisco Certified Network Associate Exam (200-301日本語版)
認証ベンダー：	Cisco
無料問題の数：	525
バージョン：	v2026-09-26
ページの閲覧量：	105
問題集の閲覧量：	5276

https://www.jpnshiken.com/shiken/Cisco.200-301J.v2026-09-26.q525.html

質問: **1**
展示資料を参照してください。



ルーターR14は現在設定中です。PC10へのホストルートを確立するには、どの設定を使用する必要がありますか？
A. ip route 10.80.65.10 255.255.255.254 10.80.65.1
B. ip route 10.8065.10 255.255.255.255 10.73.65.66
C. ip route 1073.65.65 255.0.0.0 10.80.65.10
D. ip route 10.73.65.66 0.0.0.255 10.80.65.10
正解: **B (**コメントを発表する**)**
ip route 10.8065.10 255.255.255.255 10.73.65.66. Routing questions are solved by applying longest-prefix match, administrative distance, metric, and protocol-specific behavior in the correct order. Cisco CCNA 200-
301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue:
a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Wrong answers either use the wrong prefix, the wrong next hop, or a route source that would not be preferred. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

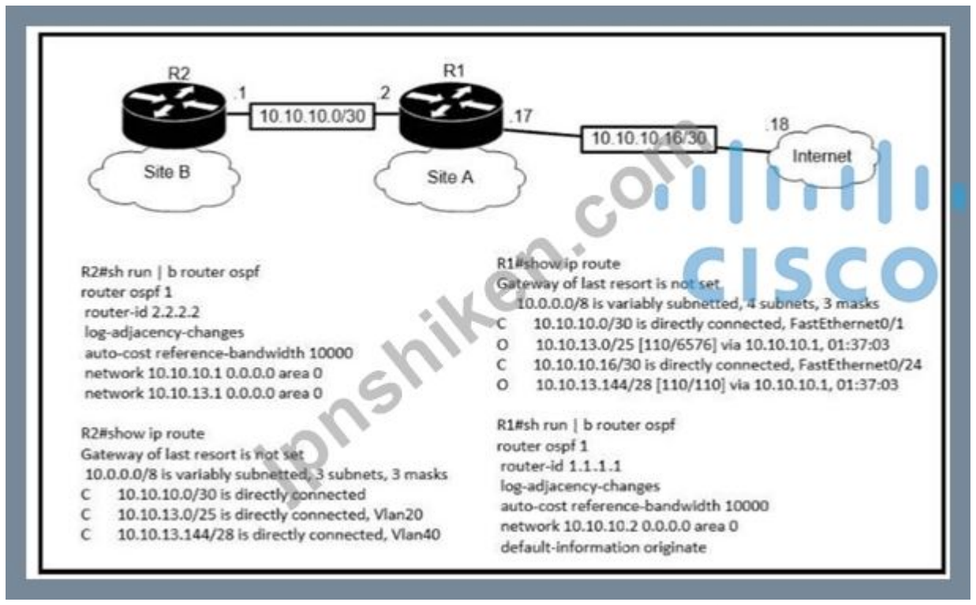
質問: **2**
PC がポートに接続されるとすぐにポートのどのコマンドがフォワーディング状態になりますか?
A. switch(config)#spanning-tree portfast デフォルト
B. switch(config)#spanning-tree portfast bpduguard default
C. switch(config-if)#spanning-tree portfast トランク

D. switch(config-if)#no スパニング ツリー ポートファスト
正解: **A (**コメントを発表する**)**
Use A for this item. The global spanning-tree portfast default command makes access ports transition to forwarding immediately when endpoints connect. PortFast is intended for host-facing access ports so DHCP and initial connectivity are not delayed by STP listening and learning behaviour. In Cisco CCNA 200-301 v1.
1, Network Access questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. The trunk PortFast command is for special trunk edge cases, and disabling PortFast would not meet the requirement. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **3**
最近のセキュリティ侵害とRADIUS障害を受けて、エンジニアは各エンタープライズルーターのコンソールポートをローカルのユーザー名とパスワードで保護する必要があります。このタスクを実行するために、エンジニアはどの設定を適用する必要がありますか？

A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解: **(**正解を表示します**)**
Option B. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **4**
展示資料を参照してください。



エンジニアが、ルーター1のGi0/1インターフェース上でMPLSプロバイダへの新しい回線を立ち上げています。この新しい回線はeBGPを使用し、BGPパスからVLAN25へのルートをチーミングします。ルート10.10.13.0/25のトラフィックフローの想定される動作は何ですか？

A. 10.10.13.0.25 へのトラフィックは、複数のインターフェースから負荷分散されます。

B. ルーティングテーブルに、インターフェース Gi0/1 から学習されたルート 10.10.13.0/25 が更新されました。

C. 10.10.13.0/25 へのトラフィックは非対称です

D. GiO/0 インターフェース経由で学習したルート 10.10.13.0/25 はルーティング テーブルに残っています

正解: **D** (コメントを発表する)

Route 10.10.13.0/25 learned via the GiO/0 interface remains in the routing table. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question.
That is why it remains the verified answer for this item.

質問: **5**

コピー機能を使用しながら、エンジニアが 20 のネットワーク ルーター構成をグローバルにバックアップできるプロトコルはどれですか?

A. SMTP

B. SNMP

C. TCP

D. FTP

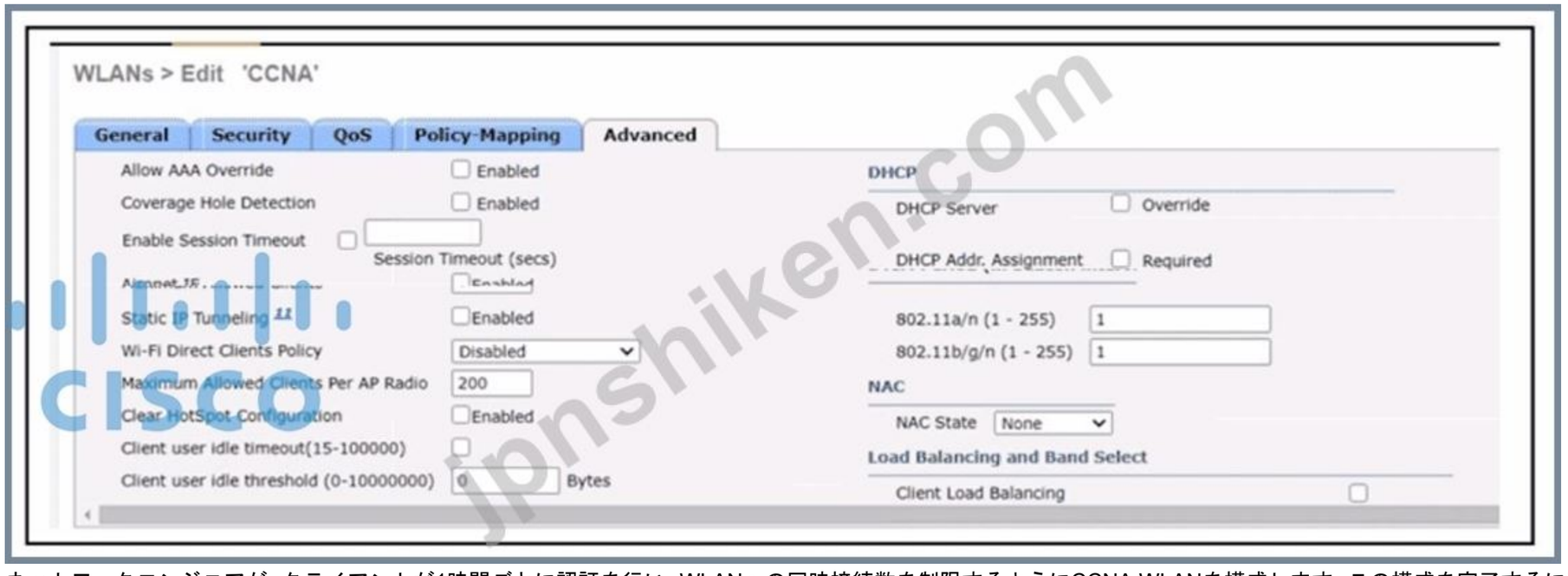
正解: (正解を表示します)

The protocol being tested is SNMP, because the question describes backing up many router configurations globally through a management mechanism tied to Cisco IOS MIB behavior. SNMP uses a manager-agent model and a Management Information Base to expose manageable objects on network devices. Through supported MIB objects and management tooling, an engineer can trigger or coordinate operations across many devices instead of manually logging into each router. SMTP is mail transport, not router configuration backup. TCP is a transport protocol, not the management protocol being selected here. FTP can transfer files, but the wording about global backup using the copy function in this exam item is aimed at SNMP-based management through Cisco IOS MIB support. Cisco CCNA 200-301 v1.1 IP Services

includes SNMP because monitoring and management are core operational services. The correct answer is B: SNMP. In practical operations, the file transfer target may still use a file service, but the management protocol controlling the function is SNMP.

質問: **6**
無線LANのニーズが最小限で、中央管理を必要としない小規模オフィスに最適なアーキテクチャはどれですか？
A. クラウドベースのアクセスポイント
B. MACを分割
C. 自律型AP
D. メッシュネットワーク
正解: **(**正解を表示します**)**
autonomous AP. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **7**
展示資料を参照してください。



ネットワークエンジニアが、クライアントが1時間ごとに認証を行い、WLANへの同時接続数を制限するようにCCNA WLANを構成します。この構成を完了するには、次のうちどの2つの操作を実行すればよいですか？
(2つ選択してください。)
A. [セッションタイムアウトを有効にする] オプションを有効にし、値を 3600 に設定します。
B. 最大許可クライアント数を 10 に設定します。

C. クライアント除外オプションを有効にして、値を3600に設定します。
D. Wi-Fi Directクライアントポリシーオプションを有効にします。
E. AP無線あたりの最大許容クライアント数を10に設定します。
正解: **A,B (**コメントを発表する**)**
Answer A,B is correct: A. Enable the Enable Session Timeout option and set the value to 3600.; B. Set the Maximum Allowed Clients value to 10.. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band.
The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities.
Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right- looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **8**
WPA3で実装された機能強化とは何ですか？
A. アクセスポイントを識別するためにPKIとRADIUSを使用します
B. 802.1x認証とAES-128暗号化を適用します
C. TKIPとパケットごとの鍵交換を使用します
D. 認証解除攻撃および解離攻撃から防御します
正解: **D (**コメントを発表する**)**
defends against deauthentication and disassociation attacks. Wireless questions depend on AP mode, WLAN security, RF band selection, controller interfaces, and client roaming or authentication behavior.
Cisco CCNA
200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong options confuse encryption with authentication, local switching with tunneling, or controller management with client data handling. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

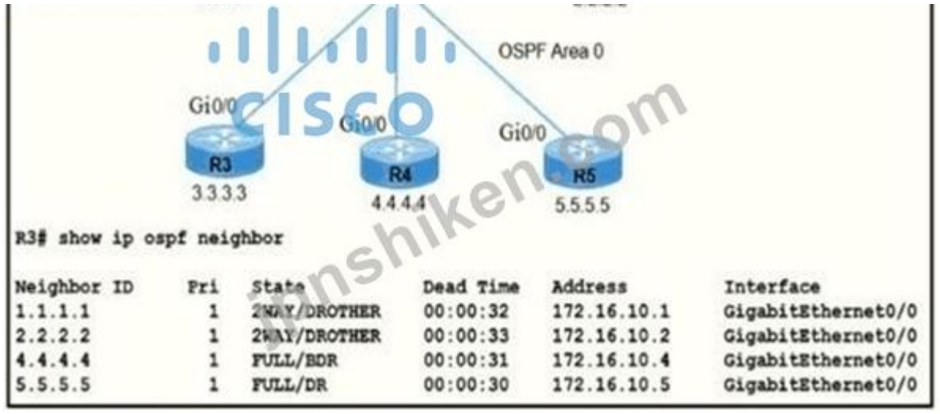
質問: **9**

図を参照してください。動的ルーティングプロトコルで学習された経路のうち、最も優先度の低いメトリックを持つのはどれですか？
A. EIGRP
B. OSPF
C. ローカル
D. RIP

正解: (正解を表示します)
RIP. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **10**
FlexConnectモードで動作するAPに接続し、WLANがFlexローカルスイッチングを使用する場合、どのスイッチポート構成を設定する必要がありますか？
A. VLANが1つあるアクセスポート
B. プルーニングされたVLANを持つトランクポート
C. IPアドレスを持つレイヤ3ポート
D. MACフィルタリングが有効になっているタグ付きポート
正解: (正解を表示します)
trunk port with pruned VLANs. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band.
The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities.
Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right- looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **11**
展示資料を参照してください。



R5 は現在ネットワーク上の DR であり、R4 は BDR です。これらのインターフェースがフラッピングを起こしているため、ネットワーク エンジニアは OSPF ネットワークで別の DR と BDR を選出したいと考えています。エンジニアはどのような設定を行う必要がありますか？

A.
```
R4(config)#interface gi0/0
R4(config-if)#ip ospf priority 20

R5(config)#interface gi0/0
R5(config-if)#ip ospf priority 10
```

B.
```
R2(config)#interface gi0/0
R2(config-if)#ip ospf priority 259
R3(config)#interface gi0/0
R3(config-if)#ip ospf priority 256
```

C.
```
R5(config)#interface gi0/0
R5(config-if)#ip ospf priority 120
R4(config)#interface gi0/0
R4(config-if)#ip ospf priority 110
```

D.
```
R3(config)#interface gi0/0
R3(config-if)#ip ospf priority 255
R2(config)#interface gi0/0
R2(config-if)#ip ospf priority 240
```

正解: (正解を表示します)

The correct response is D. OSPF DR and BDR election on a broadcast network is influenced by interface priority. To force different routers to win, the flapping routers should be given priority 0 or lower priority while the desired routers have higher priority, followed by a neighbor reset if needed. For Cisco CCNA 200-
301 v1.1, the important point is the mechanism, not a generic description of the technology. Changing unrelated process values or router IDs alone does not reliably replace an already elected DR/BDR on a live segment. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **12**

Rapid PVST+ が設定されたスイッチで入力されるコマンドのうち、特定の期間リッスンして学習するものはどれですか。

A. スイッチ(config)#スパニングツリーVLAN 1最大年齢6

B. スイッチ(config)#スパニングツリーVLAN 1 hello-time 10

C. スイッチ(config)#スパニングツリーVLAN 1 優先度4096

D. スイッチ(config)#スパニングツリーVLAN 1 転送時間 20

正解: (正解を表示します)

Forward-time is the Rapid PVST+/STP timer that controls the listening and learning periods before a port is allowed to forward user traffic. The command spanning-tree vlan 1 forward-time 20 sets that timer for VLAN
1 to 20 seconds. The other commands tune different STP values: max-age controls how long bridge protocol information is retained, hello-time controls BPDU transmission frequency, and priority affects root-bridge election. For CCNA 200-301 v1.1 Network Access, the key distinction is that a port must listen, then learn MAC addresses, then forward. Cisco Catalyst documentation describes forward time as the value that determines how long the listening and learning states last before forwarding begins. Because the question specifically says the switch "listens and learns for a specific time period," the only command that directly matches that behavior is the VLAN forward-time command. Reference: Cisco Catalyst Spanning Tree configuration guidance; CCNA 200-301 v1.1 Network Access objectives.

質問: **13**

エンジニアがフローティングスタティックルートを設定する理由を2つ挙げてください。(2つ選択してください)

A. プライマリパスがダウンしたときに、トラフィックをセカンダリパスに自動的にルーティングする

B. パケットの送信元IPに基づいてトラフィックを異なる方法でルーティングする

C. 動的ルーティングプロトコルが失敗した場合にフォールバック静的ルーティングを有効にする

D. 静的ルーティングによる負荷分散をサポートする

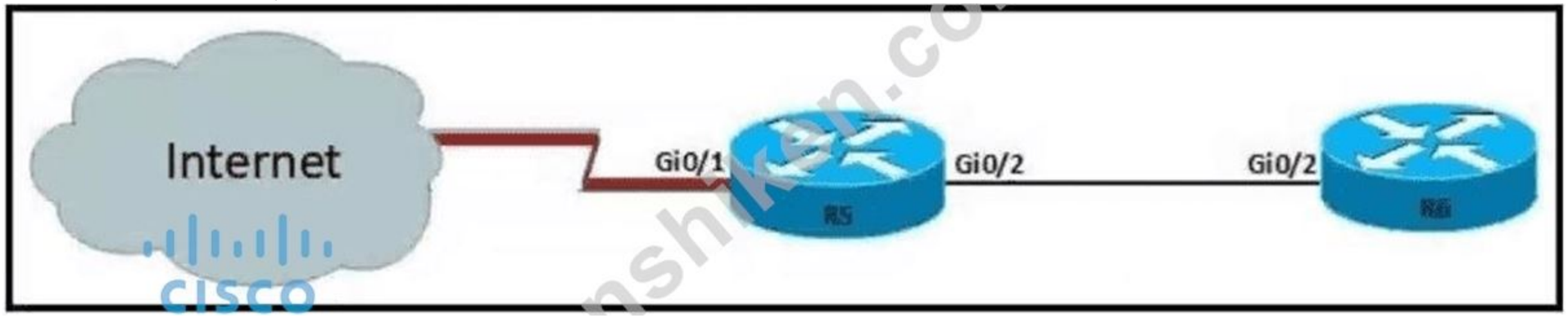
E. ルーターから送信されるトラフィックの戻り経路を制御する

正解: (正解を表示します)

Answer A,C is correct: A. to automatically route traffic on a secondary path when the primary path goes down; C. to enable fallback static routing when the dynamic routing protocol fails. Cisco routers forward by longest prefix match first, then use administrative distance and metric when competing routes describe the same destination prefix. Cisco CCNA 200-301 v1.1 includes this topic under IP Connectivity, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it

is configured, and what result it produces. Choices with the wrong prefix, mask, next hop, or administrative distance would either not match the traffic or would not behave as the intended backup path. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **14**
展示資料を参照してください。



セキュリティ上の理由から、R5のGi0/1インターフェースでは自動ネイバー検出を無効にする必要があります。以下のタスクを完了してください。
* R5インターフェースGiO/1上のすべての近隣探索方法を無効にします。
* R5インターフェースGiO/2での近隣ノード検出を許可する。
* R5インターフェースGi0/1に動的に学習されたネイバーが存在しないことを確認します。
* R6*のインターフェースGi0/2のIPアドレスを表示します。
どの構成を使用すべきですか？

R5(config)#int Gi0/1
R5(config-if)#no cdp run
R5(config-if)#exit
R5(config)#lldp run
R5(config)#cdp enable
R5#sh cdp neighbor
R5#sh lldp neighbor

R5(config)#int Gi0/1
R5(config-if)#no cdp enable
R5(config-if)#exit
R5(config)#no lldp run
R5(config)#cdp run
R5#sh cdp neighbor
R5#sh lldp neighbor

R5(config)#int Gi0/1
R5(config-if)#no cdp enable
R5(config-if)#exit
R5(config)#no lldp run
R5(config)#cdp run
R5#sh cdp neighbor detail
R5#sh lldp neighbor

R5(config)#int Gi0/1
R5(config-if)#no cdp enable
R5(config-if)#exit
R5(config)#lldp run
R5(config)#no cdp run
R5#sh cdp neighbor detail
R5#sh lldp neighbor

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)
Option C. The answer follows directly from normal Cisco device behavior and the wording of the scenario.
Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **15**
展示資料を参照してください。

ルーターは192.168.12.16へのトラフィックをどのように管理しますか？
A. 宛先アドレスを含めた最長のプレフィックスを持つRIPルートを選択します。
B. 宛先アドレスを含めた最長のプレフィックスを持つため、OSPF ルートを選択します。

C. 3つのルートすべて間でトラフィックの負荷分散を行います
D. 管理距離が最も低いEIGRPルートを選択します
正解: **A (**コメントを発表する**)**
Routers choose the route with the longest matching prefix before comparing protocol preference for equally specific routes. If the RIP entry contains the longest prefix that includes destination 192.168.12.16, that route is selected even though RIP has a worse administrative distance than OSPF or EIGRP. Administrative distance only becomes the deciding factor when competing routes describe the same prefix length. Cisco CCNA 200-301 v1.1 IP Connectivity repeatedly tests this rule because it is fundamental to forwarding decisions. The router does not load-balance among routes simply because multiple protocols know related networks. It also does not choose EIGRP solely because EIGRP has a lower administrative distance when another route is more specific. The forwarding lookup starts with the destination IP address and finds the most specific matching prefix in the routing table. In this exhibit, the RIP route is the longest prefix inclusive of
192.168.12.16, so A describes the router behavior correctly.

質問: **16**
展示資料を参照してください。

TenGigabitEthernet0/0インターフェースを介して流れるトラフィックの転送速度が低下しています。この問題の原因は何でしょうか？
A. 深刻な交通渋滞
B. 二重鎖の不適合
C. 速度の競合
D. キューイングドロップ
正解: **(**正解を表示します**)**
a speed conflict. The answer follows from normal Cisco device behavior and the operating clue in the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command.
The other options use adjacent terms, wrong-layer behavior, or configuration that would not produce the requested result. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **17**

図を参照してください。ルーター1は、ホスト10.10.13.165宛てのパケットをどのデバイスに送信しますか？

A. ルーター2
B. ルーター3
C. ルーター4
D. ルーター5

正解: **B** (コメントを発表する)

Router3. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **18**

プライベートIPv4アドレスを使用する利点を2つ挙げてください。(2つ選択してください。)

A. 外部インターネットネットワーク接続を提供します
B. 無制限のアドレス範囲を提供します
C. WANリンクにルーティング情報を伝播する
D. 複数のサイトでアドレスを再利用します

E. グローバルに一意なアドレス空間を節約します
正解: (正解を表示します)
Answer D,E is correct: D. reuses addressses at multiple sites; E. conserves globally unique addresss space.
Network fundamentals questions require careful attention to address scope, media type, cabling limits, topology design, virtualization, cloud service models, and the difference between TCP and UDP. The CCNA
200-301 v1.1 blueprint expects candidates to identify not only definitions but also the operational consequence of each choice. For example, public and private addressing have different routing behavior; fiber and copper use different physical media; TCP and UDP make different reliability tradeoffs; and virtualization abstracts physical resources through a hypervisor. The wrong answers are usually plausible terms from the same area, but they do not match the exact condition described in the question. The selected answer is correct because it is the only option that fits the stated network behavior, design requirement, or physical/logical property. That is the level of precision needed for Cisco troubleshooting and implementation work.

質問: **19**
どの操作の組み合わせが多要素認証の要件を満たしますか？
A. ユーザーはユーザー名とパスワードを入力し、モバイルデバイス上の認証アプリの通知をクリックします。
B. ユーザーがキーフォブをスワイプし、メールのリンクをクリックします。
C. ユーザーはRSAトークンにPINを入力し、ログイン画面に表示されたRSAキーを入力します。
D. ユーザーはユーザー名とパスワードを入力し、その後、2番目の画面で認証情報を再入力します。
正解: (正解を表示します)
The user enters a user name and password, and then clicks a notification in an authentication app on a mobile device.. Security questions in CCNA 200-301 v1.1 require matching the control to the threat or access requirement. Authentication proves identity, authorization controls what the user can do, and accounting records activity. Firewalls inspect and permit or deny traffic based on policy, while ACLs match packet fields in a defined order. VPN and IPsec questions require knowing whether the design protects unicast traffic, supports tunneling, or encrypts the original packet. Password and SSH questions depend on IOS behavior, including encrypted secrets, local users, domain names, and cryptographic images. The incorrect choices often use a valid technology in the wrong role or provide weaker protection. The selected answer is the Cisco- consistent control because it directly satisfies the access, confidentiality, or threat-mitigation requirement stated in the question.

質問: **20**
左側のIPv6アドレスの種類を、右側のそれぞれの説明にドラッグ＆ドロップしてください。

正解:

Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.

質問: **21**

コミットされたアクセスレートを超えるトラフィックを破棄するQoS機能はどれですか？

A. シェーピング

B. 警察活動

C. 重み付き公平キューイング

D. FIFO

正解: **(**正解を表示します**)**

Policing. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic.

Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

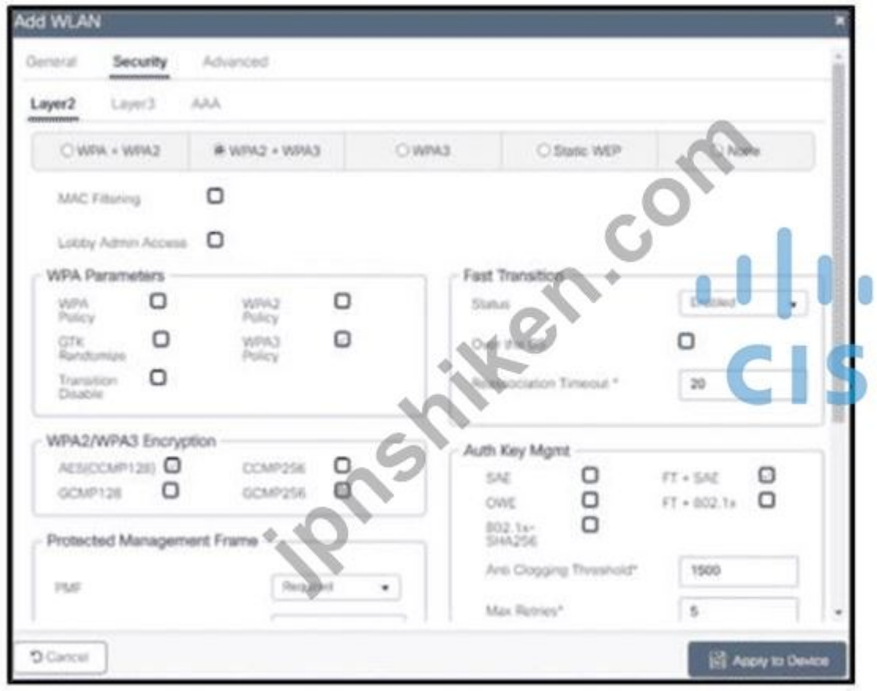
質問: **22**

管理、ローミング、および SSID 設定を中央コントローラに依存するアクセス ポイント モードはどれですか?

A. リピーターモード

B. 自律モード
C. ブリッジモード
D. 軽量モード
正解: (正解を表示します)
lightweight mode. Wireless questions require separating client association, RF design, AP mode, WLAN security, and controller policy. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Incorrect answers usually confuse an encryption method with authentication, or a controller feature with a switchport feature. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **23**



図を参照してください。このSSIDは、無線クライアントが使用する際にどのような機能を持ちますか？
A. オフライン辞書攻撃に対するネットワークセキュリティを低下させ、ネットワークへの容易なアクセスを助長します
B. オフライン辞書攻撃に対するネットワークセキュリティを強化し、時間のかかるブルートフォース攻撃を抑制します。
C. 中間者攻撃に対するネットワークセキュリティを強化し、サービス拒否攻撃を抑制します。
D. 無線傍受攻撃に対するネットワークセキュリティを低下させ、複雑なパスワードの使用を抑制します。
正解: (正解を表示します)
decreases network security against air sniffing attacks and discourages the use of complex passwords. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1

includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

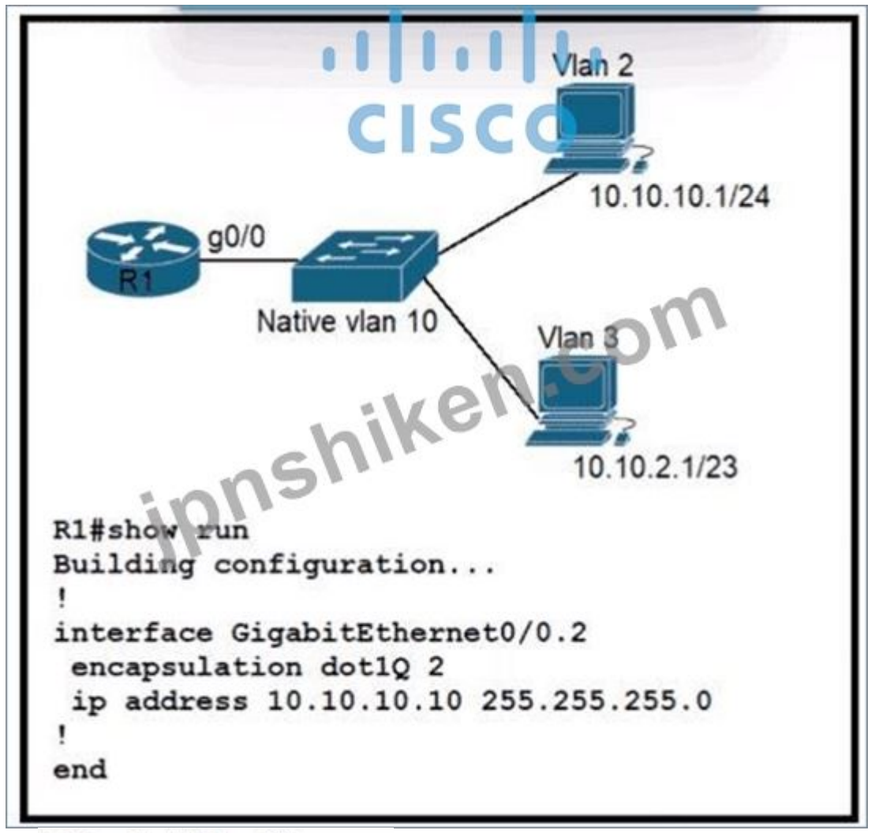
質問: **24**
攻撃者がシステム管理者の平文パスワードを傍受できた場合、パスワード攻撃を軽減する上で適切な解決策はどれですか？
A. ステートフルパケットインスペクションを維持する次世代ファイアウォール
B. 2つの異なる認証ソースを使用した多要素認証
C. 受信Telnetセッションの「admin」アカウントを制限するACL
D. 既知の攻撃ベクトルのブロックリストを備えたIPS
正解: **A (**コメントを発表する**)**
next-generation firewall to keep stateful packet inspection. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **25**
VRRP で仮想アドレスとして使用される MAC アドレスは何ですか?
A. 00-00-0C-07-AD-89
B. 00-00-5E-00-01-0a
C. 00-07-C0-70-AB-01
D. 00-C6-41-93-90-91
正解: **(**正解を表示します**)**
00-00-5E-00-01-0a. IP services must be selected by their exact operational role: addressing, translation, time, monitoring, logging, redundancy, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The wrong options name real services or commands, but they solve a different infrastructure problem. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path.
The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **26**
組織は、従業員のスマートフォンの認証アプリを使用して、多要素認証でネットワークを保護します。ユーザーのスマートフォンが紛失または盗難にあった場合、アプリケーションはどのように保護されますか?
A. アプリケーションは、構成された間隔の後に再アクティブ化するために管理者パスワードを必要とします。
B. アプリケーションは、2 番目の要素を提供する前に、ユーザーが PIN を入力することを要求します。
C. アプリケーションは、スマートフォンの再起動時に管理者パスワードの再アクティブ化を要求することで、ユーザーにチャレンジします。
D. アプリケーションは、2 番目の要素を提供する前に、ユーザーが特定の場所にいることを確認します。
正解: **(**正解を表示します**)**
The application requires the user to enter a PIN before it provides the second factor.. Security fundamentals require distinguishing identity, authorization, accounting, encryption, inspection, and physical protection.

Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The incorrect choices apply a security term in the wrong control category or protect a different part of the system. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: 27



A.
```
interface GigabitEthernet0/0
  ip address 10.10.2.10 255.255.252.0
```

B.
```
interface GigabitEthernet0/0.3
  encapsulation dot1Q 10
  ip address 10.10.2.10 255.255.255.252
```

C.
```
interface GigabitEthernet0/0.10
  encapsulation dot1Q 3
  ip address 10.10.2.10 255.255.254.0
```

D.
```
interface GigabitEthernet0/0.3
  encapsulation dot1Q 3 native
  ip address 10.10.2.10 255.255.252.0
```

正解: **C** (コメントを発表する)

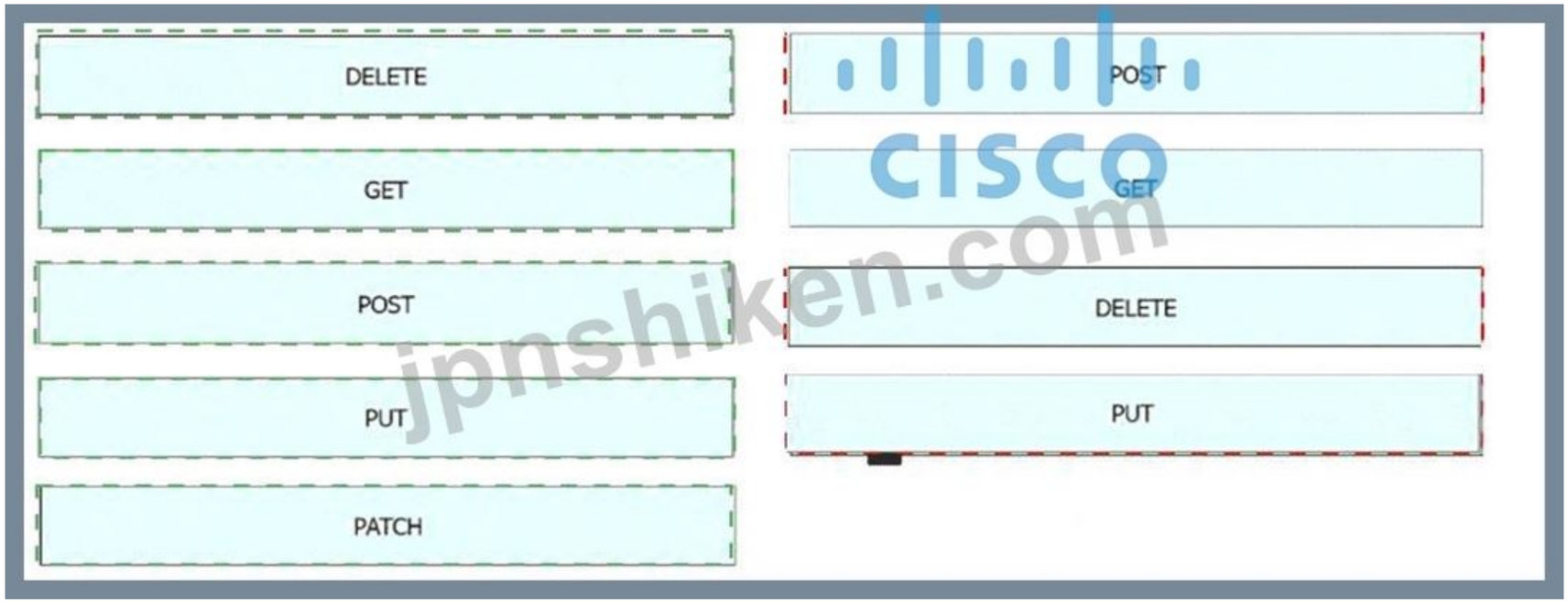
Option C. The answer follows from standard Cisco behavior and the operational clue in the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller

role. The other choices are adjacent technologies or commands, but they do not meet the stated requirement. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **28**
仮想マシンをデプロイする前に考慮すべき事項は何ですか？
A. データセンター環境内における仮想マシンの配置場所
B. 複数の仮想プロセッサを2つ以上の仮想マシンにマッピングするためにVSMを活用するかどうか
C. CPUコア数やメモリ容量などのリソース制限
D. モニター、キーボード、マウスなどの物理的な周辺機器のサポート
正解: **(**正解を表示します**)**
resource limitations, such as the number of CPU cores and the amount of memory. Network fundamentals questions require careful attention to address scope, media type, cabling limits, topology design, virtualization, cloud service models, and the difference between TCP and UDP. The CCNA 200-301 v1.1 blueprint expects candidates to identify not only definitions but also the operational consequence of each choice. For example, public and private addressing have different routing behavior; fiber and copper use different physical media; TCP and UDP make different reliability tradeoffs; and virtualization abstracts physical resources through a hypervisor. The wrong answers are usually plausible terms from the same area, but they do not match the exact condition described in the question. The selected answer is correct because it is the only option that fits the stated network behavior, design requirement, or physical/logical property. That is the level of precision needed for Cisco troubleshooting and implementation work.

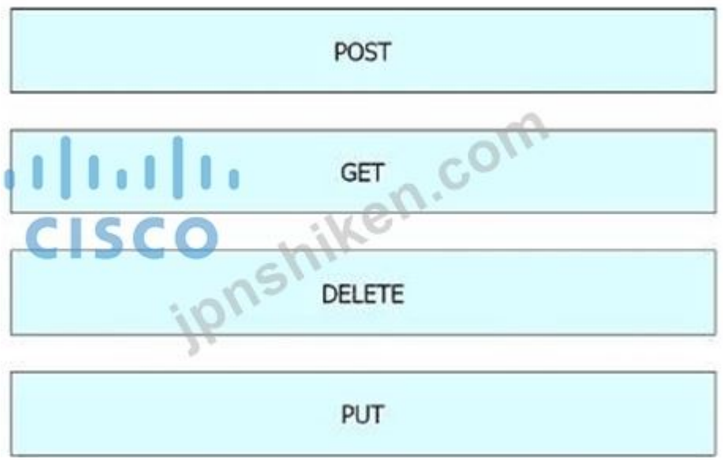
質問: **29**
左側のHTTP用REST API呼び出しメソッドを、右側のそれらが実行するアクションにドラッグアンドドロップしてください。

正解:



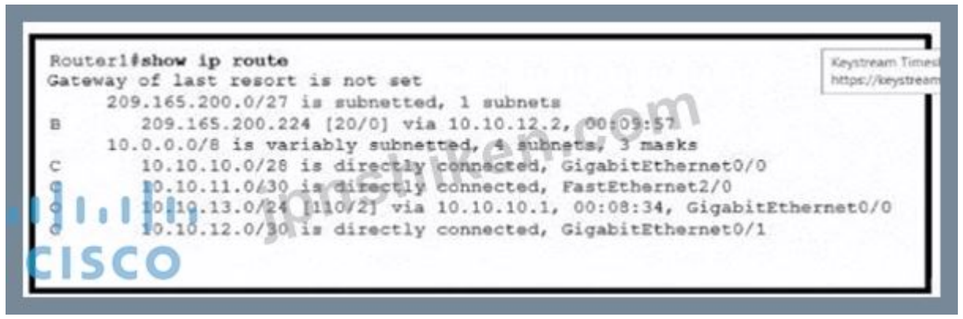
Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this form test whether each protocol, command, service, or architecture term is placed with the function it actually performs. The safest approach is to classify each item by operating layer and purpose before matching it: routing behavior belongs to IP connectivity, wireless modes belong to access, REST methods belong to automation, and AAA functions belong to security services. Several distractors are valid networking terms, but they become wrong when mapped to the wrong plane or protocol. The retained mapping follows Cisco terminology and reflects how the features are used in implementation and troubleshooting. In practice, this prevents mixing up forwarding behavior with management behavior or authentication with authorization/accounting. The mapping shown in the file is therefore retained as the verified response.



質問: 30

展示資料を参照してください。



パケットが10.10.10.2から送信され、10.10.10.16宛ての場合、ルーターはどのような動作を実行しますか？

A. 宛先アドレスに似たルートを使用します

B. パケットを破棄します。

C. 学習済みのすべてのネクストホップにパケットをフラッディングします。

D. 経路が学習されるのを待っているパケットをキューに入れます。

正解: **A** (コメントを発表する)

It uses a route that is similar to the destination address. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under IP Connectivity, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **31**

ネットワークエンジニアが、SSH経由でリモートからアクセスできるようにスイッチを設定しています。ホスト名は既に設定済みです。RSAキーを生成するコマンドを入力する前に、エンジニアはどの追加コマンドを設定する必要がありますか？

A. IPドメイン名ドメイン

B. パスワード パスワード

C. 暗号鍵生成 RSA モジュラス 1024

D. ip ssh 認証再試行回数 2

正解: (正解を表示します)

ip domain-name domain. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable
/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

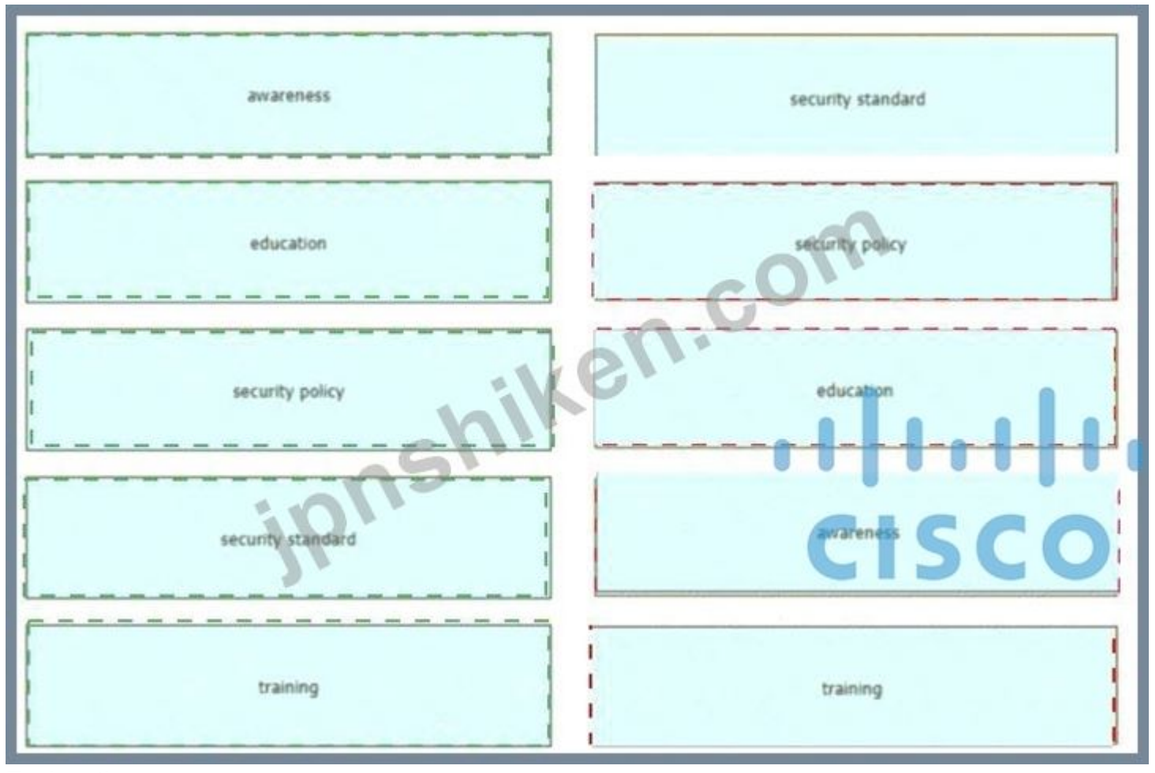
質問: **32**
サウスバウンドAPIの機能は何ですか？
A. サーバーとスイッチングファブリック間の構成変更を自動化します。
B. オーケストレーションを使用して、Web サーバーから仮想サーバー構成をプロビジョニングします。
C. SDNコントローラとスイッチングファブリック間のフロー制御を管理します。
D. SDNコントローラとアプリケーション間の情報交換を促進します。
正解: **C** (コメントを発表する)
Manage flow control between an SDN controller and a switching fabric.. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol:
LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **33**
WPA3 実装に適したセキュリティ プロトコルはどれですか?
A. CCMP
B. MD5
C. TKIP
D. GCMP
正解: (正解を表示します)
GCMP. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **34**
セキュリティプログラムの要素を左側から右側の対応する説明にドラッグ＆ドロップしてください。

jpnshiken.com

正解:



jpnshiken.com
cisco

Explanation:

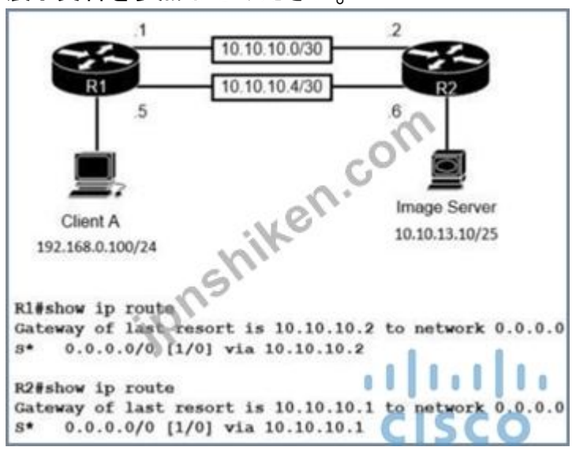
Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.

cisco
jpnshiken.com

質問: **35**
ルーターを DHCP サーバーとして実装する場合、どの 2 つの機能を構成する必要がありますか? (2つ選んでください)
A. リレーエージェント情報
B. データベース エージェント
C. アドレス プール
D. スマートリレー
E. 手動綴じ
正解: **C,E (**コメントを発表する**)**
The correct response is C and E. A Cisco router acting as a DHCP server must have a DHCP address pool and can use manual bindings when specific addresses must be reserved. The pool defines the scope of addresses and options that clients receive; bindings tie a known client identifier or MAC-related value to an address when deterministic assignment is required. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. Relay-agent information and smart-relay support relay behaviour, and a database agent is optional persistence rather than the core server configuration being tested. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **36**
不正なDHCPサーバーを識別するために何が使用されますか？
A. DHCPリクエスト

B. DHCPDISCOVER
C. DHCPACK
D. DHCPオファー
正解: **D** (コメントを発表する)
DHCPOFFER. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic.
Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **37**
展示資料を参照してください。


画像サーバーとクライアントAは、両者間で非常に大量のデータを転送するアプリケーションを実行しています。エンジニアはR1とR2の間に専用回線を設定しています。画像サーバーとクライアントA間のトラフィックのみが新しい回線を使用するようにするには、エンジニアはルーターにどのコマンドセットを適用する必要がありますか？
A. R1(config)#ip route 10.10.13.10 255.255.255.255 10.10.10.6 R2(config)#ip route 192.168.0.100
255.255.255.255 10.10.10.5
B. R1(config)#ip route 10.10.13.10 255.255.255.128 10.10.10.6R2(config)#lp route 192.168.0.100
255.255.255.0 10.10.10.5
C. R1(config)#ip route 10.10.13.10 255.255.255.252 10.10.10.6 R2(config)#tp route 192.168.0.100
255.255.255.252 10.10.10.5
D. R1(config)#ip route 10.10.13.10 255.255.255.255 10.10.10.2R2(config)#ip route 192.168.0.100
255.255.255.255 10.10.10.1
正解: (正解を表示します)
R1(config)#ip route 10.10.13.10 255.255.255.255 10.10.10.2R2(config)#ip route 192.168.0.100
255.255.255.255 10.10.10.1. Routing and redundancy questions are solved by applying longest-prefix match, administrative distance, metrics, and gateway-redundancy behavior in the correct order. Cisco CCNA 200-
301 v1.1 includes this under IP Connectivity, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Incorrect choices point to the wrong next hop, choose the wrong route source, or confuse routing with Layer 2

behavior. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **38**
無線LANコントローラへの管理接続のセキュリティを強化するために、どの2つのプロトコルを無効にする必要がありますか？(2つ選択してください。)
A. Telnet
B. SSH
C. HTTP
D. HTTPS
E. TFTP
正解: **(正解を表示します)**
Answer A,C is correct: A. Telnet; C. HTTP. Wireless operation depends on WLAN identity, AP mode, RF management, client authentication, and controller-based policy enforcement. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The distractors confuse WLAN names, authentication, encryption, RF optimization, and controller management functions. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **39**
WLCは不正なAPに関するアラームを送信し、ネットワーク管理者はアラームが正当な自律型APによって引き起こされたものであることを確認します。
A. APを手動封じ込め状態にする。
B. AP を WLC 管理から削除します。
C. APを保留状態から手動で削除します。
D. APクラスタイプをフレンドリーに設定します。
正解: **(正解を表示します)**
Set the AP Class Type to Friendly.. If the WLC detects a rogue AP but the administrator verifies that it is legitimate, the correct operational response is to classify it as Friendly. Manual containment is used against malicious or unauthorized rogues and can create legal and operational problems if used against a legitimate AP. Removing the AP from WLC management does not correctly classify the rogue alarm. Cisco CCNA 200-
301 v1.1 Network Access includes rogue AP handling because wireless security is partly about classification and policy, not just encryption. Setting the AP Class Type to Friendly tells the WLC that this AP is known and accepted, which suppresses inappropriate rogue treatment while preserving monitoring visibility. The corrected answer is to set the AP Class Type to Friendly.

質問: **40**
グローバルに一意のアドレス クラスを維持するのに役立つ IPv4 アドレス タイプはどれですか?
A. マルチキャスト
B. プライベート
C. ループバック
D. 公開
正解: **(正解を表示します)**
private. Network fundamentals questions require recognizing address scope, media type, connector form factor, topology, and cloud or private addressing behavior. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The incorrect choices may be plausible terms, but they do not match the scope, medium, or

topology described. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **41**
ルーターには、同じ OSPF プロセスの下で同じ宛先ネットワークへの 2 つの静的ルートがあります。
ネクストホップ デバイスが異なる場合、ルーターはどのようにパケットを宛先に転送しますか?
A. ルータは最も古い経過時間を持つルートを選択します。
B. ルーターは、宛先へのすべてのルートでトラフィックを負荷分散します。
C. ルーターは、MAC アドレスが最も小さいネクスト ホップを選択します。
D. ルーターは、IP アドレスが最も小さいネクスト ホップを選択します。
正解: **B (**コメントを発表する**)**
The router load-balances traffic over all routes to the destination.. IP services questions require matching the service to its exact operational role, such as logging, address assignment, file transfer, monitoring, redundancy, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The distractors are real technologies, but they solve different infrastructure problems. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

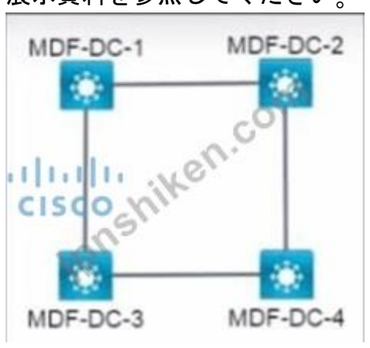
質問: **42**
どのタイプのネットワーク攻撃は、標的サーバーの半開き状態のTCPリソースが枯渇するまで、ポートに複数のパケットを送信することで標的サーバーを圧倒するのでしょうか？
A. SYNフラッド
B. 反射
C. 涙滴
D. 増幅
正解: **(**正解を表示します**)**
SYN flood. The answer follows directly from normal Cisco device behavior and the wording of the scenario.
Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **43**
エンジニアは、ISPに接続するように会社のPEルータのインターフェイスGi1/0を設定します。近隣探索が無効になります。

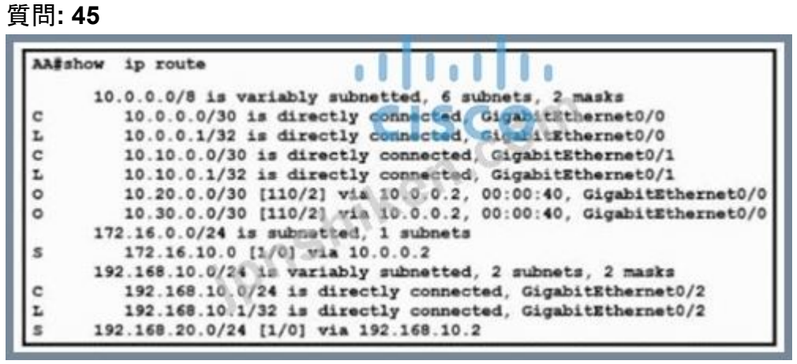
```
interface Gi1/0
description HQ_DC3978-87297
duplex full
speed 100
negotiation auto
lldp transmit
lldp receive
```

ISPがサードパーティのネットワークデバイスを使用している場合、構成を完了するために必要なアクションはどれですか。
A. LLDPをグローバルに有効にする
B. オートネゴシエーションを無効にする

C. インターフェイスでCiscoDiscoveryProtocolを無効にします
D. ISPデバイスでLLDP-MEDを有効にする
正解: **(**正解を表示します**)**
Enable LLDP globally. LLDP is the standards-based neighbor discovery protocol used in multivendor environments. Cisco Discovery Protocol is Cisco proprietary, so it is not the correct tool when the ISP uses third-party devices and Neighbor Discovery needs to work across the PE-to-ISP connection. Enabling LLDP globally allows the Cisco device to advertise and receive LLDP neighbor information, assuming the interface also permits it. Cisco CCNA 200-301 v1.1 Network Access expects engineers to know when to use CDP and when to use LLDP. Disabling autonegotiation does not solve neighbor discovery, and disabling CDP only removes Cisco proprietary discovery without replacing it. LLDP-MED is an extension mainly used for endpoint and voice-related discovery, not the basic requirement here. The necessary action is to enable LLDP globally.

質問: **44**
展示資料を参照してください。


すべてのインターフェースは同じVLANに属しています。すべてのスイッチはデフォルトのSTP優先度で設定されています。STP処理中に、どのスイッチがルートブリッジになりますか？
A. MDF-DC-4:08:E0:19: 08:B3:19
B. MDF-DC-3:08:0E:18::1A:3C:9D
C. MDF-DC-08:0E:18:22:05:97
D. MDF-DC-1:DB:E:44:02:54:79
正解: **C (**コメントを発表する**)**
MDF-DC-08:0E:18:22:05:97. Switching questions depend on MAC learning, VLAN membership, trunking, STP election, and EtherChannel behavior. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong answers misapply a Layer 2 rule or configure the wrong logical interface. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **45**


図を参照してください。ホストIPアドレス10.30.0.1を含むアドバタイズされたプレフィックスの管理距離はどれくらいですか？
A. 10.0.0.2
B. 110
C. 30
D. 2
正解: (正解を表示します)
110. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

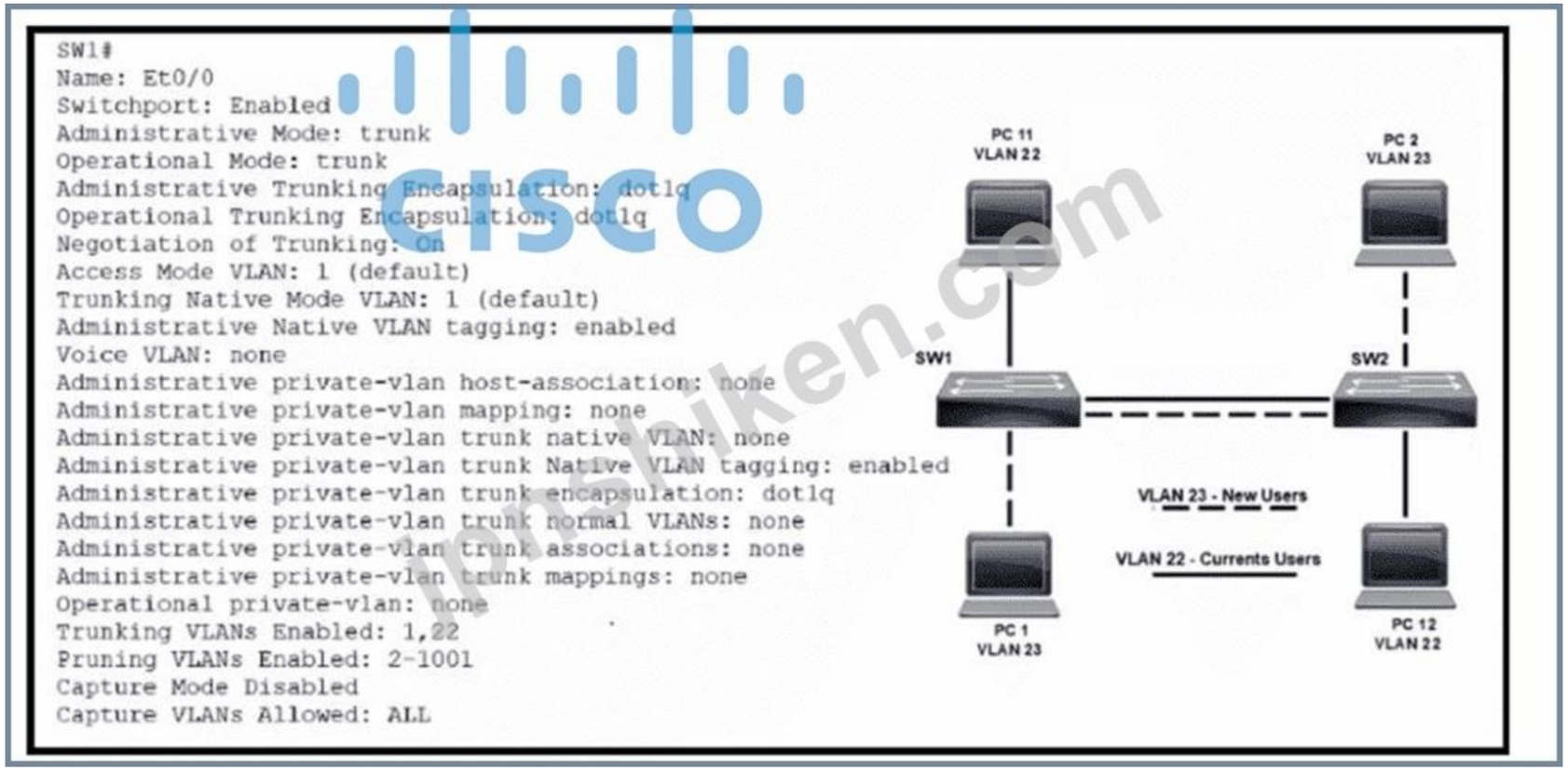
質問: **46**
ルーターで SSH 用の RSA キーを生成するには、どの構成が必要ですか?
A. SSH のバージョンを設定する
B. VTY アクセスを構成します。
C. パスワードを持つユーザーを作成します。
D. DNS ドメイン名を割り当てます
正解: (正解を表示します)
Assign a DNS domain name. IP services questions test the exact function of infrastructure services such as addressing, name resolution, time synchronization, logging, monitoring, and secure management. Cisco CCNA 200-301 v1.1 includes this topic under IP Services, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces.
The distractors name valid services, but they provide a different service function from the one required in the prompt. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
ネットワーク エンジニアは、小規模なデータ センターをアップグレードして、ピーク時に帯域幅の最大 90% を占めると予想されるサーバー バックアップを含む、いくつかの新しいアプリケーションをホストしています。
データセンターは、プライマリ回線とセカンダリ回線を介して MPLS ネットワーク プロバイダーに接続します。バックアップに関連するトラフィックによるプライマリ回線の飽和を回避するために、エンジニアはデータセンターを安価に更新するにはどうすればよいでしょうか?
A. バックアップ サーバーからのトラフィックを専用スイッチに割り当てます。
B. バックアップ トラフィック用の専用回線を構成します。
C. バックアップ サーバーを専用の VLAN に配置します。

D. セカンダリ サーキット経由でバックアップ トラフィックのより具体的なルートをアドバタイズします。
正解: (正解を表示します)
Advertise a more specific route for the backup traffic via the secondary circuit.. The inexpensive way to prevent backup traffic from saturating the primary MPLS circuit is to steer that backup traffic over the secondary circuit. Advertising a more specific route for the backup destination through the secondary path influences routing without buying a new dedicated circuit or merely moving servers between switches or VLANs. A dedicated switch or VLAN does not prevent WAN saturation if the same WAN path is still used.
Cisco CCNA 200-301 v1.1 IP Connectivity expects engineers to apply route specificity and path selection to meet traffic-engineering goals. The corrected answer is advertising a more specific route for the backup traffic via the secondary circuit. Longest-prefix matching can then direct the backup flows to the intended path while leaving other traffic on the primary circuit.

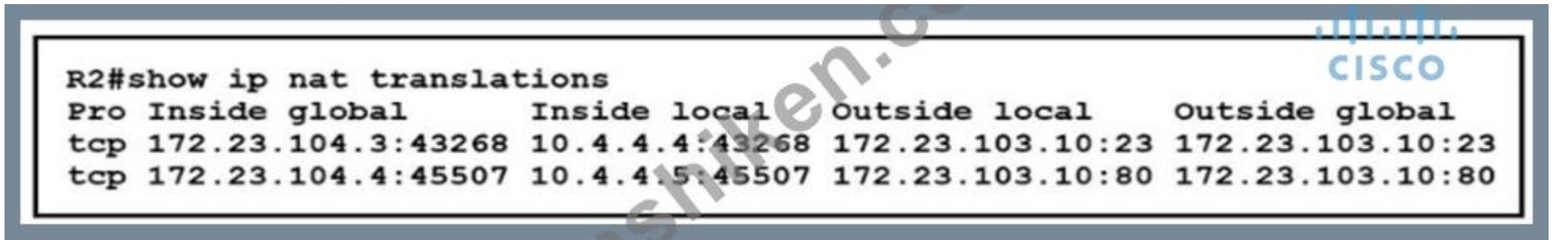
質問: **48**



図を参照してください。SW1とSW2の間でVLAN 23が実装されています。SW1でコマンドshow interface ethernet0/0 switchportが実行されました。SW1のEthernet0/0はSW2へのアップリンクです。アップリンクインターフェイスでどのコマンドを入力すると、PC 1とPC 2が通信でき、PC 11とPC 12間の通信に影響が出なくなりますか？
A. switchport trunk allowed vlan 2-1001
B. switchport trunk allowed vlan add 23
C. switchport trunk allowed vlan 23
D. switchport trunk allowed vlan 22-23
正解: (正解を表示します)
switchport trunk allowed vlan add 23. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with

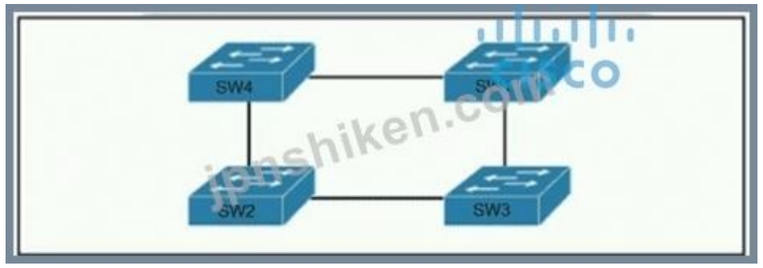
older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band.
The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities.
Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right- looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **49**
展示資料を参照してください。



エンジニアがNAT変換を設定し、設定が正しいことを確認しました。
送信元IPアドレスはどれですか？
A. 10.4.4.4
B. 10.4.4.5
C. 172.23.103.10
D. 172.23.104.4
正解: **D** (コメントを発表する)
In a NAT translation table, the source address seen after inside-to-outside translation is the inside global address. The inside local address is the private address assigned to the internal host. The inside global address is the translated address that represents that internal host to the outside network. In the exhibit-based answer set, 172.23.104.4 is the address used as the translated source, so D is correct. This question is easy to miss if NAT terms are treated as labels instead of traffic direction. For outbound traffic, NAT changes the source from the inside local value to the inside global value. For return traffic, NAT reverses the operation and maps the destination back to the inside local host. Cisco CCNA v1.1 IP Services includes NAT concepts and configuration, so candidates must know inside local, inside global, outside local, and outside global. The tested idea is not merely public versus private; it is which translated field is used as the packet source.

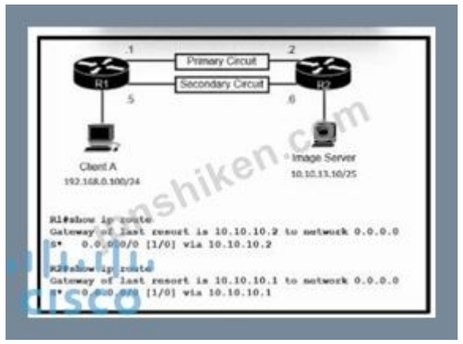
質問: **50**
展示資料を参照してください。



以下のスイッチのMACアドレスが与えられた場合、どのスイッチがルートブリッジとして選出されますか？
SW1: 0C:5A:05:53:27:17
SW2: 0C:0A:A8:1A:3C:9D
SW3: 0C:0A:18:81:83:19

SW4: 0C:0A:05:22:05:97
A. SW1
B. SW2
C. SW3
D. SW4
正解: (正解を表示します)
SW3. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology.
The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **51**



図を参照してください。ルータR1とR2は、それぞれLANインターフェースが設定されています。2つの回線は動作しており、WAN経由でアクセス可能です。プライマリ回線がダウンした場合にフェイルオーバー冗長性を確立するコマンドセットはどれですか？
A. Ri(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.62R2(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.5 2
B. Ri(config)#ip route 10.10.13.10 255.255.255.255 10.10.10.6R2(config)#ip route 192.168.0.100 255.255.255.255 10.10.10.5
C. Ri(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.6R2(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.5
D. Ri(config)#ip route 10.10.13.10 255.255.255.255 10.10.10.2R2(config)#ip route 192.168.0.100 255.255.255.255 10.10.10.1
正解: (正解を表示します)
Ri(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.62R2(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.5 2. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **52**

ネットワークエンジニアは、新しい Cisco IOS ルータにアクセスリストを設定する必要があります。アクセスリストは、192.168.240.0/20 ネットワークから 10.125.128.32/27 ネットワークへの HTTP トラフィックを拒否する必要がありますが、192.168.240.0 ネットワークからの HTTP トラフィックは許可する必要があります。
/20 ネットワークから 10.0.0.0/8 ネットワークの残りの部分にアクセスできるようにするには、エンジニアはどの設定を適用する必要がありますか？

A.
```
ip access-list extended deny_outbound
  10 deny tcp 10.125.128.32 255.255.255.224 192.168.240.0 255.255.240.0 eq 443
  20 deny tcp 192.168.240.0 255.255.240.0 10.125.128.32 255.255.255.224 eq 443
  30 permit ip 192.168.240.0 255.255.240.0 10.0.0.0 255.0.0.0
```

B.
```
ip access-list extended deny_outbound
  10 permit ip 192.168.240.0 255.255.240.0 10.0.0.0 255.0.0.0
  20 deny tcp 192.168.240.0 255.255.240.0 10.125.128.32 255.255.255.224 eq 443
  30 permit ip any any
```

C.
```
ip access-list extended deny_outbound
  10 deny tcp 192.168.240.0 0.0.15.255 10.125.128.32 0.0.0.31 eq 80
  20 permit ip 192.168.240.0 0.0.15.255 10.0.0.0 0.255.255.255
  30 deny ip any any log
```

D.
```
ip access-list extended deny_outbound
  10 deny tcp 192.168.240.0 0.0.15.255 any eq 80
  20 deny tcp 192.168.240.0 0.0.15.255 10.125.128.32 0.0.0.31 eq 80
  30 permit ip 192.168.240.0 0.0.15.255 10.0.0.0 0.255.255.255
```

正解: **C** (コメントを発表する)

Option C. Routing and redundancy questions are solved by applying longest-prefix match, administrative distance, metrics, and gateway-redundancy behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Incorrect choices point to the wrong next hop, choose the wrong route source, or confuse routing with Layer 2 behavior. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **53**
サブネット間の通信を提供し、インターネット上でルーティングできない IPv6 アドレスの種類はどれですか?
A. グローバルユニキャスト
B. 一意のローカル
C. リンクローカル
D. マルチキャスト
正解: **(**正解を表示します**)**
unique local. IPv6 questions require identifying the address scope, address block, assignment method, and the role of multicast, link-local, unique-local, or global-unicast addressing. Cisco CCNA 200-301 v1.1 includes this topic under Network Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The wrong choices describe another IPv6 scope or an assignment process that does not match the address behavior in the prompt.
In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **54**

図を参照してください。R3のループバックIPは、R1の2つのインターフェースを介して学習されています。R1は、10Gbpsの基準帯域幅で設定されています。メトリック計算に基づくと、送信ルーティングにはどのネクストホップIPが使用されますか？

A. 10.12.0.5
B. 10.12.0.2
C. 10.12.0.1
D. 10.12.0.6

正解: **D** (コメントを発表する)

10.12.0.6. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **55**

ネットワーク自動化のメリットを2つ挙げてください。(2つ選択してください。)

A. より迅速な変更とより信頼性の高い結果
B. 運用コストの削減
C. ネットワーク障害の減少
D. ハードウェアのフットプリントを削減
E. ネットワークセキュリティの強化

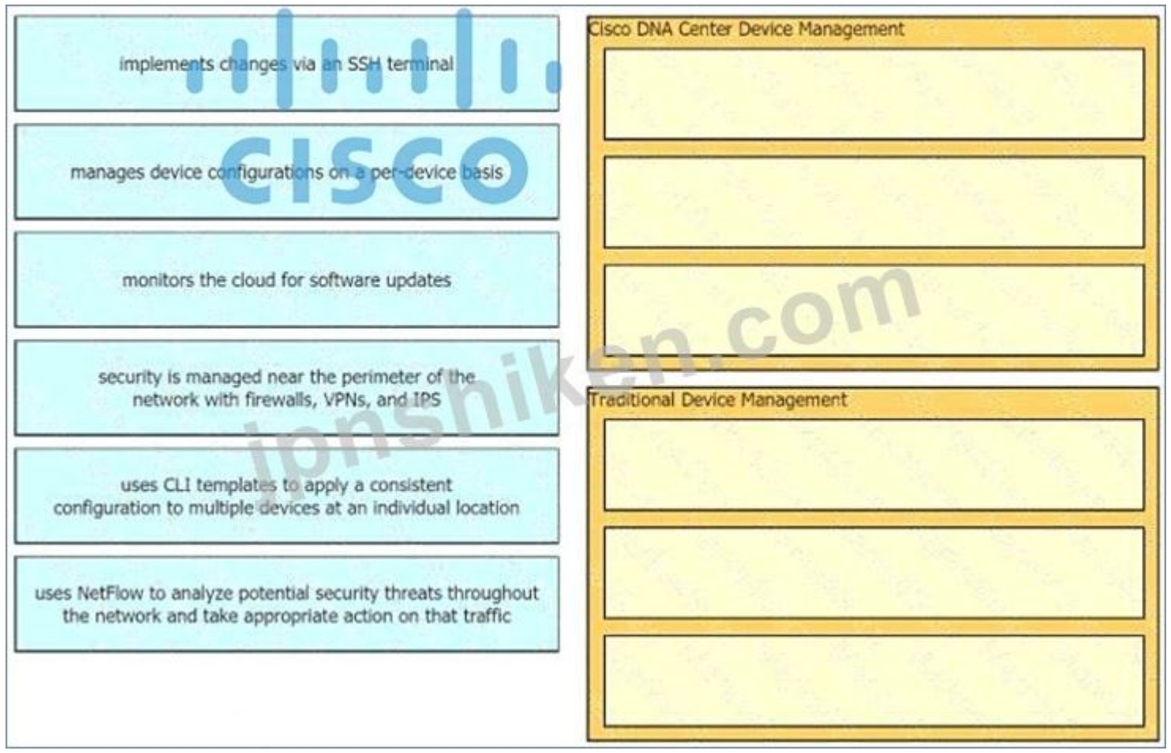
正解: (正解を表示します)

Answer A,B is correct: A. Faster changes with more reliable results; B. Reduced operational costs. Security questions in CCNA 200-301 v1.1 require matching the control to the threat or access requirement. Authentication proves identity, authorization controls what the user can do, and accounting records activity.

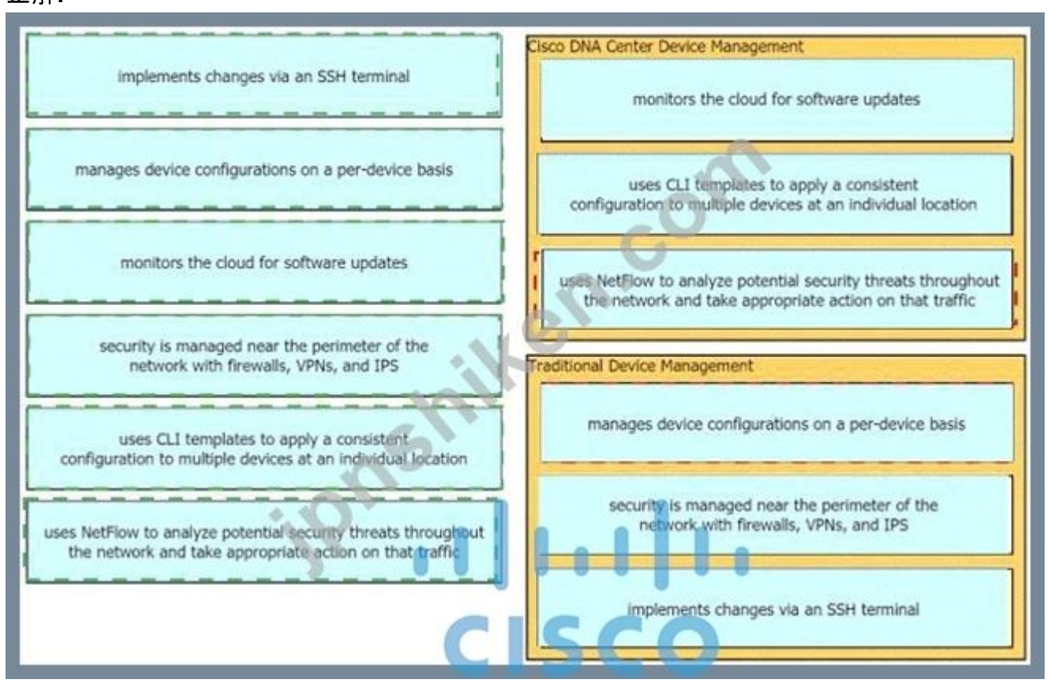
Firewalls inspect and permit or deny traffic based on policy, while ACLs match packet fields in a defined order. VPN and IPsec questions require knowing whether the design protects unicast traffic, supports tunneling, or encrypts the original packet. Password and SSH questions depend on IOS behavior, including encrypted secrets, local users, domain names, and cryptographic images. The incorrect choices often use a valid technology in the wrong role or provide weaker protection. The selected answer is the Cisco-consistent control because it directly satisfies the access, confidentiality, or threat-mitigation requirement stated in the question.

質問: **56**

左側のデバイス管理の説明を、右側のデバイス管理の種類にドラッグしてください。



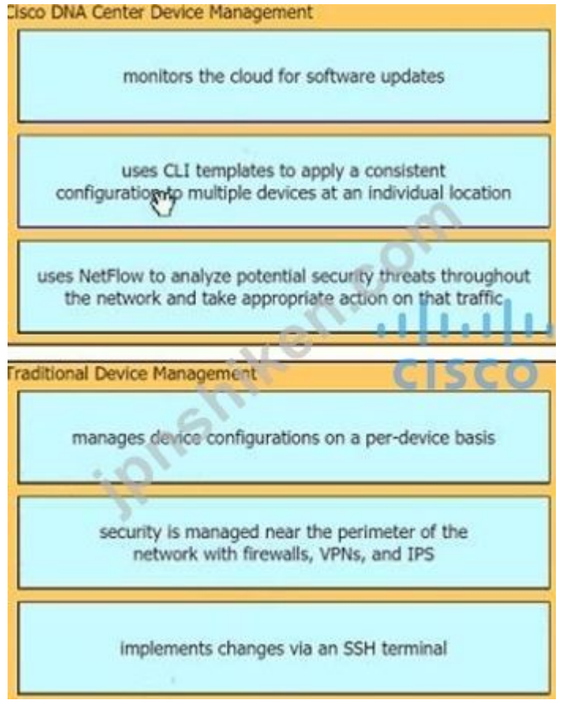
正解:



Explanation:

Cisco CCNA 200-301 v1.1 Automation and Programmability questions of this type test whether each protocol, component, address type, or management concept is matched to its correct operating role. The safe method is to classify every item by function: what it does, where it operates, and what problem it solves.

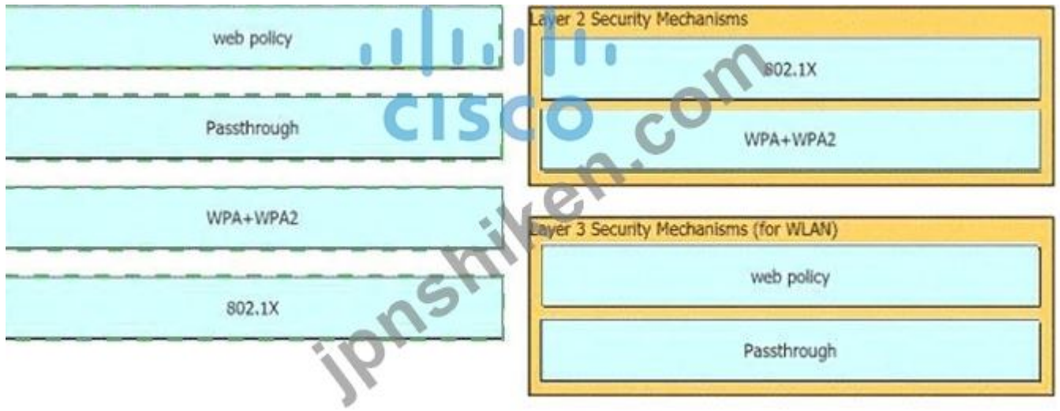
Several distractors are usually valid networking terms, but they belong to a different layer or a different operational workflow. The shown mapping keeps those boundaries straight and avoids assigning a feature to the wrong technology. In practice, this same skill is required when troubleshooting because confusing a management-plane function with a forwarding-plane function, or a wireless security feature with an authentication feature, leads to incorrect fixes. The mapping shown in the file is therefore retained and explained as the verified selection.



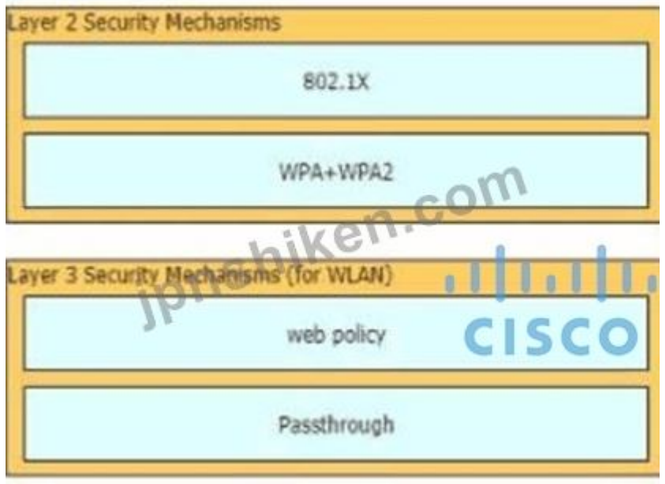
質問: 57

左側のCiscoワイヤレスLANコントローラのセキュリティ設定を、右側の適切なセキュリティメカニズムのカテゴリにドラッグアンドドロップしてください。

正解:



Explanation:
The verified answer is the displayed drag-and-drop mapping. Cisco WLC WLAN security settings map to Layer 2 security, Layer 3 security, and AAA-related mechanisms. Correct matching depends on separating authentication/encryption methods, web policy, and AAA server interaction. Cisco CCNA 200-301 v1.1 places this skill in Security Fundamentals, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. Mixing cipher settings with authentication servers is the usual error in this drag-and-drop item. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.



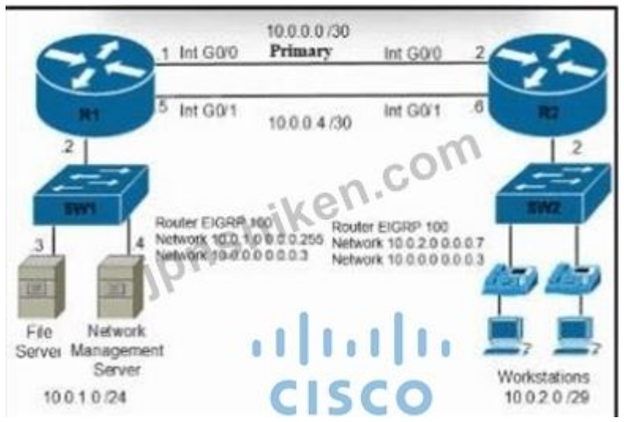
質問: **58**
Software-Defined Architecture で、Cisco ルーターを通過するトラフィックのスイッチングを処理するのはどこですか?
A. コントロール
B. 管理
C. データ
D. アプリケーション
正解: (正解を表示します)
The correct response is C. The data plane handles packet switching and forwarding through a router. It moves transit traffic from ingress to egress based on forwarding information produced by the control plane. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology.

The control plane builds routes, management handles administration, and application is not the router forwarding plane. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **59**
WPA3 に実装されている拡張機能はどれですか?
A. 802.1x 認証を適用
B. TKIP を使用
C. PKI を使用してアクセス ポイントを識別します。
D. ブルート フォース攻撃から保護します。
正解: **(**正解を表示します**)**
protects against brute force attacks. Wireless questions require separating client association, RF design, AP mode, WLAN security, and controller policy. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Incorrect answers usually confuse an encryption method with authentication, or a controller feature with a switchport feature. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **60**
シンプルな品質と可用性の組み合わせを提供する WAN トポロジはどれですか?
A. 部分メッシュ
B. フルメッシュ
C. ポイントツーポイント
D. ハブアンドスポーク
正解: **(**正解を表示します**)**
The verified answer is A. A partial-mesh WAN balances simplicity, link quality, and availability better than full mesh or pure hub-and-spoke. Critical sites can have direct redundant paths while less important sites avoid the cost and complexity of a full mesh. Cisco CCNA 200-301 v1.1 places this skill in Network Fundamentals, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. Point-to-point is simple but does not scale well, and hub-and-spoke can create a hub dependency. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **61**



図を参照してください。プライマリリンクが故障した場合に、ルーターR1からR2上のLANネットワークへトラフィックを転送するために、セカンダリルートが必要です。ルーターを設定するには、どのコマンドを入力する必要がありますか？

A. ip route 10.0.2.0 255.255.255.240 10.0.0.6 91

B. ip route 10.0.2.0 255.255.255.248 10.0.0.6 91

C. ip route 10.0.2.0 255.255.255.248 null0 93

D. ip route 10.0.2.0 255.255.255.240 10.0.0.7 92

正解: **(**正解を表示します**)**

ip route 10.0.2.0 255.255.255.248 10.0.0.6 91. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **62**

ある組織が新しいセキュリティポリシーを策定し、そのポリシーを印刷して全従業員に配布し、従業員がポリシーを確認して適用できるようにすることにしました。この組織は、セキュリティプログラムのどの要素を実施しているのでしょうか？

A. 資産識別

B. ユーザー研修

C. 物理的なアクセス制御

D. 脆弱性制御

正解: **(**正解を表示します**)**

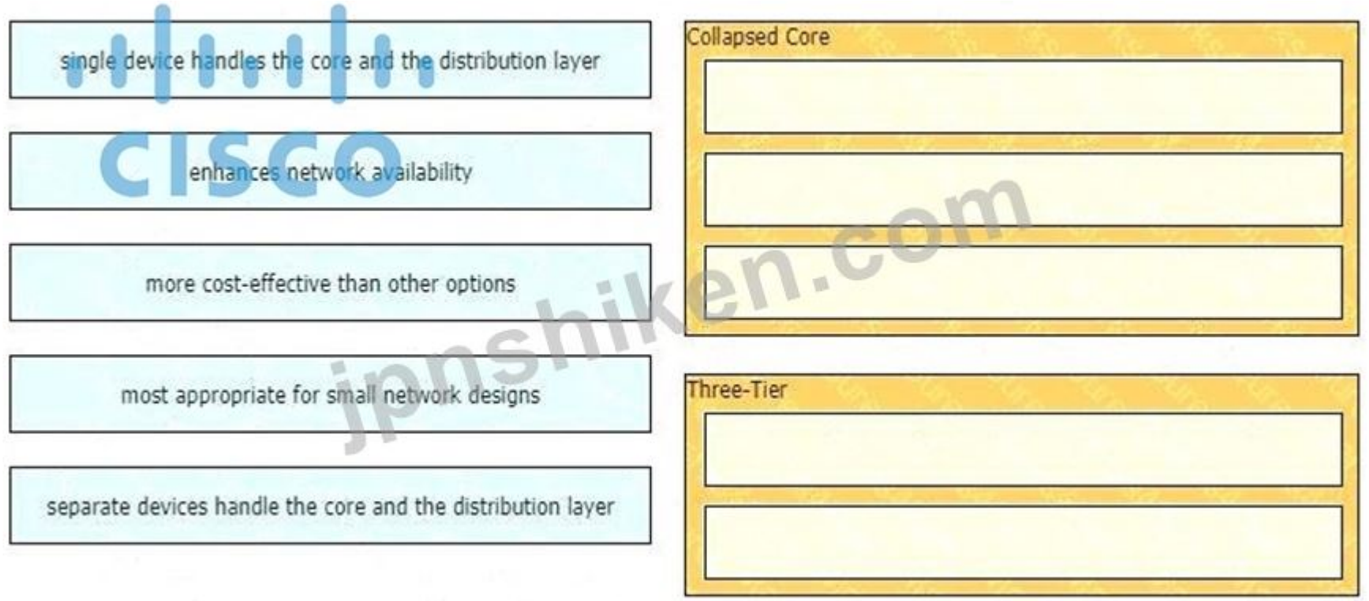
User training. Security questions in CCNA 200-301 v1.1 require matching the control to the threat or access requirement. Authentication proves identity, authorization controls what the user can do, and accounting records activity. Firewalls inspect and permit or deny traffic based on policy, while ACLs match packet fields in a defined order. VPN and IPsec questions require knowing whether the design protects unicast traffic, supports tunneling, or encrypts the original packet. Password and SSH questions depend on IOS behavior, including encrypted secrets, local users, domain names, and cryptographic images.

The incorrect choices often use a valid technology in the wrong role or provide weaker protection. The selected answer is the Cisco- consistent control because it directly satisfies the access, confidentiality, or threat-mitigation requirement stated in the question.

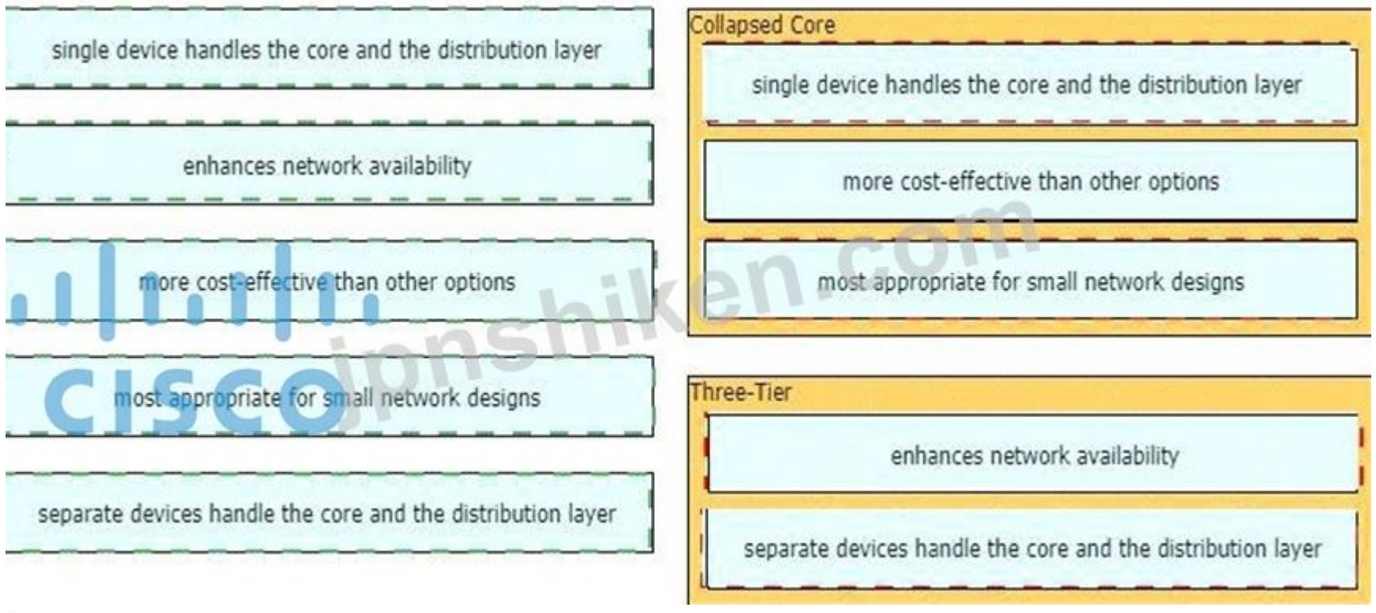
質問: **63**
JSON に関する正しい選択肢はどれですか?
A. 定義済みのタグまたは山かっこ () を使用して、マークアップ テキストを区切ります。
B. 配列を含む構造化データを記述するために使用されます
C. 情報の保存に使用
D. HTML に似ていますが、XML よりも詳細です。
正解: (正解を表示します)
JSON is commonly used to describe structured data and it supports arrays. A JSON object is written as name- value pairs enclosed in braces, while an array is an ordered list enclosed in brackets. This makes JSON compact and easy for REST APIs, scripts, controllers, and network automation tools to exchange data. Cisco CCNA 200-301 v1.1 includes JSON because network programmability often requires reading API responses from systems such as Cisco DNA Center or device controllers. Option A describes markup-style languages such as XML or HTML, which use angle brackets and tags. Option D is backwards because XML is usually more verbose than JSON. Option C is too vague; JSON can be stored, but the defining exam feature here is its structured representation, including arrays. A fast way to recognize JSON is to look for curly braces, quoted keys, colons between keys and values, and square brackets when multiple values are grouped.

質問: **64**
レイヤ2スイッチの特徴は何ですか？
A. アクティブなTCP接続数を追跡します
B. 半二重通信のみで送信します。
C. サーバーへのリンクバンドルを提供します
D. ルーターを使用して衝突ドメインを作成します
正解: (正解を表示します)
offers link bundling to servers. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First- hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **65**
左側のネットワークアーキテクチャの特徴を、右側のアーキテクチャの種類にドラッグ＆ドロップしてください。

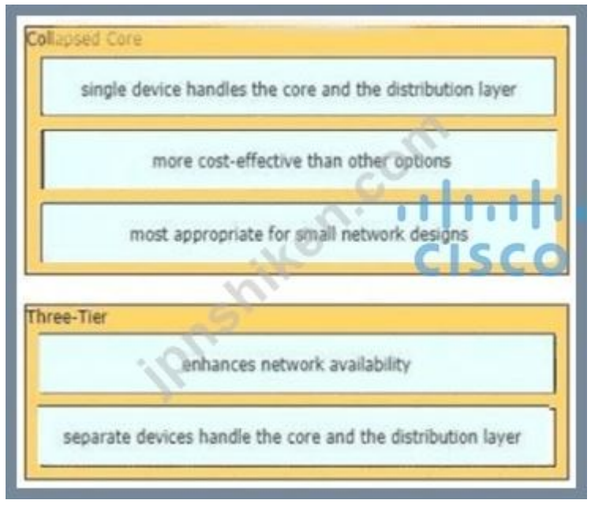


正解:

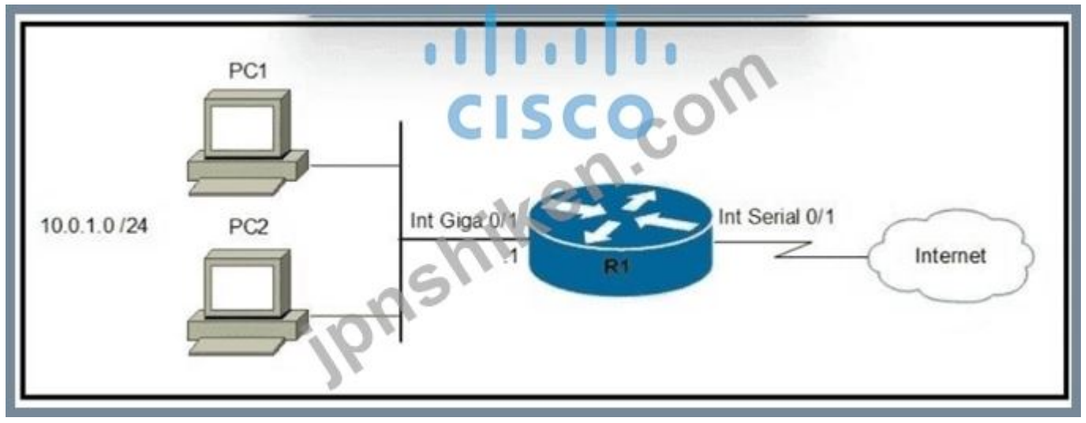


Explanation:

The correct response is the displayed drag-and-drop mapping. Network architecture characteristics distinguish two-tier, three-tier, spine-leaf, WAN, SOHO, and cloud designs. The correct mapping depends on where devices attach, where aggregation occurs, how redundancy is built, and whether the design optimizes campus access, data-center east-west traffic, or remote connectivity. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. The distractors normally mix access, distribution, core, and data-center terms, so matching function to layer is the safest method. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.



質問: **66**
ワークステーションがDHCPアドレスを取得できない原因は何ですか？
A. DTP
B. STP
C. VTP
D. 802.10
正解: **B (コメントを発表する)**
The verified answer is B. STP can temporarily prevent a workstation from receiving a DHCP address because the port may not forward immediately. Without PortFast, an access port can spend time in spanning-tree transitional states before forwarding DHCP traffic. Cisco CCNA 200-301 v1.1 places this skill in Network Access, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. DTP and VTP handle trunking and VLAN propagation, and 802.10 is not the cause in this access-port scenario. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **67**
展示資料を参照してください。


ルーターR1でセキュアなリモートアクセス接続を受け入れるようにするには、どの2つのコマンドを設定する必要がありますか？(2つ選択してください)

A. トランスポート入力telnet
B. 暗号鍵生成rsa
C. ip ssh pubkey-chain
D. ログインコンソール
E. ユーザー名 cisco パスワード 0 Cisco
正解: **(**正解を表示します**)**
Answer B,E is correct: B. crypto key generate rsa; E. username cisco password 0 Cisco. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question.
That is why it remains the verified answer for this item.

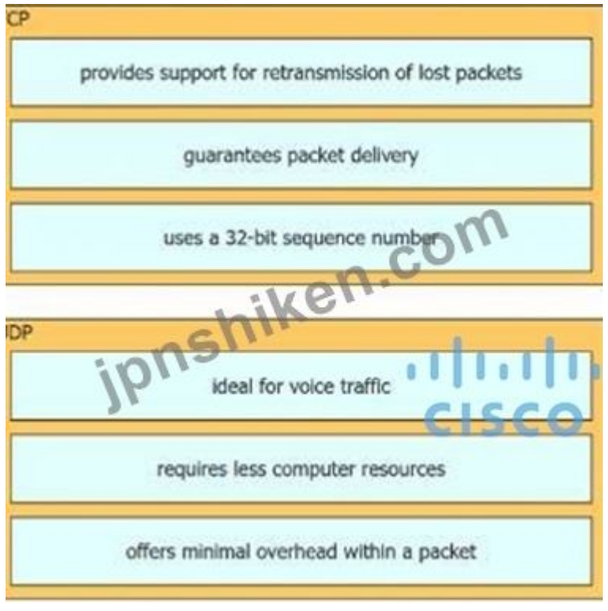
質問: **68**
サイト間 VPN が構成されている場合、元の IP パケット全体のカプセル化と暗号化を提供する IPsec モードはどれですか。
A. AHを使用したIPsecトンネルモード
B. AHを使用したIPsecトランスポートモード
C. ESPを使用したIPsecトンネルモード
D. ESPを使用したIPsecトランスポートモード
正解: **C (**コメントを発表する**)**
Answer C is the technically correct selection. IPsec tunnel mode with ESP encapsulates and encrypts the original IP packet for site-to-site VPN use. Tunnel mode wraps the entire inner packet with a new outer IP header, while ESP provides confidentiality and integrity protection for the protected payload. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. AH does not provide encryption, and transport mode protects only the transport payload rather than the whole original packet.
Treat the distractors carefully:
most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

質問: **69**
左側のトランスポート層プロトコルの特性を、右側の対応するプロトコルにドラッグアンドドロップしてください。

正解:

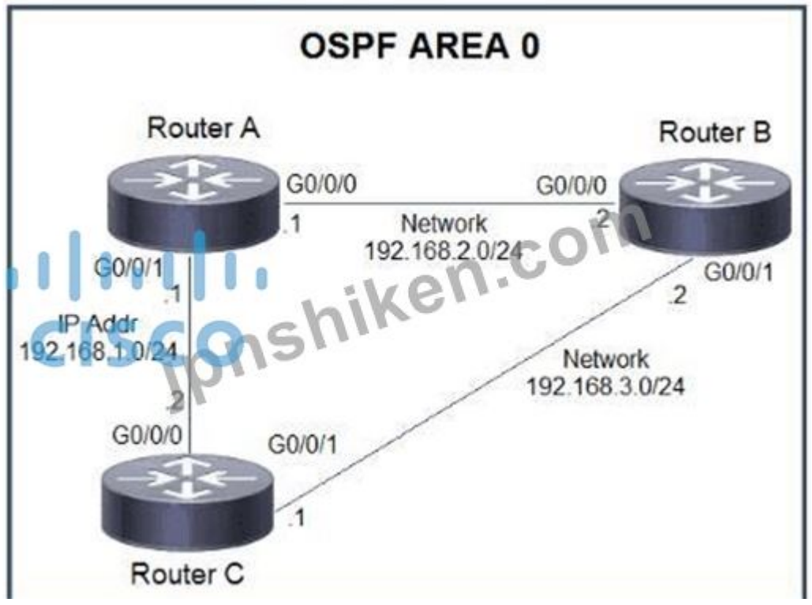
Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals drag-and-drop items test whether each protocol, address type, API action, or infrastructure component is matched to its real function. The correct way to solve these is to classify every item by layer, scope, and operational behavior before matching it. Several distractors are legitimate networking terms, but they are wrong when placed under the wrong protocol family or management model. The retained mapping preserves the Cisco distinctions between TCP and UDP behavior, AAA functions, IPv6 address scopes, device-management approaches, and REST operations. In implementation work, these distinctions matter because applying a feature at the wrong layer or associating a control with the wrong service creates broken configurations and wasted troubleshooting effort. The shown mapping is therefore retained as the verified response.



質問: 70

展示資料を参照してください。



ルーターAがOSPFエリア0のDRとして選出されるようにするには、どのような措置を講じる必要がありますか？

A. ルーター A のインターフェースを、エリア内で最も高い OSPF 優先度値に設定します。

B. ルーター B とルーター C をルーター A の OSPF ネイバーとして設定します。

C. 3台のルーターの中で最も低い値でルーターAのOSPF優先度を設定します。

D. ルーター A を固定 OSPF ルーター ID で設定します。

正解: **(**正解を表示します**)**

Configure the router A interfaces with the highest OSPF priority value within the area.. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default- gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **71**

SNMP トラップと SNMP ポーリングの違いは何ですか?

A. プロアクティブ監視には SNMP トラップが使用され、リアクティブ監視には SNMP ポーリングが使用されます。

B. SNMP トラップは MIB を介して定期的に更新を送信し、SNMP ポーリングは要求に応じてデータを送信します。

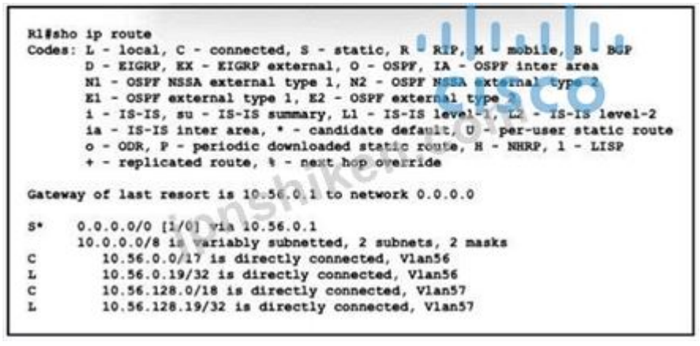
C. SNMP トラップはネットワーク管理システムによって開始され、ネットワーク デバイスは SNMP ポーリングを開始します。

D. SNMP トラップは、ネットワーク デバイスでプッシュ モデルを使用して開始され、SNMP ポーリングはサーバーで開始されます。

正解: **C (**コメントを発表する**)**

SNMP traps are initiated by the network management system, and network devices initiate SNMP polling.. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **72**
展示資料を参照してください。

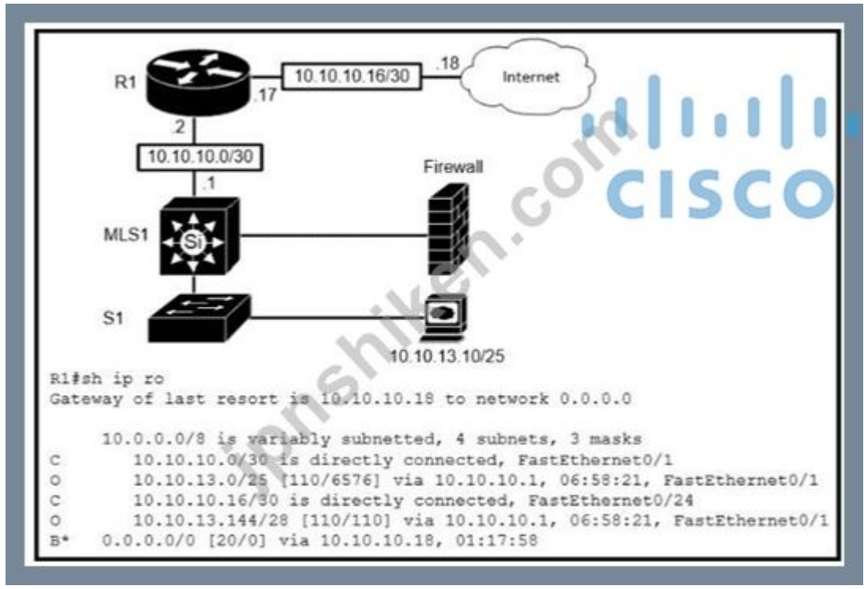


ルーターR1がIPアドレス10.56.192.1宛てにトラフィックを送信する場合、パケットのルーティングにはどのインターフェースまたはネクストホップアドレスが使用されますか？
A. 0.0.0.0/0
B. 10.56.0.1
C. 10.56.128.19
D. VLAN57
正解: (正解を表示します)
10.56.0.1. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **73**
スパイン・アンド・リーフ・アーキテクチャは、追加のアクセスポートが必要になった場合に、ネットワークのスケーラビリティをどのように実現するのでしょうか？
A. スパインスイッチとリーフスイッチが追加され、それらの間に冗長な接続があります。
B. 少なくとも40GBのアップリンクを備えたスパインスイッチが追加されます。
C. コアスパインスイッチに単一の接続でリーフスイッチが追加されます。
D. リーフスイッチが追加され、すべてのスパインスイッチに接続されます。
正解: (正解を表示します)
A leaf switch is added with connections to every spine switch.. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol:
LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **74**
スイッチでフレームフラッディングが発生する2つの理由は何ですか？(2つ選択してください。)

A. 不良パッチケーブルがスイッチポートに接続されています
B. スパニングツリー内でトポロジーの変更が発生しています
C. 古いMACテーブルエントリが原因で過剰な更新が発生しています
D. ポートセキュリティはグローバルに設定されています
E. 転送テーブルがオーバーフローしました
正解**: B,E (**コメントを発表する**)**
Answer B,E is correct: B. Topology changes are occurring within spanning-tree; E. The forwarding table has overflowed. A switch floods frames when it does not have a usable destination MAC entry. Spanning-tree topology changes can flush or age MAC table entries, forcing unknown-unicast flooding until the switch relearns addresses. A forwarding table overflow, including a CAM table overflow attack, also causes flooding because the switch cannot maintain complete MAC-to-port mappings. A defective patch cable usually causes physical errors, CRCs, or link instability, not ordinary frame flooding. Globally configured port security is not itself a flooding trigger. Cisco CCNA 200-301 v1.1 Network Access tests this because excessive flooding can look like a performance problem while the root cause is Layer 2 learning instability. The corrected choices are topology changes and forwarding-table overflow.

質問**: 75**
展示資料を参照してください。


R1はホスト10.10.13.10/32に到達するために、どのタイプのルートを使用しますか？
A. フローティングスタティックルート
B. ホストルート
C. デフォルトルート
D. ネットワークルート
正解**: (**正解を表示します**)**
R1 uses a network route, not a host route, floating static route, or default route. The destination host is
10.10.13.10/32, but the routing-table entry that matches it is the OSPF-learned network prefix 10.10.13.0/25.
That prefix covers host addresses from 10.10.13.1 through 10.10.13.126, so the host address is included. A host route would be a /32 entry specifically for 10.10.13.10. A default route would be 0.0.0.0/0 and would be used only if no more specific route matched. A floating static route is a backup static route with a higher administrative distance; the exhibit shows an OSPF route being selected. Cisco CCNA v1.1 IP

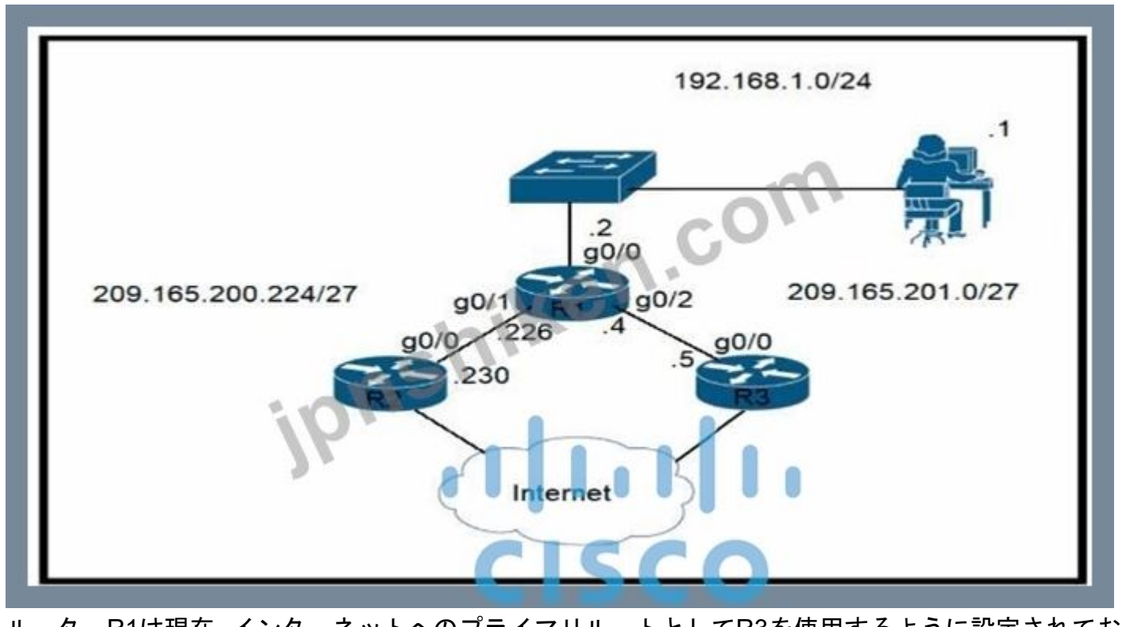
Connectivity emphasizes longest-prefix match and route-code interpretation. The router does not care that the destination is a single host; it forwards by the most specific matching route in the table. Here, that route is a network route.

質問: **76**
コントローラベースのアーキテクチャでエッジ デバイスとやり取りするために使用される API はどれですか?
A. オーバーレイ
B. 北行き
C. 下敷き
D. 南行き
正解: **(**正解を表示します**)**
In controller-based networking, the southbound API is the interface between the controller and the network devices it manages. The controller uses southbound communication to discover devices, collect operational data, push configuration, and influence forwarding behavior. Cisco CCNA 200-301 v1.1 separates this from northbound APIs, which are used by applications, orchestration tools, or business systems to communicate with the controller. The answer cannot be overlay or underlay because those terms describe logical and physical network transport designs, not API direction. Northbound is also wrong because it faces upward toward applications, not downward toward routers, switches, and access points. Common southbound technologies include NETCONF, RESTCONF, gNMI, and in SDN discussions, OpenFlow. The safest exam model is directional: northbound equals application-to-controller, while southbound equals controller-to- device. Since edge devices are the managed infrastructure, the API used to interact with them is southbound.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **77**
パケットをユニキャスト アドレスではなくマルチキャスト アドレスに転送する IPv6 アドレス ブロックはどれですか?
A. 2000::/3
B. FC00::/7
C. FE80::/10
D. FF00::/12
正解: **(**正解を表示します**)**
FF00::/12. IPv6 questions require identifying the address scope, address block, assignment method, and the role of multicast, link-local, unique-local, or global-unicast addressing. Cisco CCNA 200-301 v1.1 includes this topic under Network Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The wrong choices describe another IPv6 scope or an assignment process that does not match the address behavior in the prompt.
In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **78**
展示資料を参照してください。



ルーターR1は現在、インターネットへのプライマリルートとしてR3を使用するように設定されており、ルートはデフォルトの管理距離設定を使用しています。ネットワークエンジニアは、R3がダウンした場合にのみR2をバックアップとして使用するようにR1を設定する必要があります。R3へのリンクの管理距離設定を変更せずに、R2をバックアップルートとして正しく使用するようにするには、エンジニアはR1にどのコマンドを設定する必要がありますか？

A. ip route 0.0.0.0 0.0.0.0 g0/1 1
B. ip route 0.0.0.0 0.0.0.0 209.165.201.5 10
C. ip route 0.0.0.0 0.0.0.0 209.165.200.226 1
D. ip route 0,0.0.0 0.0.0.0 g0/1 6

正解: **B (**コメントを発表する**)**

ip route 0.0.0.0 0.0.0.0 209.165.201.5 10. A floating static route is installed only when its administrative distance is worse than the current primary route. R1 already uses R3 as the primary Internet path with the default administrative distance. To make R2 a backup, the new default route must point toward R2 and use a higher administrative distance, such as 10. A route with administrative distance 1 would compete directly with the primary static route and could replace or load-share instead of acting as a backup. Cisco CCNA 200-
301 v1.1 IP Connectivity requires engineers to recognize that the numeric value at the end of an ip route command is the administrative distance. In this scenario, the corrected route is the one using the R2 next hop and an administrative distance higher than the primary path. That makes the route a true fallback path rather than an equal primary route.

質問: **79**

Cisco DNA Centerのどの2つの機能が、従来のキャンパスデバイス管理と比較して拡張性を高めているのでしょうか？(2つ選択してください)

A. Cisco IOSソフトウェアのすべてのファミリーをサポートするアダプタ
B. サードパーティ製ネットワーク機器との連携をサポートするSDK
C. 中小企業および大企業向けにカスタマイズされたバージョン
D. 外部アプリケーションがCisco DNA Centerとネイティブに連携できるようにするREST API
E. 必要に応じてアップグレード可能なモジュール設計

正解: **B,D (**コメントを発表する**)**

Cisco DNA Center is more extensible than traditional device-by-device campus management because it exposes APIs and integration points. REST APIs allow external applications and automation systems to interact with Cisco DNA Center programmatically instead of relying only on manual GUI or CLI workflows.

SDKs extend the platform model by helping integrate third- party network devices and applications where supported. This is fundamentally different from logging into each switch with SSH and pasting commands.
Adapters that support every IOS family are not the central extensibility answer, and customized product versions by enterprise size are not what the question asks. Modular design may describe software architecture generally, but the explicit extensibility capabilities tested by Cisco are APIs, adapters, and SDKs. Cisco CCNA v1.1 Automation and Programmability includes controller-based networking, REST APIs, and Cisco DNA Center. The exam logic is direct: extensibility means outside systems can interact with and build on the controller platform. REST APIs and third-party SDK support provide that ability.

質問: **80**
一元化され、ルーティングの決定を管理するネットワーク プレーンはどれですか?
A. ポリシー プレーン
B. 管理プレーン
C. コントロール プレーン
D. データプレーン
正解: **C (**コメントを発表する**)**
control plane. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Automation and Programmability, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **81**

```
1  [
2  {"switch": "SW_admin", "interface": "ge7/41"},
3  {"VPN concentrator": "VPN_finance", "interface": "te0/5"},
4  {"IDS": "IPS_admin", "interface": "te2/10"},
5  ]
```

図を参照してください。このJSDNスキーマの2行目には何が示されていますか？
A. キー
B. 値
C. オブジェクト
D. 配列
正解: **(**正解を表示します**)**
object. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE. JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact with a controller, while southbound APIs allow the controller to communicate with network devices. NETCONF and RESTCONF are configuration
/management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to- device communication with application-to-controller communication or confuse a data format with a protocol.

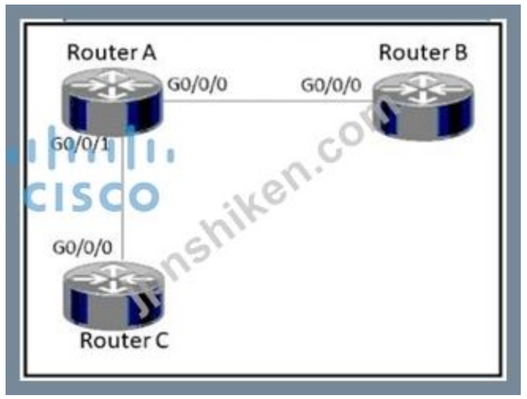
Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers. The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

質問: **82**
展示資料を参照してください。

```
access-list 101 permit ospf any any
 access-list 101 permit tcp any any eq 179
 access-list 101 permit tcp any eq 179 any
 access-list 101 permit gre any any
 access-list 101 permit esp any any

access-list 101 deny ospf any any
 access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet
 access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq 500
 access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq 4500
 access-list 101 deny ip any any log

interface Ethernet0/0
  ip address 10.1.1.25 255.255.255.0
  ip access-group 101 in
```

ネットワーク管理者は、ルーターへのVTYアクセスを保護するよう指示されました。この目的を達成するには、どのアクセスリストエントリを使用すればよいでしょうか？
A. アクセスリスト 101 permit tcp 10.1.10 0.0.0.255 172.16.10 0.0.0.255 eq ssh
B. access-list 101 permit tcp 10.11.0 0.0.0.255 172.16.10 0.0.0.255 eq scp
C. access-list 101 permit tcp 10.11.0 0.0.0.255 172.16.10 0.0.0.255 eq telnet
D. access-list 101 permit tcp 10.1.10 0.0.0.255 172.16.10 0.0.0.255 eq https
正解: **A (**コメントを発表する**)**
access-list 101 permit tcp 10.1.10 0.0.0.255 172.16.10 0.0.0.255 eq ssh. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control- plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **83**
展示資料を参照してください。



ルータAがCisco Discovery Protocol情報のみをルータCに送信するようにするには、どのように設定すればよいですか？

```
#config t
Router A (config)#cdp run
Router A (config)#interface gi0/0/0
Router A (config-if)#no cdp enable

#config t
Router A (config)#cdp run
Router A (config)#interface gi0/0/0
Router A (config-if)#cdp enable

#config t
Router A (config)#cdp run
Router A (config)#interface gi0/0/1
Router A (config-if)#cdp enable

#config t
Router A (config)#no cdp run
Router A (config)#interface gi0/0/1
Router A (config-if)#cdp enable
```

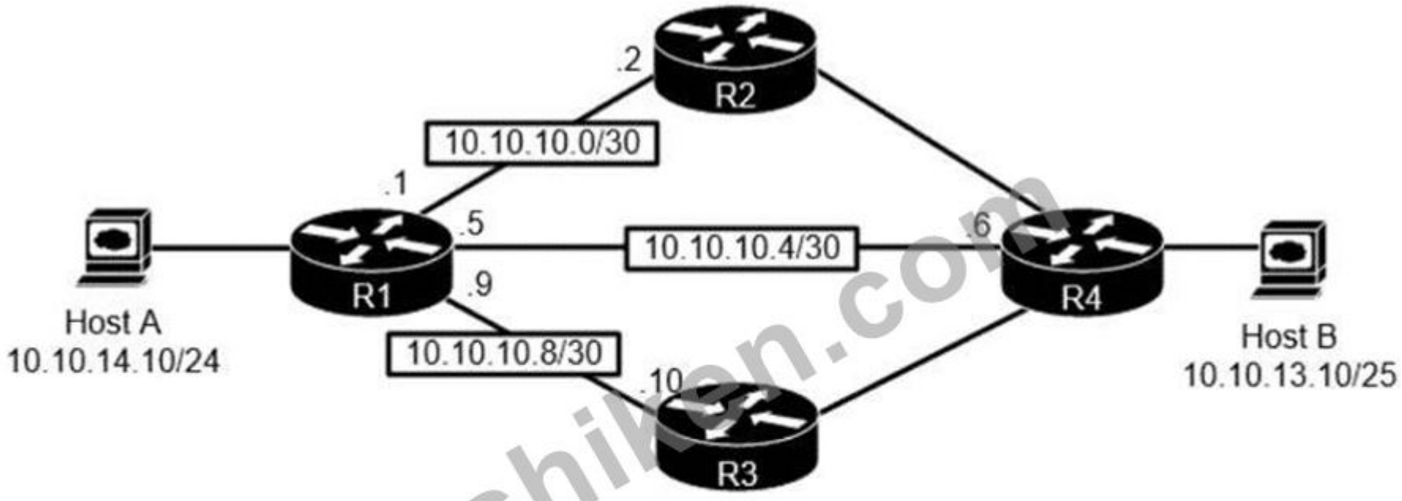
A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解: **D** (コメントを発表する)
The correct response is D. To send CDP information only toward Router C, CDP must remain enabled on the interface facing C and be disabled on the other relevant interfaces. CDP is a Cisco Layer 2 neighbor discovery protocol, so interface-level control determines which neighbors receive advertisements. For Cisco CCNA 200-
301 v1.1, the important point is the mechanism, not a generic description of the technology. A global shutdown would stop CDP everywhere, and clearing the table would not change future advertisements. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **84**
任意のインターフェースで LLDP を初期化するための遅延時間を秒単位で指定するために使用されるコマンドはどれですか?
A. lldpタイマー
B. LLDPホールドタイム
C. lldp の再初期化
D. lldp tlv-select
正解: (正解を表示します)
The lldp reinit command controls the delay before LLDP reinitializes on an interface. LLDP is a vendor- neutral neighbor discovery protocol, and Cisco IOS exposes several global LLDP timers. lldp timer sets how often LLDP advertisements are sent. lldp holdtime tells the receiving device how long to retain LLDP information before aging it out. lldp tlv-select controls which TLVs are included in advertisements. The

question specifically asks for the delay time in seconds for LLDP to initialize, which matches lldp reinit. The option labeled lldp holdtimt is also a typo and refers to the wrong function even if corrected to holdtime.
CCNA v1.1 Network Access includes Layer 2 discovery protocols such as CDP and LLDP. The exam often tests command intent rather than full configuration output. Here, the word initialize is the giveaway. Timer means advertisement interval; holdtime means neighbor retention; reinit means initialization delay.

質問: **85**
パケットを転送するかどうかを決定するために、アクティブな接続の状態を追跡するデバイスはどれですか?
A. 無線アクセスポイント
B. ファイアウォール
C. 無線LANコントローラー
D. ルーター
正解: **(**正解を表示します**)**
Answer B is the technically correct selection. A stateful firewall tracks active connection state and uses that state to permit or deny packets. Return traffic that belongs to an established connection can be allowed while unsolicited traffic can be blocked. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. Access points and WLCs handle wireless connectivity, and routers forward based on routing and policy rather than maintaining firewall session state by default. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

質問: **86**
展示資料を参照してください。




```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
R1(config)#ip route 10.10.13.0 255.255.255.128 10.10.10.2 111
R1(config)#ip route 10.10.13.0 255.255.255.128 10.10.10.6 112
R1(config)#ip route 10.10.13.0 255.255.255.128 10.10.10.10 108
R1(config-router)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 10.10.10.5 0.0.0.0 area 0
R1(config-router)#network 10.10.10.1 0.0.0.0 area 0
R1(config-router)#network 10.10.14.1 0.0.0.0 area 0
```

R1はホストAからホストB宛てのパケットを受信しました。R1がホストBに到達するために使用するルーティングテーブルのルートはどれですか？

A. 10.10.10.10 経由の 10.10.13.0/25 [108/0]

B. 10.10.10.2 経由の 10.10.13.0/25 [110/2]

C. 10.10.10.6 経由の 10.10.13.0/25 [110/2]

D. 10.10.10.2 経由の 10.10.13.0/25 [1/0]

正解: **D** (コメントを発表する)

10.10.13.0/25 [1/0] via 10.10.10.2. Routing questions are solved by applying longest-prefix match, administrative distance, metric, and protocol-specific behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function.

Wrong answers either use the wrong prefix, the wrong next hop, or a route source that would not be preferred.

In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **87**

ネットワーク管理者は、別のスイッチのポートへのレイヤー 2 接続をネゴシエートする必要がある単一の論理リンクに 4 つのポートを集約する必要があります。

接続の両側でアクティブ モードを使用する場合、何を設定する必要がありますか?

A. 802.1q トランク

B. Cisco vPC
C. LLDP
D. LACP
正解: (正解を表示します)
LACP. Switching features such as trunks and EtherChannels are controlled by negotiation mode, encapsulation, VLAN membership, and whether the selected protocol is Cisco proprietary or standards based. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces.
The incorrect options either disable negotiation, select the wrong negotiation protocol, or configure a mode that cannot form the requested link under the stated conditions. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **88**
スイッチにおけるMAC学習はどのように機能するのですか？
A. フレームをキューイングせずにすべてのポートにブロードキャストします。
B. 不明な送信元MACアドレスをアドレステーブルに追加します
C. 新しいフレームを受信したときに再送信要求を送信します
D. 宛先不明のフレームをマルチキャストグループに送信する
正解: (正解を表示します)
adds unknown source MAC addresses to the address table. Switching questions depend on MAC learning, VLAN membership, trunking, STP election, and EtherChannel behavior. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong answers misapply a Layer 2 rule or configure the wrong logical interface. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **89**
Ciscoのエンジニアが、工場出荷時のデフォルト設定のルーターに以下の3つのパスワードを設定しています。
* コンソールアクセス用のユーザーEXECパスワードはp4ssw0rd1です
* Telnetアクセス用のユーザーEXECパスワードはs3cr3t2です
特権EXECモードのパスワードはpr1v4t3p4ssです。エンジニアはどのコマンドシーケンスを設定する必要がありますか？
A.

```
enable secret priv4t3p4ss
!
line con 0
password login p4ssw0rd1
!
line vty 0 15
password login s3cr3t2
login
```

B.
```
enable secret privilege 15 priv4t3p4ss

line con 0
password p4ssw0rd1
login

line vty 0 15
password s3cr3t2
login
```

C.
```
enable secret priv4t3p4ss
!
line con 0
password p4ssw0rd1
login
!
line vty 0 15
password s3cr3t2
login
```

D.
```
enable secret priv4t3p4ss
!
line con 0
```

正解: **B** (コメントを発表する)

Option B. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **90**

左側のSNMPコンポーネントを右側の説明にドラッグアンドドロップしてください。

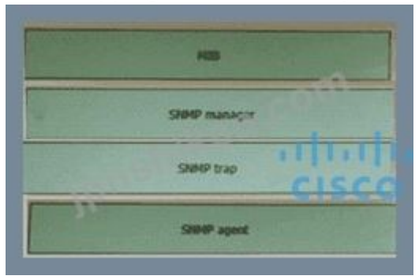
正解:

Explanation:

SNMP uses a manager-agent model. The SNMP manager, usually a network management system, polls devices or receives notifications. The SNMP agent runs on the managed device and exposes operational data.

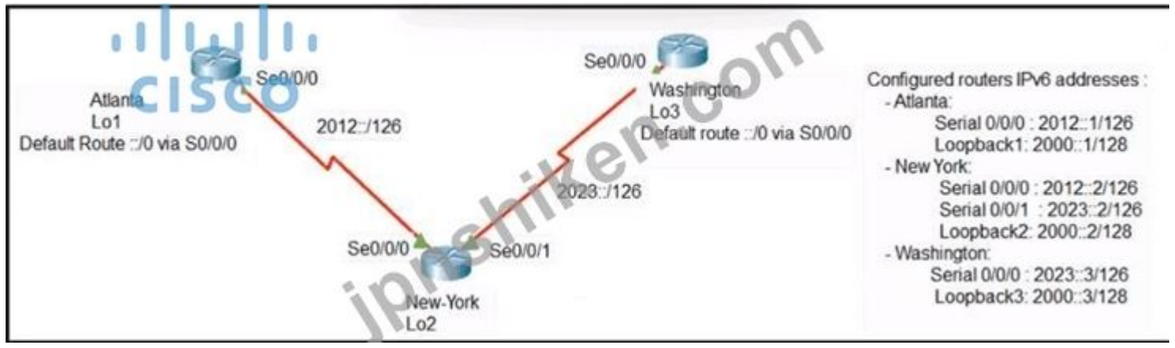
The Management Information Base is the structured database of managed objects, and object identifiers identify specific variables inside that hierarchy. Traps or informs are unsolicited notifications sent from the agent to the manager when configured events occur. Cisco CCNA 200-301 v1.1 IP Services includes SNMP because engineers use it for monitoring, inventory, alerting, and operational visibility. In drag-and-drop form, match each component to its role: manager equals monitoring system, agent equals device-side SNMP process, MIB equals object database, OID equals individual object path, and trap/inform equals notification.

That mapping is the stable way to solve the item regardless of the exact wording in the left column.



質問: **91**

展示資料を参照してください。



アトランタルーターのループバック1インターフェースは、ワシントンルーターのループバック3インターフェースに到達する必要があります。

A. ipv6 ルート 2000::1/128 2012::2

B. ipv6 ルート 2000::1/128 2012::1

C. ipv6 ルート 2000:3 123 s0/0/0

D. ipv6 ルート 2000::3/128 2023::3

E. ipv6 ルート 2000::1/128 s0/0/1

正解**: (**正解を表示します**)**

Answer B,D is correct: B. ipv6 route 2000::1/128 2012::1; D. ipv6 route 2000::3/128 2023::3. Routing questions are solved by applying longest-prefix match, administrative distance, metric, and protocol-specific behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Wrong answers either use the wrong prefix, the wrong next hop, or a route source that would not be preferred. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu 「**1813**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問**: 92**

ネットワーク エンジニアは、vlan 2000 インターフェイスに IPv6 構成を実装して、インターネットへのアドバタイズをブロックされたルーティング可能なローカルで一意のユニキャスト アドレスを作成する必要があります。

エンジニアはどの構成を適用する必要がありますか?

A. インターフェイス VLAN 2000

IPv6 アドレス ffc0:0000:aaaa::1234:2343/64

B. インターフェイス VLAN 2000

IPv6 アドレス fc00:0000:aaaa:a15d:1234:2343:8aca/64

C. インターフェイス VLAN 2000

IPv6 アドレス fe80:0000:aaaa::1234:2343/64

D. インターフェイス VLAN 2000

IPv6 アドレス fd00::1234:2343/64

正解: **(**正解を表示します**)**
interface VLAN 2000ipv6 address fc00:0000:aaaa:a15d:1234:2343:8aca/64. IPv6 questions depend on prefix scope, correct route syntax, and whether an address is link-local, unique local, multicast, or global unicast.
Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The wrong answers use an invalid scope, the wrong command family, or a prefix that does not meet the reachability requirement. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

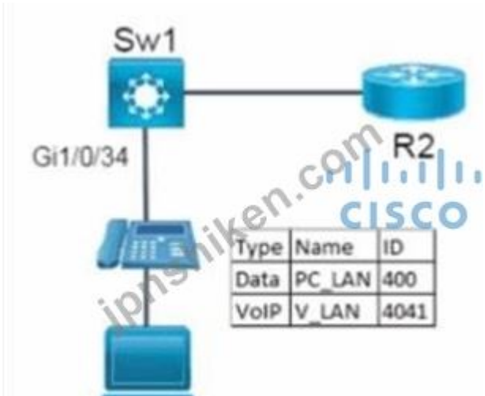
質問: **93**
NAT デバイスのパブリック IP アドレスはどのタイプのアドレスですか?
A. グローバル外
B. ローカル外
C. グローバル内部
D. ローカル内部
E. 外部公開
F. パブリック内
正解: **C (**コメントを発表する**)**
For NAT terminology, the public address that represents an inside host to the outside network is the inside global address. The inside local address is the private address configured on the internal device, commonly from RFC 1918 space. When traffic leaves the inside network, NAT changes the source from inside local to inside global so that the packet can be routed through the outside network. The outside global address is the real address of an external host, not the translated public address used by the inside device. Outside local describes how that external host may appear to the inside network. Cisco CCNA 200-301 v1.1 covers these NAT terms in IP Services because engineers must read translation tables correctly during troubleshooting.
The phrase public IP address of a NAT device is often imprecise, but in the context of a translated inside source, the Cisco term being tested is inside global. That is why C is the correct answer.

質問: **94**
WLCにおけるインバンド無線ネットワーク管理のデフォルトインターフェースは何ですか？
A. 冗長ポート
B. 帯域外
C. サービスポート
D. ワイヤレス管理
正解: **D (**コメントを発表する**)**
Wireless management. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **95**
802.11b/g/n/ax 2.4GHz周波数帯において、重複しないチャネルのグループはどれですか？
A. チャンネル1、5、10
B. チャンネル1、5、11

C. チャンネル1、6、10
D. チャンネル1、6、11
正解: **(**正解を表示します**)**
channels 1, 6, and 11. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **96**
展示資料を参照してください。



インターフェースGil/0734でネットワークサービスを有効にする必要があります。この実装の要件を満たす構成はどれですか？

A.
```
interface Gi1/0/34
switchport mode trunk
switchport
trunk allowed vlan 400, 4041
switchport voice vlan 4041
```

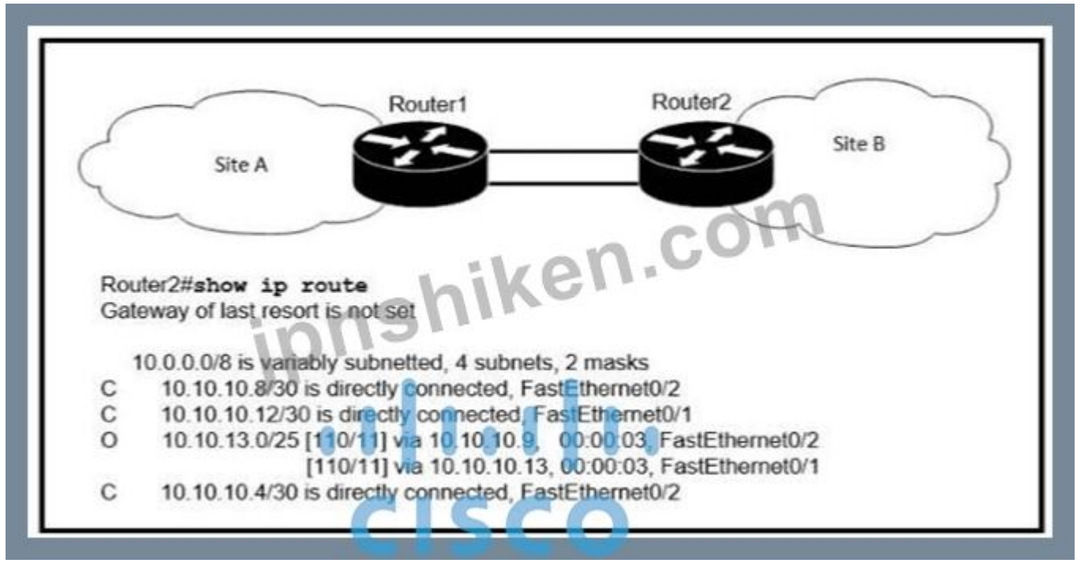
B.
```
interface Gi1/0/34
switchport mode trunk
switchport
trunk allowed native vlan 400
switchport
voice vlan 4041
```

C.
```
interface Gi1/0/34
switchport mode access
switchport
access vlan 4041
switchport voice vlan 400
```

D.
```
interface Gi1/0/34
switchport mode access
switchport
access vlan 400
switchport voice vlan 4041
```

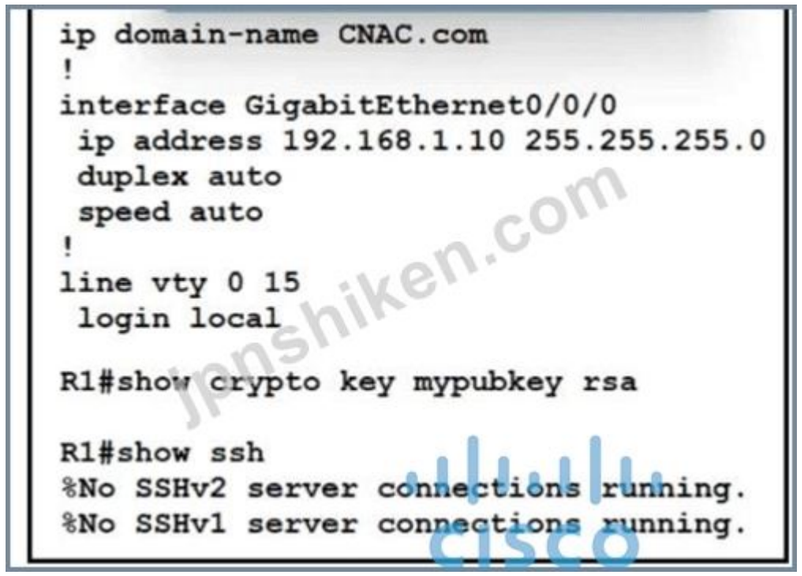
正解: **D** (コメントを発表する)
Option. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management.
A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **97**
展示資料を参照してください。



このネットワークでOSPFが動作している場合、ルーター2はサイトBからサイトAの10.10.13/25へのトラフィックをどのように処理しますか？
A. インターフェース Fa0/2 からのみパケットを送信します。
B. インターフェース Fa0/1 からのみパケットを送信します。
C. 10.10.13 128/25 にパケットを送信できません
D. Fa0/1とFa0/2からのトラフィックを負荷分散します。
正解: (正解を表示します)
The verified answer is C. Router 2 cannot forward to 10.10.13.128/25 if OSPF has only installed the
10.10.13.0/25 prefix. The 10.10.13.0/25 range ends at 10.10.13.127, so the .128/25 subnet is a different network. Cisco CCNA 200-301 v1.1 places this skill in IP Connectivity, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. OSPF cannot load-balance or choose an interface unless a matching route exists in the routing table. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **98**
展示資料を参照してください。



ルーターR1の設定を更新して、暗号化された接続のみを受け入れるようにするには、どの2つのコマンドを追加する必要がありますか？(2つ選択してください)

A. ユーザー名 CNAC シークレット R!41!4319115@

B. ip ssh バージョン 2

C. ライン vty 0 4

D. 暗号鍵生成 rsa 1024

E. トランスポート入力 ssh

正解: **D,E** (コメントを発表する)

Answer D,E is correct: D. crypto key generate rsa 1024; E. transport input ssh. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **99**

Cisco DNA Centerは、従来のキャンパスデバイス管理と比較してどのような利点がありますか？

A. クロスドメインアダプタやサードパーティSDKなど、多数の拡張オプションをサポートしています。

B. クラスタモードで動作する場合、管理機能の高可用性をサポートします。

C. ブラウンフィールド展開時にネットワーク要素の自動検出を容易にします。

D. 主にネットワークの信頼性を確保するために設計されています。

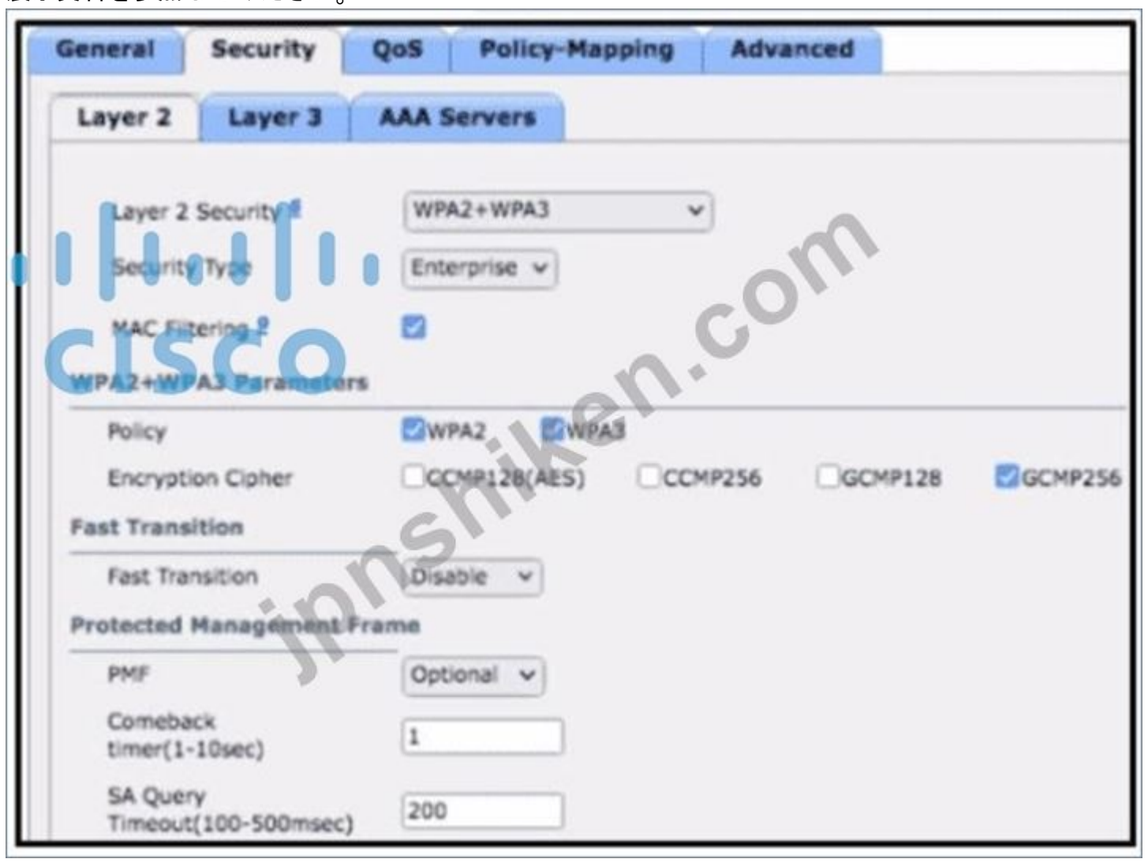
正解: **A** (コメントを発表する)

Cisco DNA Center is positioned as a controller and automation platform rather than a simple device-by- device management tool. One major advantage over traditional campus management is extensibility: APIs, integration adapters, and SDKs allow the platform to interact with other IT systems, network domains, and third-party equipment where supported. Cisco CCNA 200-301 v1.1 tests this under Automation and Programmability because controller-based management changes how networks are provisioned and operated.

High availability and assurance are valuable DNA Center capabilities, but the question asks for an advantage versus traditional campus device management, and extensibility is the answer that directly describes the platform shift. Autodiscovery can help onboarding, but it is not the broad differentiator stated in the answer set. Traditional management often means engineers manually configure individual

devices through CLI sessions or templates. DNA Center abstracts policy and exposes programmable interfaces, making operations more consistent and easier to integrate with external workflows. That is why A is correct.

質問: **100**
展示資料を参照してください。

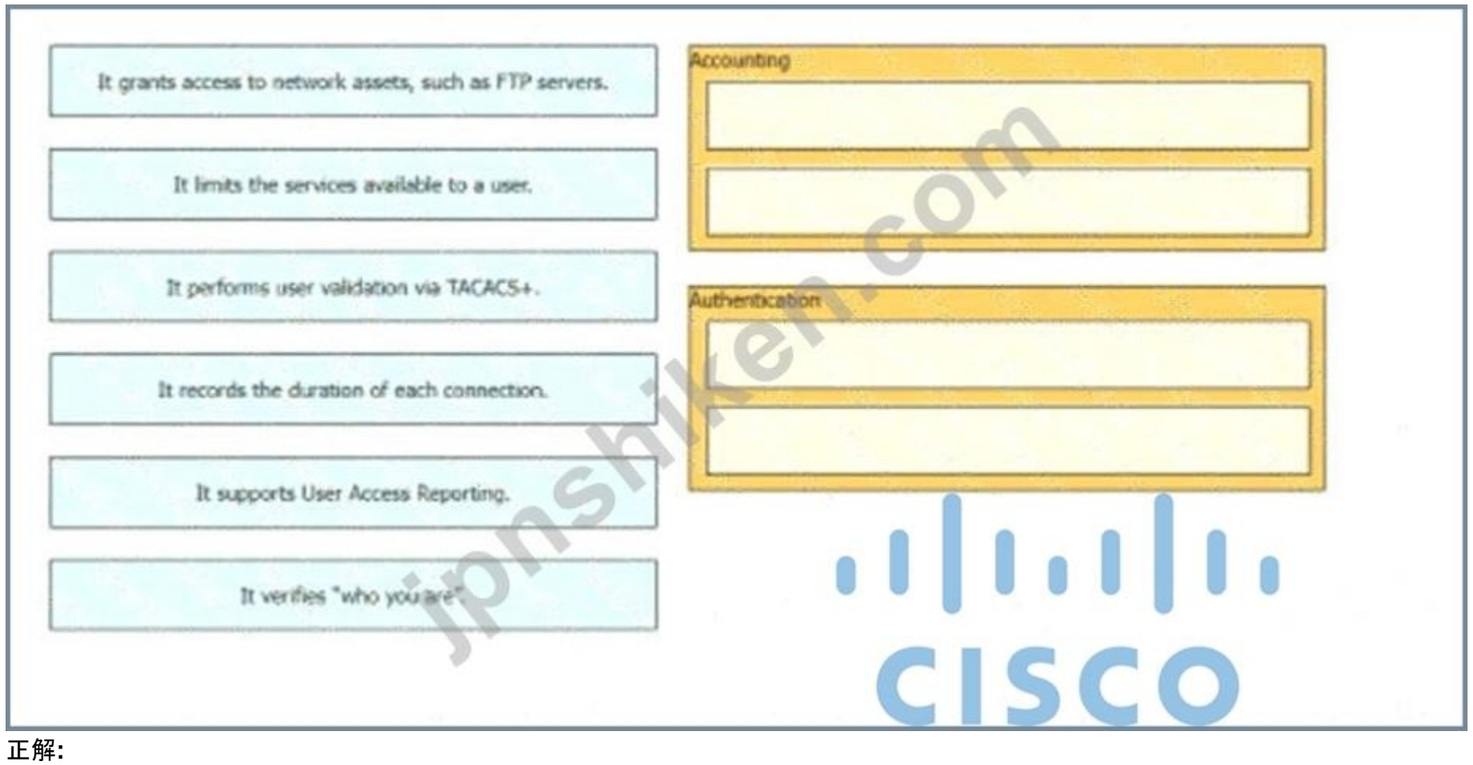


エンジニアは、新しい無線LANコントローラ上のすべてのWi-Fiサービスを文書化する必要があります。Wi-Fi SSID「Office_WLan」はレイヤ2セキュリティを備えています。この構成によって何が決定されますか？

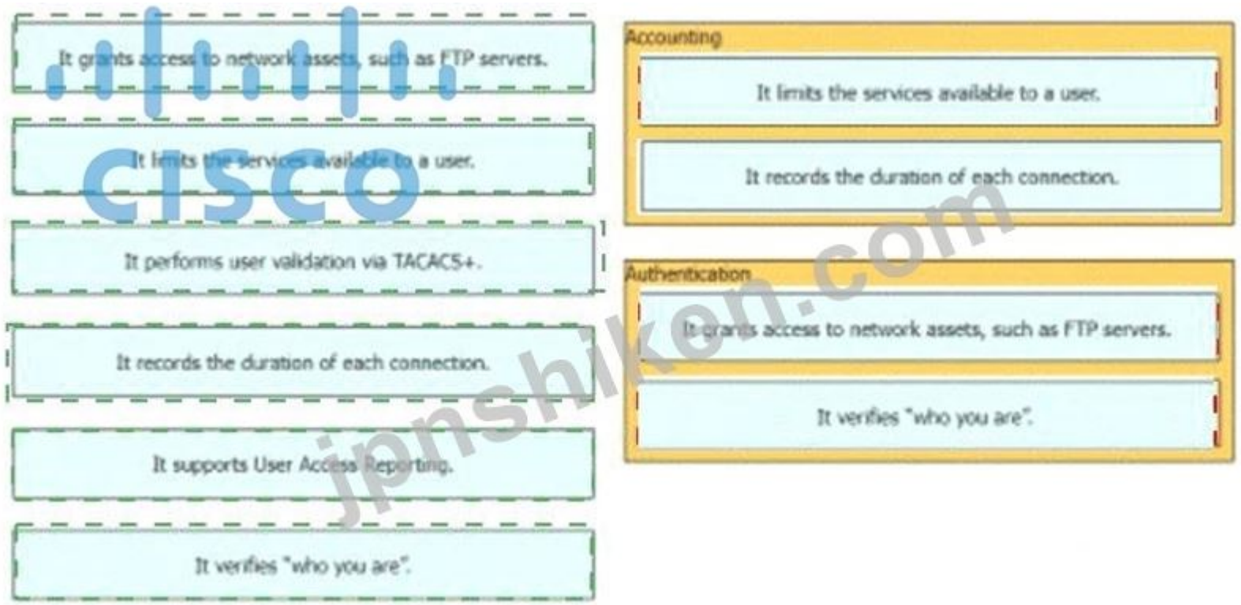
A. NACとネットワークデバイス間では、x.509規格を使用した強力な相互認証が行われます。
B. 既知のMACアドレスを持つ承認済みデバイスのみがネットワークに接続できるようにするための追加のセキュリティ層があります。
C. さまざまなレイヤー2およびレイヤー3攻撃から保護するように構成された堅牢なセキュリティメカニズムがあります。
D. 強力な暗号化と認証を提供するガロアキャッシュアルゴリズムが設定されています。
正解: **(**正解を表示します**)**
There is a robust security mechanism configured to protect against various Layer 2 and Layer 3 attacks..
Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **101**
ネットワークにおけるSNMPの役割は何ですか？
A. プレゼンテーション層で動作するTCPアンダーレイを使用してネットワークデバイスと機能を監視する
B. トランスポート層で動作するSSLアンダーレイを使用して、ネットワークデバイスから直接データを収集します。
C. アプリケーション層で動作するUDPアンダーレイを使用してネットワークデバイスを監視および管理する
D. ネットワーク層で動作するSSHアンダーレイを使用して、ネットワークデバイスからテレメトリと重要な情報を収集します。
正解: (正解を表示します)
to monitor and manage network devices using a UDP underlay that operates on the application layer. Security questions require separating secure protocols, insecure management, authentication, authorization, accounting, and threat-prevention controls. Cisco CCNA 200-301 v1.1 includes this under IP Services, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. The distractors either use weaker controls or protect a different part of the system.
In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco- consistent behavior for this item.

質問: **102**
左側のAAAサービスに関する記述を、右側の対応するAAAサービスにドラッグアンドドロップしてください。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:



Explanation:
Cisco CCNA 200-301 v1.1 Network Fundamentals drag-and-drop items test whether each protocol, address type, API action, or infrastructure component is matched to its real function. The correct way to solve these is to classify every item by layer, scope, and operational behavior before matching it. Several distractors are legitimate networking terms, but they are wrong when placed under the wrong protocol family or management model. The retained mapping preserves the Cisco distinctions between TCP and UDP behavior, AAA functions, IPv6 address scopes, device-management approaches, and REST operations. In implementation work, these distinctions matter because applying a feature at the wrong layer or associating a control with the wrong service creates broken configurations and wasted troubleshooting effort. The shown mapping is therefore retained as the verified response.

質問: **103**
エンジニアは、Cisco スイッチとサードパーティ製スイッチの間のスイッチ間 VLAN 通信を構成する必要があります。どのアクションを実行する必要がありますか?
A. IEEE 802.1p を構成する
B. IEEE 802.1q を構成する
C. ISL の構成
D. DSCP を構成する
正解: **(**正解を表示します**)**
When configuring VLAN trunking between a Cisco switch and a third-party switch, use IEEE 802.1Q. It is the open standard for VLAN tagging on Ethernet trunks. Cisco ISL was Cisco-proprietary and is obsolete on modern platforms. IEEE 802.1p relates to Class of Service marking inside the Ethernet header, not trunk encapsulation for interswitch VLAN transport. DSCP is an IP-layer QoS marking, not a Layer 2 VLAN trunking method. Cisco CCNA 200-301 v1.1 Network Access expects candidates to know that 802.1Q inserts a VLAN tag so multiple VLANs can traverse one physical trunk link. The native VLAN is carried untagged by default, while other VLANs are tagged. In multivendor networks, standards-based encapsulation is mandatory. Therefore, the action is to configure IEEE 802.1Q. The correct answer is B.

質問: **104**
次世代IPSの機能とは何ですか？
A. RADIUSサーバーと統合して、レイヤー2デバイス認証ルールを適用します。
B. コントローラベースのネットワーク内でコントローラとして機能する

C. 学習したMACアドレスに基づいて転送決定を行います
D. ユーザーアクティビティとネットワークイベントを関連付けます
正解: **(**正解を表示します**)**
Correlates user activity with network events. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity.
The selected answer matches Cisco switching operation.

質問: **105**
ネットワーク エンジニアは、顧客環境内で 20 のネットワーク ルーター構成をグローバルにバックアップする必要があります。
エンジニアが Cisco IOS MIB を使用してこの機能を実行できるプロトコルはどれですか?
A. CDP
B. SNMP
C. SMTP
D. ARP
正解: **(**正解を表示します**)**
SNMP is the protocol associated with IOS MIB access and centralized network management. The Management Information Base is the structured set of managed objects that an SNMP manager can query or, where permitted, modify on an SNMP agent. In the context of backing up many router configurations globally, SNMP can be used by management software to interact with Cisco IOS MIB objects and trigger configuration-copy operations. CDP discovers directly connected Cisco neighbors; it is not a configuration backup protocol. SMTP is for mail transfer. ARP resolves IPv4 addresses to MAC addresses on a local segment. Cisco CCNA v1.1 IP Services includes device management protocols such as SNMP, syslog, and NTP. The important distinction is scope: SNMP gives a management station structured visibility and control through MIB objects across many devices. That is why the Cisco IOS MIB clue points directly to SNMP.

質問: **106**
新しい多要素認証ソリューションを導入する際に、どの方法の組み合わせが最低限のセキュリティ要件を満たすでしょうか？
A. 8〜15文字のパスワードと12桁の個人用PIN
B. 認証済みUSBドングルと携帯電話
C. 指紋スキャンと顔認識
D. 複雑なパスワードと時間ベースのワンタイムパスワード
正解: **D (**コメントを発表する**)**
complex password and time-based one-time password. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **107**
どのデバイスがセキュリティドメインごとにネットワークを分離しますか？
A. ファイアウォール
B. アクセスポイント
C. 侵入防御システム
D. ワイヤレスコントローラー
正解: **(**正解を表示します**)**
firewall. Wireless questions depend on AP mode, WLAN security, RF band selection, controller interfaces, and client roaming or authentication behavior. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong options confuse encryption with authentication, local switching with tunneling, or controller management with client data handling. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **108**
左側の特性を右側のIPv6アドレスタイプにドラッグアンドドロップしてください。

provides one-to-many communications

has a unicast source sent to a group

enables aggregation of routing prefixes

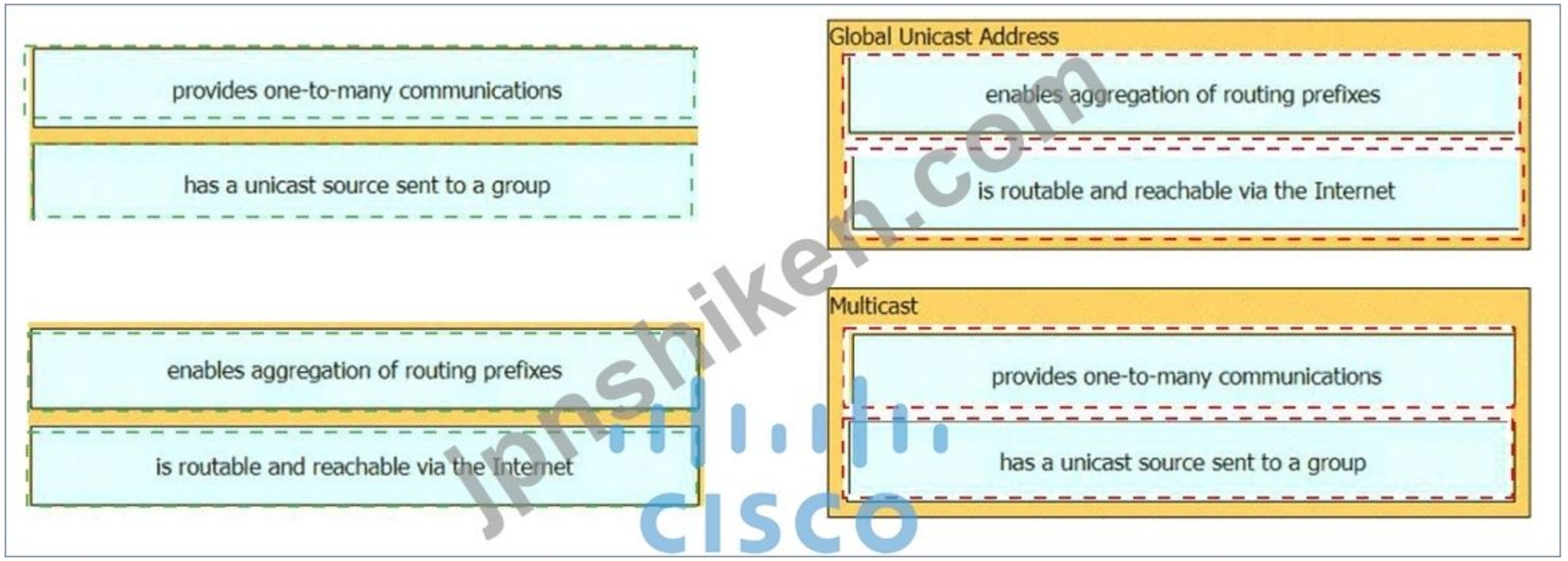
is routable and reachable via the Internet

Global Unicast Address

Multicast

jpnshiken.com

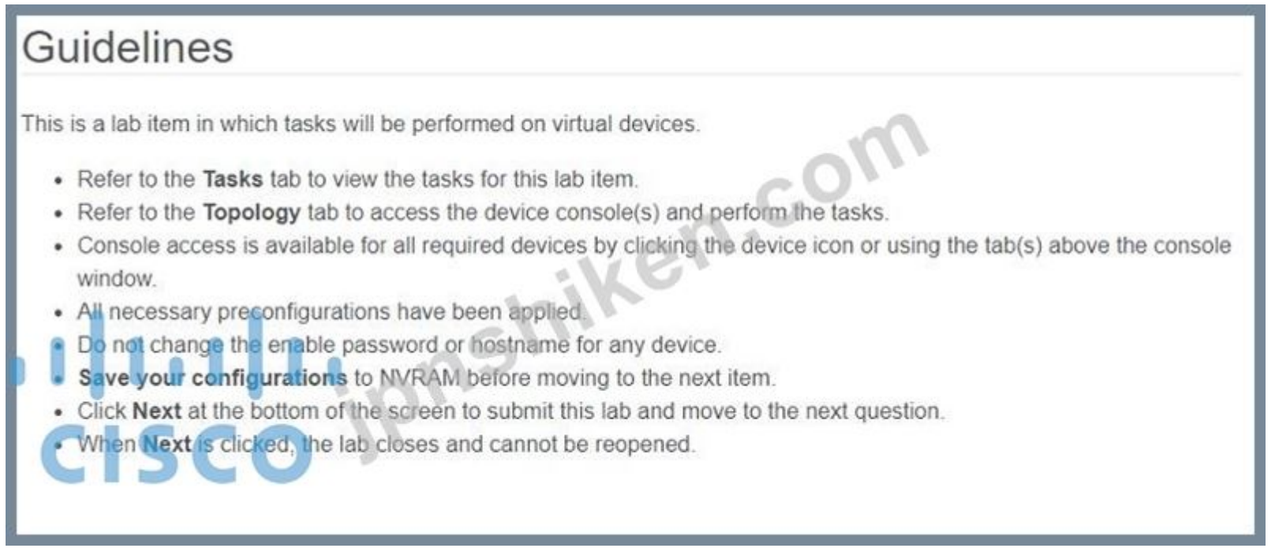
正解:



Explanation:
Cisco CCNA 200-301 v1.1 Network Fundamentals drag-and-drop items test whether each protocol, address type, API action, or infrastructure component is matched to its real function. The correct way to solve these is to classify every item by layer, scope, and operational behavior before matching it. Several distractors are legitimate networking terms, but they are wrong when placed under the wrong protocol family or management model. The retained mapping preserves the Cisco distinctions between TCP and UDP behavior, AAA functions, IPv6 address scopes, device-management approaches, and REST operations. In implementation work, these distinctions matter because applying a feature at the wrong layer or associating a control with the wrong service creates broken configurations and wasted troubleshooting effort. The shown mapping is therefore retained as the verified response.

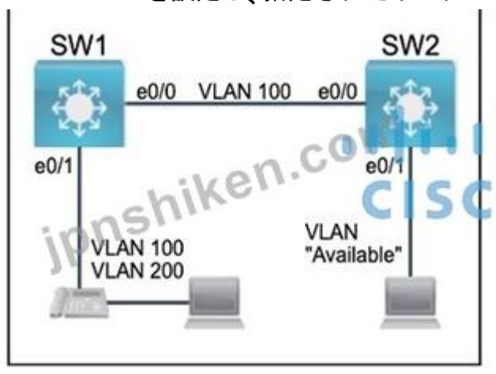
質問: **109**
社内セキュリティチームは、フィッシング攻撃の被害に遭う従業員が増加していることに気づきました。この問題を軽減するために、どのようなセキュリティプログラムを導入すべきでしょうか？
A. メールシステムのパッチ
B. 物理的なアクセス制御
C. すべてのPCでソフトウェアファイアウォールが有効になっています
D. ユーザー意識向上トレーニング
正解: **D** (コメントを発表する)
user awareness training. Security questions in CCNA 200-301 v1.1 require matching the control to the threat or access requirement. Authentication proves identity, authorization controls what the user can do, and accounting records activity. Firewalls inspect and permit or deny traffic based on policy, while ACLs match packet fields in a defined order. VPN and IPsec questions require knowing whether the design protects unicast traffic, supports tunneling, or encrypts the original packet. Password and SSH questions depend on IOS behavior, including encrypted secrets, local users, domain names, and cryptographic images. The incorrect choices often use a valid technology in the wrong role or provide weaker protection. The selected answer is the Cisco-consistent control because it directly satisfies the access, confidentiality, or threat-mitigation requirement stated in the question.

質問: **110**



2台のスイッチ間の物理的なケーブル配線はすべて完了しています。指定されたVLANとインターフェースを使用して、スイッチ間のネットワーク接続を設定してください。

1. 各タスクに必要な場所に、Computeという名前のVLAN 100とTelephonyという名前のVLAN 200を設定します。
2. SW2 の Ethernet0/1 を、Available という名前の既存の VLAN を使用するように設定します。
3. アクセスポートを使用してスイッチ間の接続を設定します。
4. SW1のEthernet0/1をデータVLANと音声VLANを使用して設定します。
5. SW2 の Ethemet0/1 を設定し、指定されたインターフェイスのみで Cisco 独自のネイバー検出プロトコルが無効になるようにします。



正解:

See the Explanation below.

Explanation:

Answer as below configuration:

on sw1

enable

conf t

vlan 100

name Compute

vlan 200

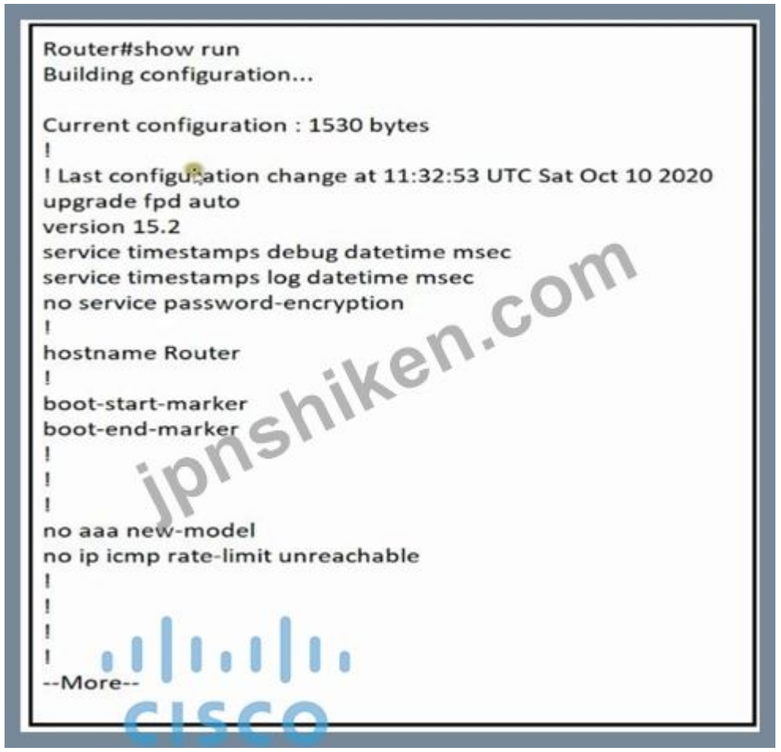
name Telephony
int e0/1
switchport voice vlan 200
switchport access vlan 100
int e0/0
switchport mode access
do wr
on sw2
Vlan 99
Name Available
Int e0/1
Switchport access vlan 99
do wr

質問: **111**
TCPとUDPは、クエリ・レスポンスモデルにどのように適合するのでしょうか？
A. TCPはデータ送信前に接続を確立し、UDPは即座に送信します。
B. TCPはパケットのエラー検出を使用し、UDPはエラー回復を使用します。
C. TCPはシーケンス処理を回避し、UDPは確認応答を回避します。
D. TCPはパケットの順不同配信を推奨し、UDPは順序変更を禁止します。
正解: (正解を表示します)
TCP establishes a connection prior to sending data, and UDP sends immediately.. The answer follows from standard Cisco behavior and the operational clue in the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The other choices describe related terms, but they do not satisfy the requirement stated in the prompt. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **112**
ネットワーク設計者は、どのような状況で、固有のローカルユニキャストサブネットではなく、グローバルユニキャストサブネットを実装することを決定するのでしょうか？
A. サブネットが組織内でのみ利用可能である必要がある場合
B. サブネットがルーティング可能である必要がない場合
C. サブネット上のアドレスがプライベート IPv4 アドレスと等価でなければならない場合
D. サブネットがインターネット経由でルーティング可能である必要がある場合
正解: (正解を表示します)
when the subnet must be routable over the internet. Network fundamentals questions require careful attention to address scope, media type, cabling limits, topology design, virtualization, cloud service models, and the difference between TCP and UDP. The CCNA 200-301 v1.1 blueprint expects candidates to identify not only definitions but also the operational consequence of each choice. For example, public and private addressing have different routing behavior; fiber and copper use different physical media; TCP and UDP make different reliability tradeoffs; and virtualization abstracts physical resources through a hypervisor. The wrong answers are usually plausible terms from the same area, but they do not match the exact condition described in the question. The selected answer is correct because it is the only option that fits the stated network behavior, design requirement, or physical/logical property. That is the level of precision needed for Cisco troubleshooting and implementation work.

質問: **113**

展示資料を参照してください。



R15へのセキュアシェルバージョン2アクセスを有効にするために必要な最小限の構成項目は何ですか？

A.
```
Router(config)#hostname R15
R15(config)#crypto key generate rsa general-keys modulus 1024
R15(config-line)#line vty 0 15
R15(config-line)# transport input ssh
R15(config)#ip ssh source-interface Fa0/0
R15(config)#ip ssh stricthostkeycheck
```

B.
```
Router(config)#crypto key generate rsa general-keys modulus 1024
Router(config)#ip ssh version 2
Router(config-line)#line vty 0 15
Router(config-line)# transport input ssh
Router(config)#ip ssh logging events
R15(config)#ip ssh stricthostkeycheck
```

C.
```
Router(config)#ip domain-name cisco.com
Router(config)#crypto key generate rsa general-keys modulus 1024
Router(config)#ip ssh version 2
Router(config-line)#line vty 0 15
Router(config-line)# transport input all
Router(config)#ip ssh logging events
```

D.
```
Router(config)#hostname R15
R15(config)#ip domain-name cisco.com
R15(config)#crypto key generate rsa general-keys modulus 1024
R15(config)#ip ssh version 2
R15(config-line)#line vty 0 15
R15(config-line)# transport input ssh
```

正解: **(**正解を表示します**)**

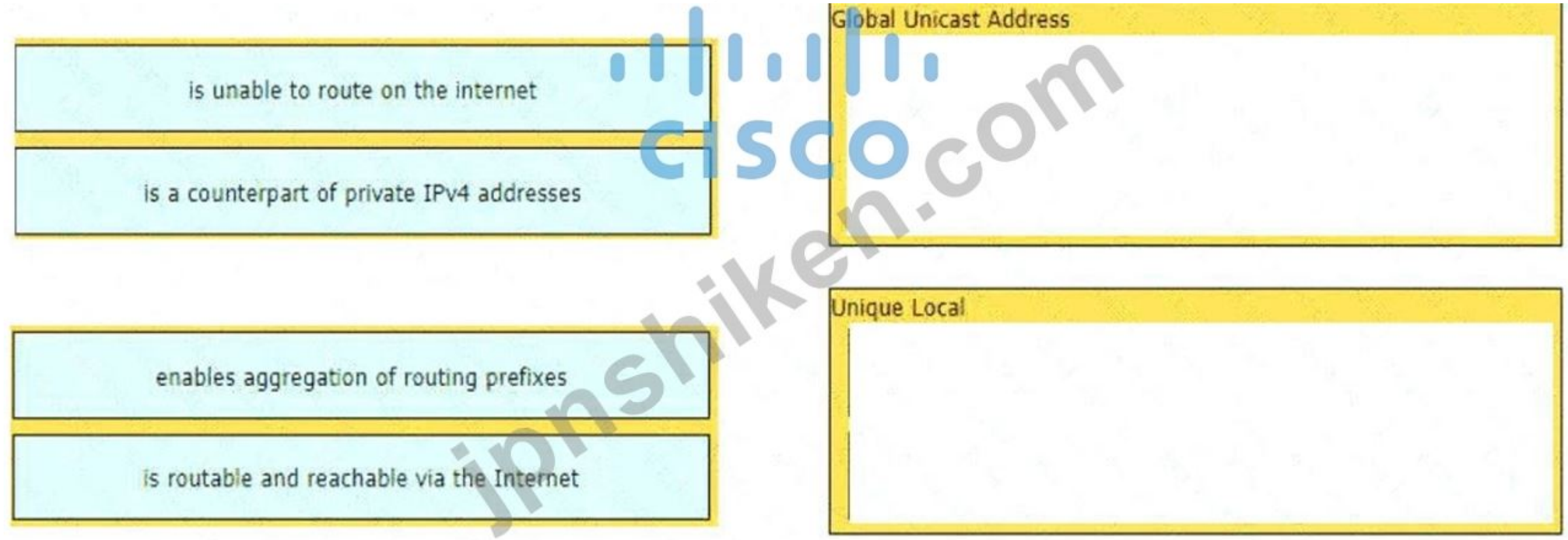
Option C. The answer follows from normal Cisco device behavior and the operating clue in the scenario.

Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The other options use adjacent terms, wrong-layer behavior, or configuration that would not

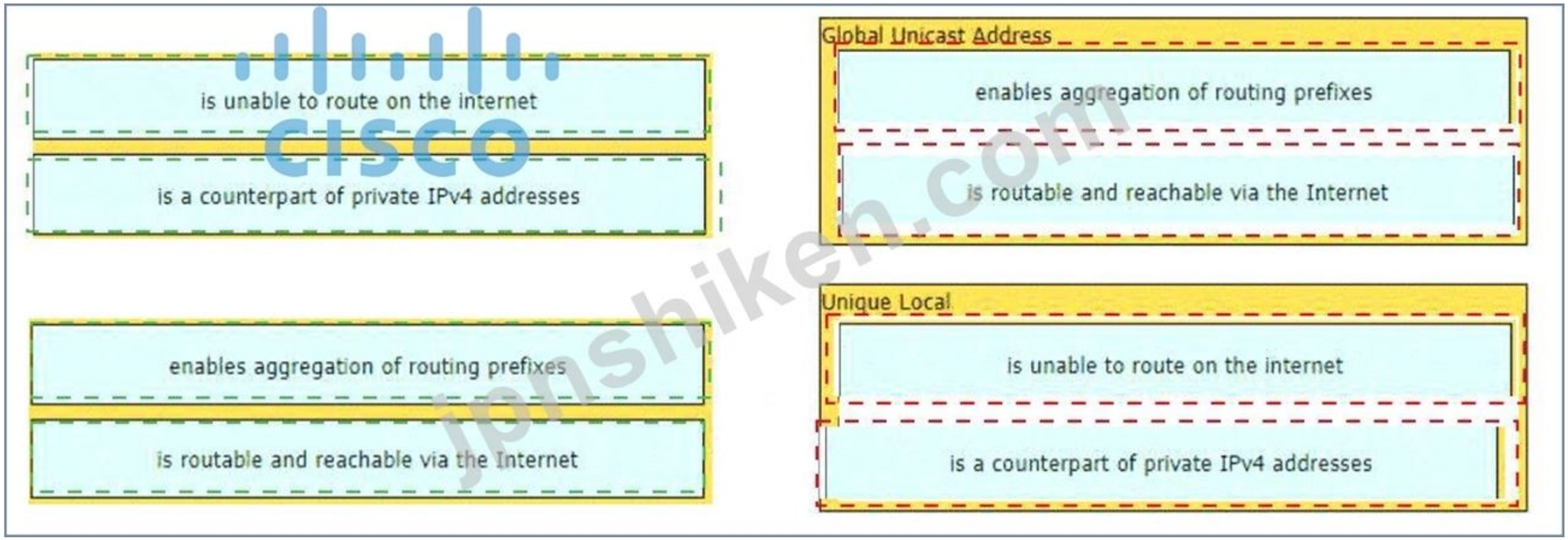
produce the requested result. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **114**
新しいネットワークにsyslogを実装する際に、エンジニアはどの事実を考慮しなければならないか？
A. Syslogは、メッセージをトリガーしたソフトウェアまたはハードウェアコンポーネントを定義します。
B. ログレベルは16段階あります(0〜15)。
C. デフォルトでは、すべてのメッセージレベルが syslog サーバーに送信されます。
D. ログレベルは、特定のメッセージの重大度を定義します。
正解: (正解を表示します)
The logging level defines the severity of a particular message.. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **115**
左側の特性を右側のIPv6アドレスタイプにドラッグアンドドロップしてください。

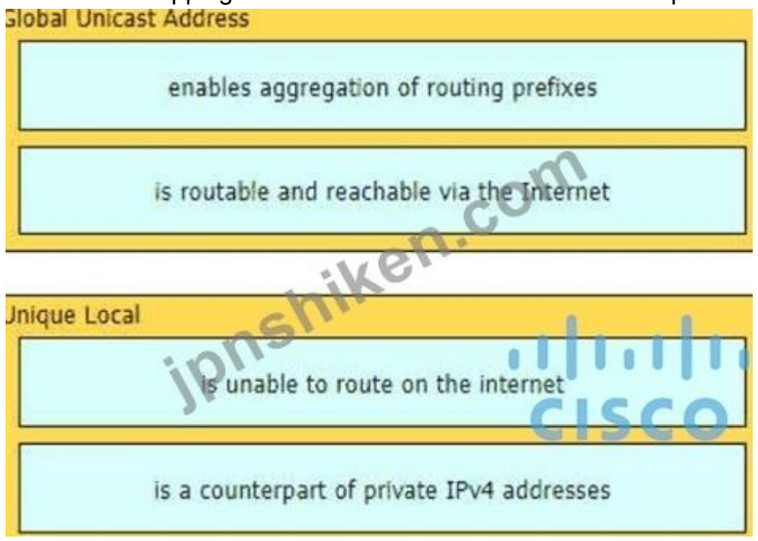


正解:



Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals drag-and-drop items test whether each protocol, address type, API action, or infrastructure component is matched to its real function. The correct way to solve these is to classify every item by layer, scope, and operational behavior before matching it. Several distractors are legitimate networking terms, but they are wrong when placed under the wrong protocol family or management model. The retained mapping preserves the Cisco distinctions between TCP and UDP behavior, AAA functions, IPv6 address scopes, device-management approaches, and REST operations. In implementation work, these distinctions matter because applying a feature at the wrong layer or associating a control with the wrong service creates broken configurations and wasted troubleshooting effort. The shown mapping is therefore retained as the verified response.



質問: 116

この出力では、どのインターフェース条件が発生していますか？

A. デュプレックスミスマッチ

B. NICに問題あり

C. 高スループット

D. ブロードキャストストーム

正解: **(**正解を表示します**)**

high throughput. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

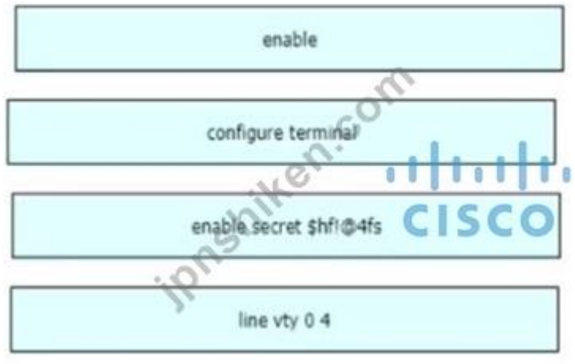
質問: **117**

エンジニアが、ローカルユーザーデータベースが既に設定されているルーターのenableコマンドに暗号化されたパスワードを設定しています。左側の設定コマンドを右側の正しい順序にドラッグアンドドロップしてください。すべてのコマンドが使用されるわけではありません。

正解:

Explanation:

Answer the displayed drag-and-drop sequence is the technically correct selection. The secure enable configuration sequence enters privileged configuration mode and sets an encrypted enable secret. When a local user database already exists, the remaining task is to configure privileged access securely rather than store a plaintext enable password. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. enable password is weaker than enable secret, and line-password steps do not create the encrypted enable credential. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.



質問: **118**

データ プレーン内で発生するネットワーク アクションはどれですか?

A. 宛先 IP アドレスを IP ルーティング テーブルと比較します。

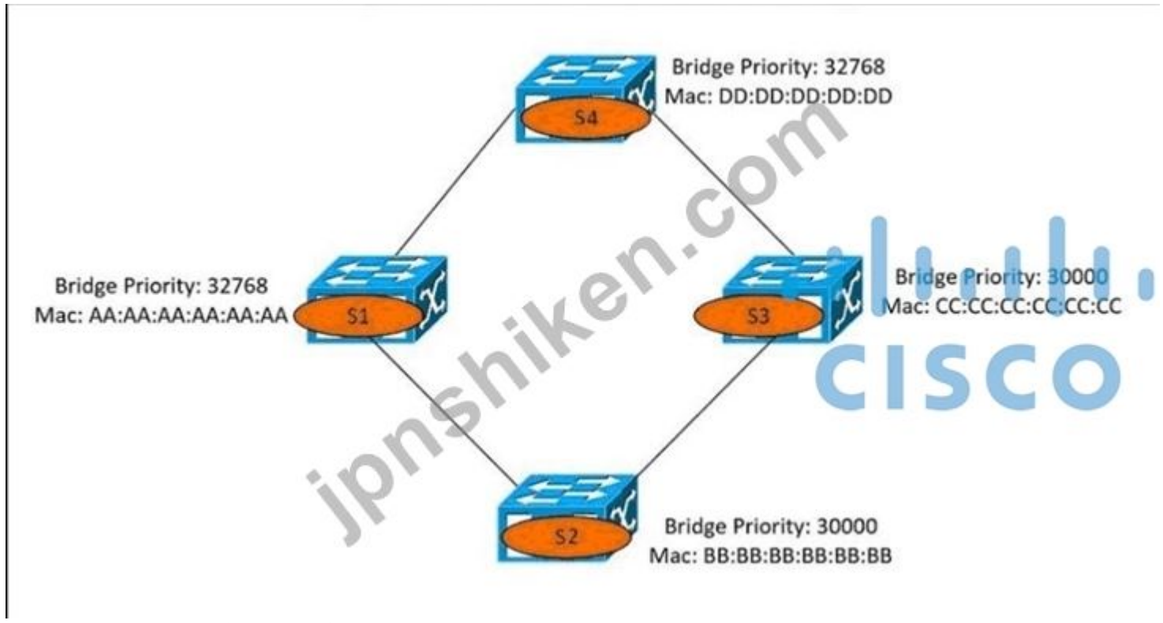
B. ルーティング プロトコルの実行 (OSPF、EIGRP、RIP、BGP)

C. 着信 NETCONF RPC から構成を変更します

D. 着信 ICMP エコー要求に応答する

正解: (正解を表示します)
The correct response is A. The data plane forwards transit traffic by comparing the destination IP address to forwarding information. A router uses the routing table or FIB result to decide the outgoing interface and next hop for a packet. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. Routing protocols, NETCONF configuration changes, and locally generated ICMP replies are control or management-plane activities. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **119**
展示資料を参照してください。



どちらのスイッチがルートブリッジになりますか？
A. S1
B. S2
C. S3
D. S4
正解: (正解を表示します)
The root bridge is the switch with the lowest bridge ID in the spanning-tree instance. The bridge ID comparison starts with priority. If priorities tie, the lower MAC address wins. In many exam exhibits, the correct root is not the switch drawn at the top or center of the topology; it is the switch with the numerically lowest STP identifier. For this exhibit, S2 has the lowest resulting bridge ID, so it becomes the root bridge. Cisco CCNA 200-301 v1.1 Network Access expects engineers to calculate this cleanly because root selection determines which links forward and which links block. Once S2 is elected, all other switches calculate their lowest-cost path back to S2 and choose root ports accordingly. Design practice is to place the root bridge deliberately, normally near the distribution layer, rather than leaving the outcome to MAC address tie- breakers. In this question, the election result is S2, which maps to answer B.

質問: **120**
プラグを差し込むとすぐにネットワーク接続を確立するスイッチ技術はどれですか?
A. PortFast
B. BPDUガード

C. アップリンクファースト
D. バックボーンファースト
正解: (正解を表示します)
Use A for this item. PortFast lets an edge port move to forwarding immediately when a host is connected. It bypasses the traditional listening and learning delay for endpoint ports while still allowing STP protection features such as BPDU Guard. In Cisco CCNA 200-301 v1.1, Network Access questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. BPDU Guard protects edge ports, while UplinkFast and BackboneFast are older convergence enhancements with different purposes. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **121**

図を参照してください。エンジニアがCisco WLC GUIを使用して、AES暗号化方式のWPA2と事前共有キーCisc0123456を使用するWLANを設定しています。エンジニアがレイヤ2セキュリティのドロップダウンリストからWPA + WPA2オプションを選択した後、プロセスを完了するために実行する必要がある2つのタスクはどれですか？(2つ選択してください)
A. WPA2ポリシーとAESのチェックボックスを選択します。
B. PSKフォーマットのドロップダウンリストからASCIIを選択し、キーを入力して、認証キー管理の設定は空白のままにします。
C. WPA2ポリシー、AES、TKIPのチェックボックスを選択します。
D. 認証キー管理ドロップダウンリストでCCKMを選択し、PSKフォーマットをHexに設定して、キーを入力します。
E. 認証キー管理ドロップダウンリストからPSKを選択し、PSKフォーマットをASCIIに設定して、キーを入力します。
正解: (正解を表示します)
Answer A,E is correct: A. Select the WPA2 Policy and AES check boxes; E. Select PSK froin the Auth Key Mgmt drop-down list, set the PSK Format to ASCII, and enter the key. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

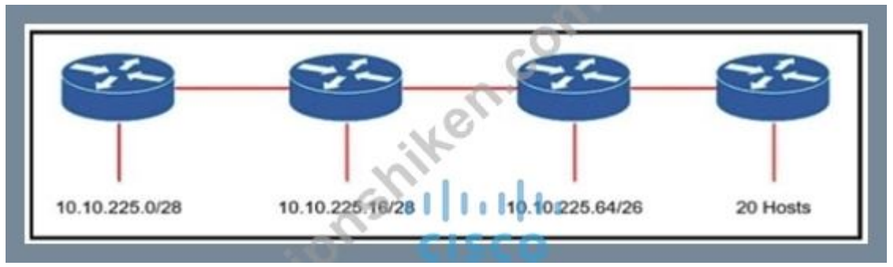
質問: **122**
コントロール ベースのネットワーク アーキテクチャにおけるサウスバウンド API の目的は何ですか?
A. コントローラとアプリケーション間の機能通信
B. コントローラとネットワーク ハードウェア間のファシリティ通信
C. アプリケーション開発者がネットワークとやり取りできるようにします
D. コントローラーを他の自動化およびオーケストレーション ツールと統合します。
正解: **B (**コメントを発表する**)**
The correct response is B. A southbound API enables communication between the controller and network hardware. The controller uses southbound protocols to read state and push operational intent or configuration to switches, routers, and other devices. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. Northbound APIs face applications, and integration APIs connect management or orchestration systems. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **123**
DHCP がルーターに設定されている場合、デフォルト ゲートウェイが自動的に配布されるようにするには、どのコマンドを入力する必要がありますか?
A. デフォルトルーター
B. デフォルトゲートウェイ
C. ip ヘルパーアドレス
D. DNS サーバー
正解: **(**正解を表示します**)**
The verified answer is A. The default-router command in a Cisco DHCP pool supplies the default gateway option to DHCP clients. Clients receive that address as the router to use for destinations outside their local subnet. Cisco CCNA 200-301 v1.1 places this skill in IP Services, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. default- gateway is used differently on some switches, ip helper-address relays DHCP, and dns-server supplies name- resolution servers. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **124**
データプレーンが提供する主要な機能は何ですか？
A. ルーティング決定を行う
B. 発信パケット
C. 次のホップへトラフィックを転送しています
D. ルーティングテーブルデータの交換
正解: **(**正解を表示します**)**
Forwarding traffic to the next hop. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First- hop redundancy protocols add a separate default-gateway resiliency function for hosts

on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **125**



図を参照してください。エンジニアは、ネットワークに20人のユーザーを追加する新しいオフィス用にサブネットを追加する必要があります。
エンジニアは、アドレスの無駄を最小限に抑えるために、どのIPv4ネットワークとサブネットマスクの組み合わせを割り当てるでしょうか？
A. 10.10.225.48 255.255.255.240
B. 10.10.225.32 255.255.255.240
C. 10.10.225.48 255.255.255.224
D. 10.10.225.32 255.255.255.224
正解: **D** (コメントを発表する)
10.10.225.32 255.255.255.224. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Network Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **126**

展示資料を参照してください。
ネットワーク管理者が、インターフェース制御スイッチをCat9300-1スイッチのインターフェースGi1/0/1に接続するように設定しました。新しいインターフェースにはどの設定を適用する必要がありますか？
A.
```
switchport mode trunk
switchport trunk native vlan 321
switchport trunk allowed vlan 100,200,300
```

B.
```
switchport trunk encapsulation dot1q
switchport trunk native vlan 321
switchport trunk allowed vlan 100-300
```

C.
```
switchport mode dynamic desirable
switchport trunk native vlan 321
switchport trunk allowed vlan 100,200,300
```

D.
```
switchport nonegotiate
switchport access vlan 321
switchport trunk allowed vlan except 2-1001
```

正解: (正解を表示します)

Option A. Switching questions depend on MAC learning, VLAN membership, trunking, STP election, and EtherChannel behavior. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong answers misapply a Layer 2 rule or configure the wrong logical interface. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco- consistent behavior for this item.

質問: **127**

エンジニアがIPサブネット10.139.58.0/28からルーターへのリモートアクセスを設定しています。ドメイン名、暗号鍵、SSHは既に設定済みです。宛先ルーターでトラフィックを有効にするには、どの設定が必要ですか？

A.
```
interface FastEthernet0/0
   ip address 10.122.49.1 255.255.255.240
   access-group 120 in

ip access-list extended 120
   permit tcp 10.139.58.0 255.255.255.248 any eq 22
```

B.
```
interface FastEthernet0/0
   ip address 10.122.49.1 255.255.255.252
   ip access-group 110 in

ip access-list extended 110
   permit tcp 10.139.58.0 0.0.0.15 host 10.122.49.1 eq 22
```

C.
```
interface FastEthernet0/0
   ip address 10.122.49.1 255.255.255.248
   ip access-group 10 in

ip access-list standard 10
   permit udp 10.139.58.0 0.0.0.7 host 10.122.49.1 eq 22
```

D.
```
interface FastEthernet0/0
   ip address 10.122.49.1 255.255.255.252
   ip access-group 105 in

ip access-list standard 105
   permit tcp 10.139.58.0 0.0.0.7 eq 22 host 10.122.49.1
```

正解: (正解を表示します)
Option B. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **128**
SFP モジュールを使用する場合、カッパー インターフェイスとファイバー インターフェイスの両方で同じことは何ですか?
A. 信号強度を高めるインライン光減衰器をサポート
B. ホットスワップ可能であるため、サービスの中断が最小限に抑えられます
C. 半二重モードで最大 100 Mbps の信頼できる帯域幅を提供します。
D. 1 つのモジュールでシングルモードとマルチモードに対応します。
正解: (正解を表示します)
They provide minimal interruption to services by being hot-swappable. Physical-layer and Ethernet questions depend on media characteristics, interface counters, duplex behavior, and how frames are transmitted or errored on the link. Cisco CCNA 200-301 v1.1 includes this topic under Network Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario.
The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The incorrect answers either describe a different medium, the wrong connector, or an error counter that would not increment for the condition described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

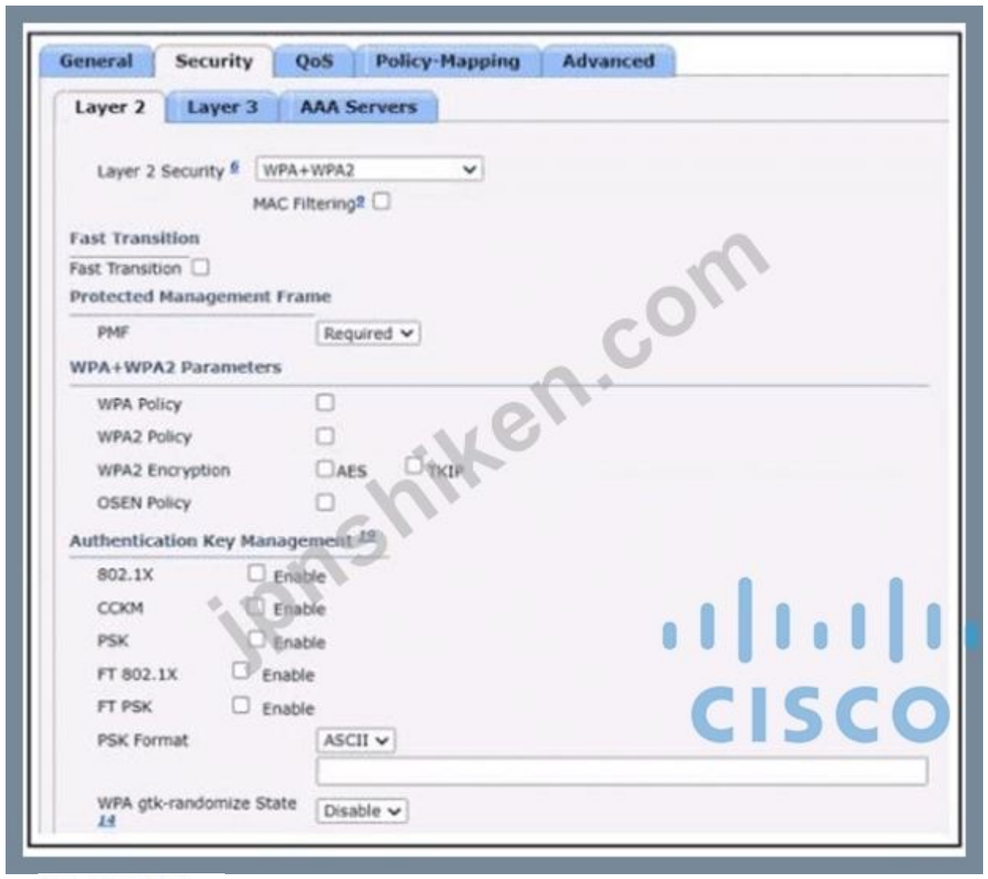
質問: **129**
R1はIS-IS、OSPF、RIP、および内部EIGRPを介してルート192.168.12.0/24を学習しました。通常の動作条件下では、どのルーティングプロトコルのルートがルーティングテーブルにインストールされますか？
A. IS-IS
B. 安らかにお眠りください
C. OSPF
D. 内部EIGRP
正解: (正解を表示します)
Internal EIGRP. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **130**
認証と認可の違いは?
A. 認証はネットワークにアクセスする人物の身元を確認し、承認はユーザーがアクセスできるリソースを決定します。
B. 認証はユーザーがアクセスするリソースを記録するために使用され、承認はユーザーがアクセスできるリソースを決定するために使用されます。

C. 認証は、ユーザーがアクセスできるリソースを決定するために使用され、承認は、ネットワークへのアクセスが許可されている機器を追跡するために使用されます。
D. 認証は個人の身元を確認するために使用され、認可はログイン用の syslog メッセージを作成するために使用されます。
正解**: (**正解を表示します**)**
Authentication verifies the identity of a person accessing a network, and authorization determines what resource a user can access.. IP services must be selected by their exact operational role: addressing, translation, time, monitoring, logging, redundancy, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The wrong options name real services or commands, but they solve a different infrastructure problem. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問**: 131**
インターフェイスで IPv6 を構成する場合、参加する 2 つの IPv6 マルチキャスト グループはどれですか? (2 つ選択)
A. 2000::/3
B. 2002::5
C. FC00::/7
D. FF02::1
E. FF02::2
正解**: D,E (**コメントを発表する**)**
An IPv6-enabled router interface joins the all-nodes multicast group FF02::1 and the all-routers multicast group FF02::2. FF02::1 is used to reach all IPv6 nodes on the local link. FF02::2 is used to reach IPv6 routers on the local link. The interface also joins a solicited-node multicast group derived from its IPv6 address, but that specific group is not one of the answer choices. 2000::/3 represents global unicast space, FC00::/7 is unique local addressing, and 2002::/5 or similar values are not the required local multicast groups. The "FF" prefix is the key sign that the address is multicast, while the "02" scope means link-local scope. CCNA 200-
301 v1.1 Network Fundamentals expects candidates to identify common IPv6 address types and multicast groups used by Neighbor Discovery and routing functions. Therefore the verified answers are D and E.
Reference: Cisco IPv6 multicast addressing and IPv6 interface behavior.

質問**: 132**
展示資料を参照してください。



A. Select **WPA Policy**
Select **WPA2 Policy**
Enable **FT PSK**

B. Select **WPA2 Policy**
Disable **PMF**
Enable **PSK**

C. Select **WPA Policy**
Enable **CCKM**
Enable **PSK**

D. Disable **PMF**
Enable **PSK**
Enable **802.1x**

正解: **C** (コメントを発表する)

Option C. The answer follows from standard Cisco behavior and the operational clue in the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The other choices describe related terms, but they do not satisfy the requirement stated in the prompt. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **133**

PC1 は、新しくインストールされた PC2 にトラフィックを送信しようとします。PC2 MAC アドレスはスイッチの MAC アドレス テーブルにリストされていないため、スイッチは同じ VLAN 内のすべてのポートにパケットを送信します。これはどのスイッチングの概念を表していますか?

A. MAC アドレス エージング
B. MACアドレステーブル
C. フレームフラッディング
D. スパニング ツリー プロトコル
正解: **(**正解を表示します**)**
frame flooding. When a switch receives a frame and does not have the destination MAC address in its MAC address table, it floods the frame out all ports in the same VLAN except the ingress port. That behavior is called frame flooding or unknown-unicast flooding. MAC address aging can cause an entry to disappear, but the described action is the flooding behavior itself. Spanning Tree prevents loops; it does not describe this forwarding action. Cisco CCNA 200-301 v1.1 Network Access expects engineers to understand how switches learn source MAC addresses and forward or flood based on destination MAC lookups. The corrected answer is frame flooding. Once the destination host replies, the switch can learn the missing MAC address and forward future traffic directly.

質問: **134**
RESTリクエストにおけるURI文字列の目的は何ですか？
A. ターゲットサーバー上のリソースを識別する。
B. データまたはペイロードをリモートリソースに転送します。
C. リモート リソースを変更する方法を指定します。
D. リクエストのデータコンテンツエンコーディングで応答します。
正解: **(**正解を表示します**)**
To specify the way in which a remote resource is modified.. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE. JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact with a controller, while southbound APIs allow the controller to communicate with network devices.
NETCONF and RESTCONF are configuration/management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to-device communication with application-to-controller communication or confuse a data format with a protocol. Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers. The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

質問: **135**
レイヤ2スイッチの特徴は何ですか？
A. ルーターを使用して衝突ドメインを作成します
B. 特定の順序でデータを送信する役割を担う
C. より高速な伝送のためにMACアドレスの保存を回避します
D. 通信にデータリンク層を使用する
正解: **D (**コメントを発表する**)**
Uses the data link layer for communications. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **136**
IPv6アドレスのうち、IPv4パブリックアドレスと同様にパブリックにルーティング可能なアドレスはどれですか？
A. グローバルユニキャスト

B. リンクローカル
C. 一意のローカル
D. マルチキャスト
正解: (正解を表示します)
global unicast. IPv6 questions require identifying the address scope, address block, assignment method, and the role of multicast, link-local, unique-local, or global-unicast addressing. Cisco CCNA 200-301 v1.1 includes this topic under Network Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The wrong choices describe another IPv6 scope or an assignment process that does not match the address behavior in the prompt.
In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu 1**813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **137**
HTTP 内の put メソッドとは何ですか?
A. 読み取り専用操作です。
B. 万能でない操作です。
C. 宛先でデータを置き換えます。
D. Web サイトを表示します。
正解: (正解を表示します)
It replaces data at the destination.. The HTTP PUT method is used to update or replace a resource at a known URI. It is not a read-only operation; GET is read-only. It is generally treated as idempotent, meaning repeating the same PUT request should leave the resource in the same final state. It also does not simply display a web site. Cisco CCNA 200-301 v1.1 Automation and Programmability expects engineers to map REST operations to CRUD behavior: POST creates, GET reads, PUT updates or replaces, PATCH partially updates, and DELETE removes. The corrected answer is that PUT replaces data at the destination. That is the REST behavior being tested by this question.

質問: **138**
コラプスド コア アーキテクチャを使用する必要があるのは、どのタイプの組織ですか?
A. 大規模で、柔軟でスケーラブルなネットワーク設計が必要
B. 大規模で、ハードウェア障害時のダウンタイムを最小限に抑える必要があります
C. 規模が小さく、現在ネットワーク コストを削減する必要がある
D. 小さいが、近い将来劇的に成長すると予想される
正解: (正解を表示します)
small and needs to reduce networking costs currently. The answer follows directly from normal Cisco device behavior and the wording of the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would

normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **139**
SDN コントローラーの 2 つの機能は何ですか? (2つ選んでください)
A. レイヤ 2 転送
B. VTN の調整
C. ホストの追跡
D. トポロジの管理
E. DDoS 攻撃からの保護
正解: **C,D (コメントを発表する)**
Answer C and D is the technically correct selection. An SDN controller tracks network topology and host information. That centralized intelligence lets applications request network behaviour while devices receive instructions through southbound communication. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. Layer 2 forwarding remains a device data-plane function, and DDoS protection is not a generic required SDN-controller function. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

質問: **140**
ネットワーク エンジニアは、マネージド サービス クライアントに属するスイッチを新しい Cisco Catalyst スイッチに交換しています。新しいスイッチは、交換を含む更新されたセキュリティ基準に合わせて構成されます。
暗号化された接続を使用し、モジュラス サイズを 1024 から 2 倍にする Telnet サービス。エンジニアが新しいスイッチに設定する必要がある 2 つのコマンドはどれですか? 2つ選んでください。)
A. 暗号鍵生成 RSA 一般鍵モジュラス 1024
B. トランスポート入力すべて
C. 暗号鍵生成 RSA 使用鍵
D. 暗号鍵生成 RSA モジュラス 2048
E. トランスポート入力 ssh
正解: **(正解を表示します)**
Answer D,E is correct: D. crypto key generate rsa modulus 2048; E. transport Input ssh. Secure Shell requires RSA keys and the VTY lines must permit SSH. For current security practice, a 2048-bit RSA modulus is the better choice than 1024-bit keys. The transport input ssh command restricts remote access to SSH instead of permitting insecure Telnet. The transport input all option would still allow Telnet and fails the requirement to replace Telnet with encrypted access. Cisco CCNA 200-301 v1.1 Security Fundamentals expects engineers to combine cryptographic key generation, local/domain prerequisites, and VTY transport settings when enabling SSH. The corrected answer pair is crypto key generate rsa modulus 2048 and transport input ssh. Together, they create the cryptographic material and enforce the encrypted management protocol on the line configuration.

質問: **141**
フローティング スタティック ルートが設定されている場合、プライマリ ルートに障害が発生したときにバックアップ ルートが確実に使用されるようにするアクションはどれですか?
A. フローティング スタティック ルートは、プライマリ ルートよりも高いアドミニストレーティブ ディスタンスを持つ必要があるため、バックアップとして使用されます。
B. バックアップ ルートがセカンダリになるように、プライマリ ルートのアドミニストレーティブ ディスタンスを大きくする必要があります。
C. フローティング スタティック ルートは、プライマリ ルートよりもアドミニストレーティブ ディスタンスを低くする必要があるため、バックアップとして使用されます。
D. ルーティング テーブルにルートをインストールするには、default-information originate コマンドを設定する必要があります。
正解: **(正解を表示します)**

A floating static route must have a higher administrative distance than the primary route. That is what keeps it out of the routing table while the primary route is valid. If the primary route fails, the routing table process removes the better route and installs the backup static route with the higher AD. Option A states that behavior correctly. If the backup route had a lower administrative distance, it would become preferred immediately and would not act as a backup. Raising the primary route's distance is not the normal design; the route intended to float is the one configured with the higher distance. The default-information originate command is for advertising a default route into a routing protocol, not for installing a floating static backup. This is core CCNA 200-301 v1.1 IP Connectivity: floating statics provide deterministic fallback when a dynamic route or primary static route disappears. Reference: Cisco IOS static routing and administrative-distance selection.

質問: **142**
ネットワーク上のサーバーの 2 つの機能は何ですか? (2つ選んでください)
A. 仮想サーバークラスタリングのみを使用して冗長化を実現
B. 要求を行うワークステーションのデータを送受信するアプリケーションを実行します
C. 複数のワークステーションからのリクエストを同時に処理します
D. 他のサーバーと通信するために同じオペレーティング システムを実行します。
E. 単一のクライアント専用のデータ センターにのみ収容されます。
正解: **(正解を表示します)**
A server provides services to clients. In practical network terms, it runs applications or services that workstations request, and it can handle requests from multiple clients at the same time. Examples include web servers, file servers, DNS servers, DHCP servers, authentication servers, and application servers. A server does not have to run the same operating system as other servers to communicate; network protocols provide interoperability. It also does not achieve redundancy only through virtual clustering, and it does not have to be housed solely in a data center dedicated to one client. Cisco CCNA 200-301 v1.1 Network Fundamentals includes endpoint and server roles because engineers must understand what traffic sources and destinations exist on the network. The two correct functions are application/data service delivery and handling simultaneous client requests. That makes B and C correct.

質問: **143**
レイヤ 2 の到達可能性とレイヤ 3 のルーティング情報を提供することで、ネットワーク デバイスがパケット転送の決定を行うのを支援するソフトウェア定義アーキテクチャ プレーンはどれですか?
A. データプレーン
B. コントロール プレーン
C. ポリシー プレーン
D. 管理プレーン
正解: **(正解を表示します)**
The control plane is the part of a network device or architecture that builds the information used for forwarding decisions. Routing protocols, Layer 2 control protocols, neighbor discovery, ARP processing, and topology calculations all live conceptually in the control plane. The data plane then uses the resulting tables to forward traffic at speed. In software-defined architecture, this distinction becomes even sharper because the controller can centralize or influence control-plane decisions while the devices still forward packets. Cisco CCNA 200-301 v1.1 expects candidates to separate control, data, and management-plane functions. The data plane moves user packets. The management plane handles administrative access and configuration. A policy plane is not the standard answer for Layer 2 reachability and Layer 3 routing information. The plane that assists devices with making packet-forwarding decisions by supplying reachability and route information is the control plane.

質問: **144**
エンジニアは、コア ルーターに、バックアップ ルーター (10.200.0.2) へのフローティング静的デフォルト ルートを設定する必要があります。

正解:

Explanation:

Cisco CCNA 200-301 v1.1 IP Connectivity questions of this form test whether each protocol, command, service, or architecture term is placed with the function it actually performs. The safest approach is to classify each item by operating layer and purpose before matching it: routing behavior belongs to IP connectivity, wireless modes belong to access, REST methods belong to automation, and AAA functions belong to security services. Several distractors are valid networking terms, but they become wrong when mapped to the wrong plane or protocol. The retained mapping follows Cisco terminology and reflects

how the features are used in implementation and troubleshooting. In practice, this prevents mixing up forwarding behavior with management behavior or authentication with authorization/accounting. The mapping shown in the file is therefore retained as the verified response.

質問: **145**

展示資料を参照してください。

ネットワークエンジニアが、図のように直接接続された2台のルーターの設定を開始しました。2台のルーターがOSPFネイバーとなるように、エンジニアはR2上でどのようなコマンドシーケンスを設定する必要がありますか？

A.
```
router ospf 1
  network 192.168.12.1 0.0.0.0 area 1
```

B.
```
interface GigabitEthernet0/1
  ip ospf 1 area 1
```

C.
```
interface GigabitEthernet0/1
  ip ospf 1 area 0
```

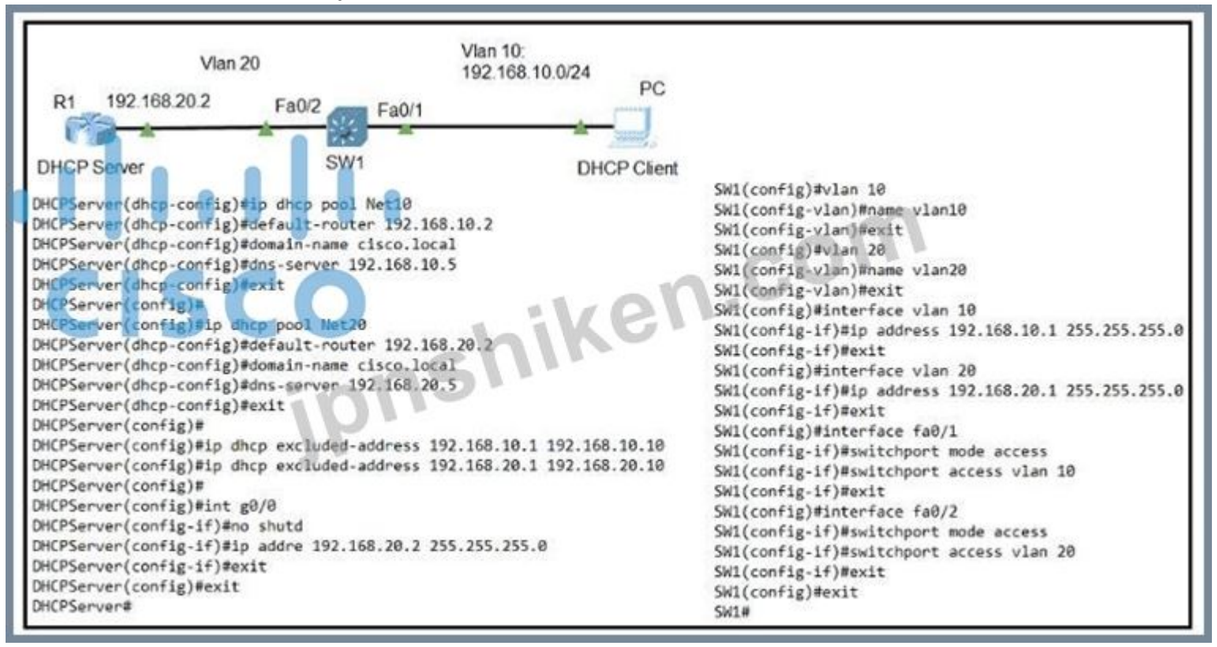
D.
```
router ospf 1
  network 192.168.12.0 0.0.0.127 area 0
```

正解: (正解を表示します)

Option D. Routing questions are solved by applying longest-prefix match, administrative distance, metric, and protocol-specific behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Wrong answers either use the wrong prefix, the wrong next hop, or a route source that would not be preferred. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **146**
コントローラベースのネットワーク アーキテクチャでノースバウンド API が果たす役割はどれですか?
A. コントローラと物理ネットワーク ハードウェア間の通信
B. デバイスのエラーをコントローラに報告します
C. ネットワーク ハードウェアとトラフィックの統計を生成します
D. コントローラとアプリケーション間の通信を容易にします
正解: **(**正解を表示します**)**
A northbound API lets applications communicate with the controller. In controller-based networking, the controller sits between applications and the network devices. Applications use northbound APIs to request services, retrieve information, or express intent. The controller then translates those requests into device-level actions through southbound communication. This is the direction model CCNA candidates must keep straight:
northbound faces applications and orchestration systems; southbound faces routers, switches, access points, and other infrastructure. A northbound API does not directly communicate with physical hardware, and it is not primarily a mechanism for raw device error reporting. It can expose statistics, but that is not its defining purpose. Cisco CCNA 200-301 v1.1 covers northbound and southbound APIs under Automation and Programmability because modern network operations increasingly use controllers and REST-style interfaces.
The answer that precisely describes the northbound role is D: it facilitates communication between the controller and the applications.

質問: **147**
展示資料を参照してください。



DHCPサーバーは、各サブネットごとにDHCPプールが設定されています。VLAN 10上のDHCPクライアントがDHCPサーバーから動的IPアドレスを受信できるようにするには、スイッチSW1でどのコマンドを設定する必要がありますか？

A. SW1(config-if)#ip helper-addresss 192.168.20.2
B. SW1(config-if)#ip helper-addresss 192.168.20.1
C. SW1(config-if)#ip helper-addresss 192.168.10.2
D. SW1(config-if)#ip helper-addresss 192.168.10.1

正解: **(**正解を表示します**)**

SW1(config-if)#ip helper-addresss 192.168.10.2. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco- consistent configuration or behavior for this wireless scenario.

質問: **148**

図を参照してください。ルーターR1は、192.168.64.22宛てのパケットをどのように処理しますか？

A. 10.1.1.1 への静的ルートを使用します。
B. 最も高いADと最も高い宛先IPを持つルートを使用します。
C. パケットを 10.1.1.2 にルーティングします。
D. パケットを破棄します。

正解: **(**正解を表示します**)**

It will drop the packets.. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First- hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **149**

組織がネットワークのパフォーマンスを検証し、問題をトラブルシューティングし、監視ツールとエンドデバイス間の通信にエージェントを使用する必要がある場合、どのプロトコルが実装されますか？

A. SNMP
B. FTP
C. NTP
D. NFS

正解: **D (**コメントを発表する**)**

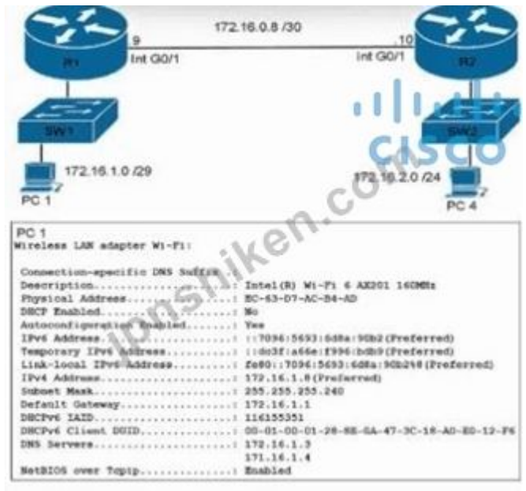
NFS. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP,

TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **150**
展示資料を参照してください。

JSONオブジェクトはいくつ表現されていますか？
A. 1
B. 2
C. 3
D. 4
正解: **(**正解を表示します**)**
4. Automation questions depend on recognizing controllers, APIs, data formats, HTTP methods, and cloud- service characteristics. Cisco CCNA 200-301 v1.1 includes this under Automation and Programmability, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The wrong options mix controller functions with data-plane forwarding or confuse API operations with unrelated management terms. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **151**



図を参照してください。初期構成テスト中に、WindowsワークステーションPC1が172.16.2.0/24ネットワークに接続できません。どの操作を行うことで構成が修正されますか？
A. IPアドレスを172.16.1.6に変更し、サブネットマスクを255.255.255.248に変更します。

B. IPアドレスを172.16.1.9に変更し、デフォルトゲートウェイを172.16.1.7に変更します。
C. IPアドレスを172.16.1.9に変更し、DNSサーバーを172.16.1.12のみに変更します。
D. IPアドレスを172.16.1.6に変更し、DNSサーバーを172.18.1.12と172.16.1.13に変更します。
正解: **(**正解を表示します**)**
Change the IP addressss to 172.16.1.9 and change the default gateway to 172.16.1.7.. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **152**
展示資料を参照してください

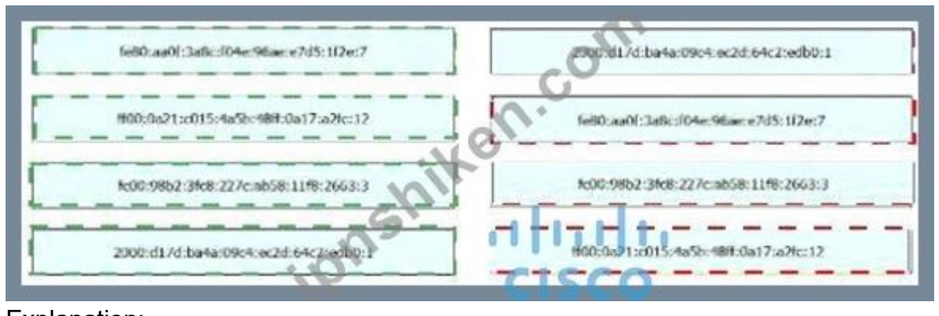
ネットワークエンジニアが新しいスイッチのポートセキュリティの設定を開始しました。以下の要件を満たす必要があります。
* MACアドレスは動的に学習する必要がある
* 不要なトラフィックが検出された場合でも、インターフェースを無効にせずにログメッセージを生成する必要があります。このタスクを完了するには、どの 2 つのコマンドを設定する必要がありますか？(2 つ選択してください)
A. SW(config-if)=switchport port-security mac-address sticky
B. SW(config-if)=switchport port-security violation restrict
C. SW(config-if)sswitchport port-security mac-address 0010.7B84.45E6
D. SW(config-if)switchport port-security maximum 2
E. SW(config-if)=switchport port-security violation shutdown
正解: **(**正解を表示します**)**
Answer A,B is correct: A. SW(config-if)=switchport port-security mac-address sticky; B. SW(config-if)

=switchport port-security violation restrict. Sticky MAC learning lets the switch dynamically learn secure MAC addresses and add them to the running configuration. The restrict violation mode drops unauthorized traffic and generates log/SNMP notifications without shutting down the interface. That exactly matches the requirements: dynamic learning and log messages without disabling the port. A statically configured MAC address fails the dynamic-learning requirement, and violation shutdown would place the interface into err- disabled state. Cisco CCNA 200-301 v1.1 Network Access and Security Fundamentals expect precise understanding of port-security violation modes: protect drops silently, restrict drops and logs, and shutdown disables the port. The corrected answer pair is sticky MAC learning and violation restrict.

質問: **153**
バックドア マルウェアの定義は?
A. コンピュータにインストールされ、権限のないユーザーによるアクセスを可能にする悪意のあるコード
B. 他の悪意のあるコードをダウンロードすることを主な目的とする悪意のあるコード
C. 他の悪意のあるプログラムを起動するために使用される悪意のあるプログラム
D. ユーザーのマシンに感染し、そのマシンを使用してスパムを送信する悪意のあるコード
正解: **(**正解を表示します**)**
malicious code that is installed onto a computer to allow access by an unauthorized user. Security questions require distinguishing authentication, authorization, encryption, secure management, malware protection, and physical controls. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The wrong options apply the right security vocabulary to the wrong control or use weaker/deprecated protection. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **154**
左側のIPv6アドレスを右側のタイプにドラッグアンドドロップしてください。

正解:

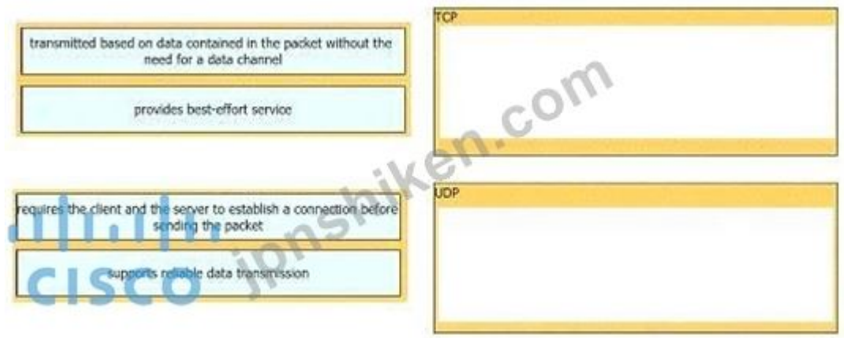


Explanation:
Cisco CCNA 200-301 v1.1 expects these items to be matched by function, protocol layer, scope, and operational role rather than by keyword similarity. The reliable method is to identify what each item actually does in a Cisco network: whether it forwards traffic, manages a device, secures access, assigns addressing, identifies a resource, or carries control information. Distractors in this format are usually valid networking terms placed under the wrong category. That is why the retained mapping is important; it keeps protocol behavior, device function, and service purpose aligned. In a real network, mixing these

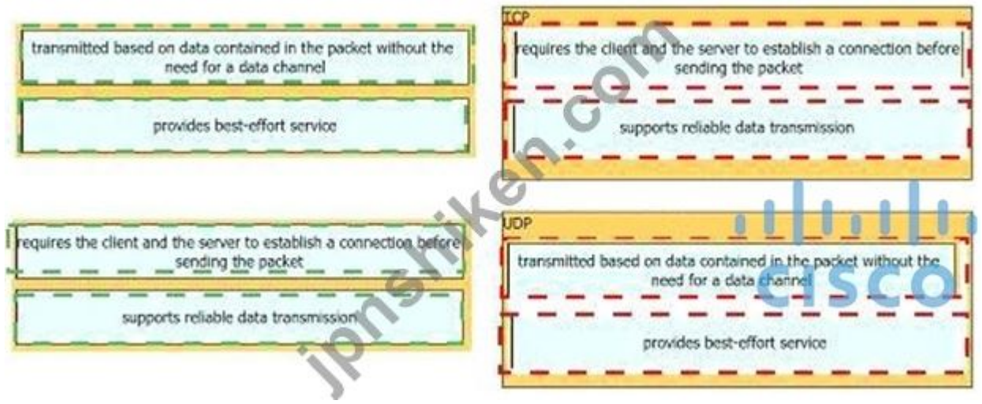
concepts leads to broken routing, failed wireless access, insecure management, or automation calls aimed at the wrong interface. The mapping shown in the document is therefore retained as the Cisco-consistent answer for this item.

質問: 155

左側のTCPまたはUDPの詳細を、右側の対応するプロトコルにドラッグアンドドロップしてください。

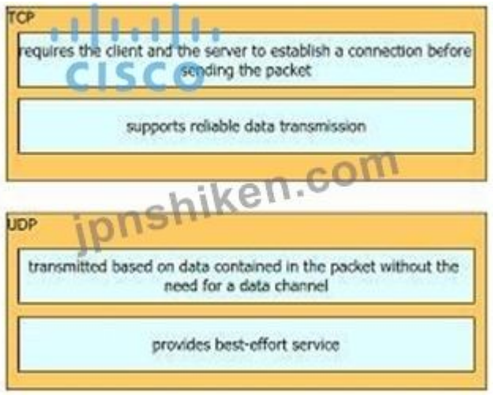


正解:



Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.



質問: **156**
コラプテッドコアアーキテクチャにおけるコア層とディストリビューション層の役割は何ですか？
A. ルーターはレイヤ3でIPv4およびIPv6アドレスを使用する必要があります。
B. コア層とディストリビューション層は、フェイルオーバーを可能にするために2つの異なるデバイスに展開されます。
C. ルーターは、IPv6 ネットワークにおけるレイヤ 2 冗長性のための HSRP をサポートできます。
D. ルーターは単一のデバイスまたは冗長ペアで動作します。
正解: **(**正解を表示します**)**
The router operates on a single device or a redundant pair.. Routing and redundancy questions are solved by applying longest-prefix match, administrative distance, metrics, and gateway-redundancy behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Incorrect choices point to the wrong next hop, choose the wrong route source, or confuse routing with Layer 2 behavior. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **157**
認証の概念を承認およびアカウンティングと区別する特徴はどれですか?
A. ユーザー アクティビティ ログ
B. サービスの制限
C. 従量課金制
D. 本人確認
正解: **D (**コメントを発表する**)**
identity verification. Security fundamentals require distinguishing identity, authorization, accounting, encryption, inspection, and physical protection. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The incorrect choices apply a security term in the wrong control category or protect a different part of the system. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **158**
Ciscoのエンジニアは、これらの要件を満たすために単一のスイッチインターフェイスを設定する必要があります。
* タグなしフレームを受け入れ、VLAN 20に配置する

* CDPがCisco IP電話を検出した場合、VLAN 30でタグ付きフレームを受け入れる
エンジニアはどのコマンドセットを適用しなければならないか？

A.
```
switchport mode dynamic desirable
switchport access vlan 20
switchport trunk allowed vlan 30
switchport voice vlan 30
```

B.
```
switchport mode dynamic auto
switchport trunk native vlan 20
switchport trunk allowed vlan 30
switchport voice vlan 30
```

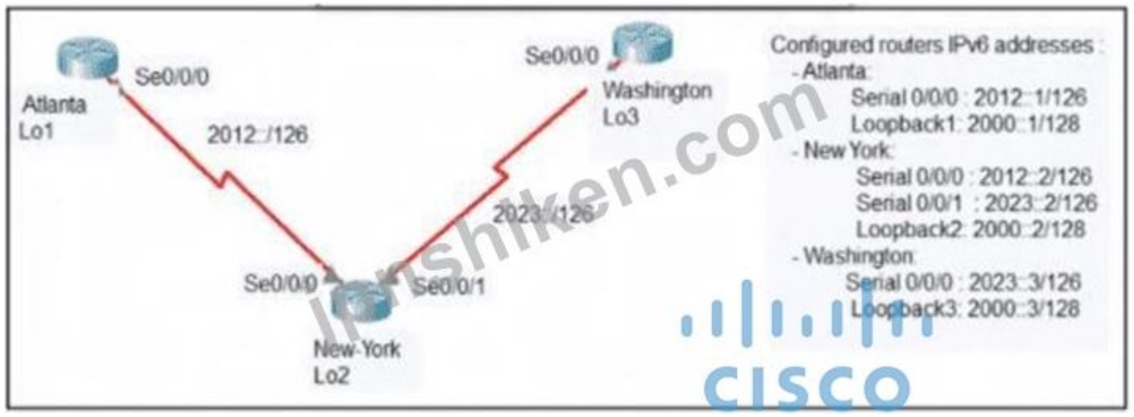
C.
```
switchport mode access
switchport access vlan 20
switchport voice vlan 30
```

D.
```
switchport mode trunk
switchport access vlan 20
switchport voice vlan 30
```

正解: **(**正解を表示します**)**
Option C. Switching behavior depends on VLAN tagging, trunk negotiation, STP role selection, EtherChannel mode, and whether a protocol is standards-based or Cisco-specific. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. Incorrect options change existing VLAN reachability, use the wrong negotiation behavior, or apply a feature to the wrong switch function. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **159**
TCPプロトコルとUDPプロトコルの違いは何ですか？
A. TCPはセグメント番号を割り当てることで送信または受信されるセグメントを追跡し、UDPはネットワークの状態に応じてデータフローを調整します。
B. TCPは転送前に相手側のデバイスとの接続を確立し、UDPは接続を確立せずに転送します。
C. TCPは上位プロトコル層でエラーチェックを行いながら一定の速度でデータを送信し、UDPはエラーチェックとシーケンス制御を提供します。
D. TCPはハンドシェイクを待たずにデータを即座に送信し、UDPは受信側からの応答を待ってから追加データを送信します。
正解: **B (**コメントを発表する**)**
TCP establishes a connection with the device on the other end before transferring, and UDP transfers without establishing a connection.. Network fundamentals questions require careful attention to address scope, media type, cabling limits, topology design, virtualization, cloud service models, and the difference between TCP and UDP. The CCNA 200-301 v1.1 blueprint expects candidates to identify not only definitions but also the operational consequence of each choice. For example, public and private addressing have different routing behavior; fiber and copper use different physical media; TCP and UDP make different reliability tradeoffs; and virtualization abstracts physical resources through a hypervisor. The wrong answers are usually plausible terms from the same area, but they do not match the exact condition described in the question. The selected answer is correct because it is the only option that fits the stated network behavior, design requirement, or physical/logical property. That is the level of precision needed for Cisco troubleshooting and implementation work.

質問: **160**
展示資料を参照してください。



エンジニアは、ニューヨークのルーターに、アトランタとワシントンのサイトを指す静的ルートを設定した。
アトランタとワシントンのルーターで、両サイトがニューヨークのルーター上のループバック2インターフェースに到達できるように、どのコマンドを設定する必要がありますか？
A. ipv6 ルート ::/0 シリアル 0/0/1
B. ipv6 ルート 0/0 シリアル 0/0/0
C. ipv6 ルート ::/0 シリアル 0/0/0
D. ip route 0.0.0.0.0.0.0.0 Serial 0/0/0
E. ipv6 ルート ::/0 2000::2
正解: **(**正解を表示します**)**
The correct response is C. The remote routers need an IPv6 default route pointing toward New York over the correct serial interface. The ::/0 prefix represents the IPv6 default route and sends unknown destinations, including New York loopback reachability, toward the next hop or exit interface. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. IPv4 default-route syntax and malformed IPv6 prefixes do not satisfy the requirement. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **161**
NOCCという名前のDHCPプールが作成されました。このプールは192.168.20.0/24を使用しており、DHCPクライアントのデフォルトゲートウェイとして、使用可能なIPアドレスの最後から2番目のアドレスを使用する必要があります。このプロセスの次のステップは何ですか？
A. デフォルトルーター 192.168.20.253
B. ネットワーク 192.168.20.254 255.255.255.0 セカンダリ
C. ip default-gateway 0.0.0.0 0.0.0.0 192.168.20.253
D. 次のサーバー 192.168.20.254
正解: **A (**コメントを発表する**)**
default-router192.168.20.253. Routing and redundancy questions are solved by applying longest-prefix match, administrative distance, metrics, and gateway-redundancy behavior in the correct order. Cisco CCNA
200-301 v1.1 includes this under IP Services, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Incorrect choices point to the wrong next hop, choose the wrong route source, or confuse routing with Layer 2 behavior. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **162**
展示資料を参照してください。

```
A# show ip ospf neighbor
Neighbor ID  Pri   State           Dead Time   Address       Interface
172.1.1.1    1     EXCHANGE/  -    00:00:36    172.16.32.1   Serial0.1
```

エンジニアは、ピアルーターAがネイバー172.1.1.1とOSPFネイバー関係を確立する必要があるという設定タスクを受任します。出力には、2時間後の隣接関係の状態が表示されます。ルーターが隣接関係を確立するための設定プロセスの次のステップは何ですか？

A. ルーター A をルーター B と同じ MTU サイズを使用するように設定します。

B. ルーター B の OSPF ID を非ホスト アドレスに設定します。

C. ルーター A とルーター B の間にポイントツーポイントリンクを設定します。

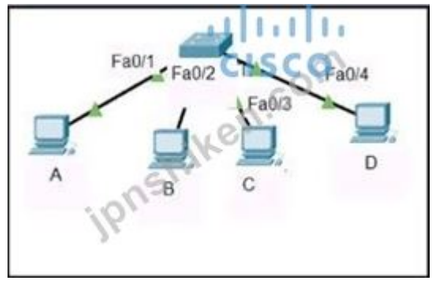
D. ルーターBのOSPF IDをIPアドレスと同じ値に設定する

正解: **(**正解を表示します**)**

Configure router A to use the same MTU size as router B.. OSPF behavior is controlled by interface state, area, timers, network type, cost, priority, router ID, and neighbor/adjacency rules. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The distractors confuse OSPF with unrelated metrics, local-only process values, or parameters that do not satisfy the adjacency or route-selection requirement. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **163**

展示資料を参照してください。



ホストAはホストD宛てのデータフレームを送信した。

スイッチはホストAからフレームを受信すると、どのような動作をしますか？

A. スイッチCAMテーブルからフレームを削除します。

B. Fa0/1ポートを除くすべてのポートからフレームをフラッディングします。

C. ポート Fa0/1 をシャットダウンし、err-disable モードにします。

D. 放送嵐に見舞われます。

正解: **(**正解を表示します**)**

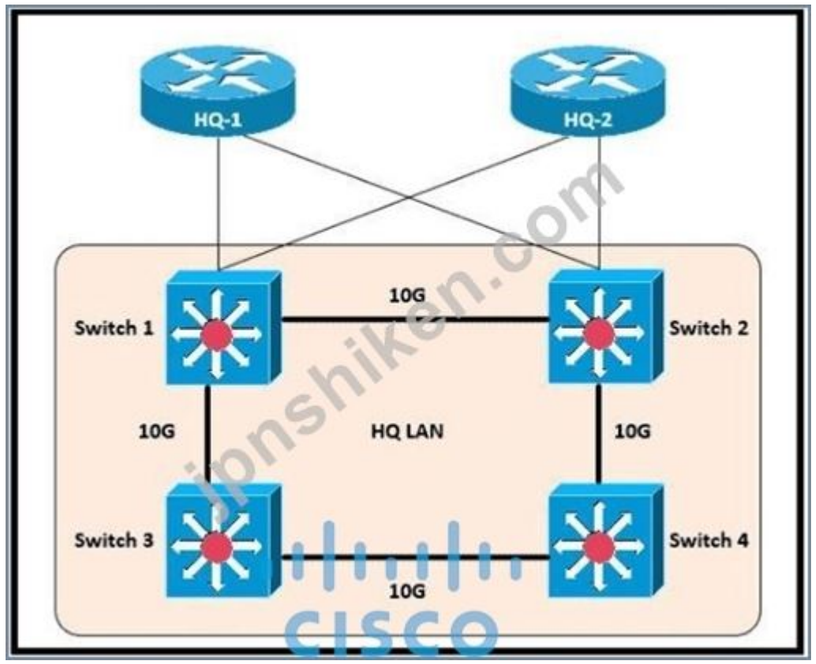
It floods the frame out of all ports except port Fa0/1.. Switching behavior is determined by MAC learning, VLAN membership, trunk state, port security, and EtherChannel negotiation. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The incorrect choices either alter the wrong interface behavior or confuse access-layer switching with routing or security

services. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **164**
ネットワーク管理者は、syslogサーバーが受信メッセージを重要度に基づいて異なるファイルにフィルタリングするようにしたいと考えています。どのフィルタリング基準を使用する必要がありますか？
A. レベル
B. メッセージ本文
C. プロセスID
D. 施設
正解: **(**正解を表示します**)**
level. IP services questions are about the supporting protocols that make a network manageable and usable:
DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **165**
個々のネットワークエンドポイントを攻撃から保護するための解決策として、どのようなものが用いられていますか？
A. ルーター
B. ワイヤレスコントローラー
C. マルウェア対策ソフトウェア
D. シスコDNAセンター
正解: **(**正解を表示します**)**
anti-malware software. Routing and redundancy questions are solved by applying longest-prefix match, administrative distance, metrics, and gateway-redundancy behavior in the correct order. Cisco CCNA 200-
301 v1.1 includes this under Security Fundamentals, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Incorrect choices point to the wrong next hop, choose the wrong route source, or confuse routing with Layer 2 behavior. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco- consistent behavior for this item.

質問: **166**
展示資料を参照してください。



VLAN 110のスパニングツリーのルートとなるスイッチはどれですか？

A. スイッチ1
B. スイッチ2
C. スイッチ3
D. スイッチ4

正解: (正解を表示します)

Use B for this item. The spanning-tree root bridge is selected by the lowest bridge ID for the VLAN. The bridge ID combines bridge priority and MAC address, so the switch with the numerically lowest effective value becomes root for VLAN 110. In Cisco CCNA 200-301 v1.1, Network Access questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. Physical placement and port count do not decide the STP root; only the STP election values do. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **167**
Cisco DNA Centerのどの2つの機能が、従来のキャンパスデバイス管理と比較して、より拡張性を高めているのでしょうか？(2つ選択してください。)
A. 外部アプリケーションがネイティブに連携できるようにするREST API
B. Cisco IOSソフトウェアのすべてのファミリーをサポートするアダプタ
C. サードパーティ製ネットワーク機器との連携をサポートするSDK
D. 中小企業および大企業向けにカスタマイズされたバージョン
E. 必要に応じてアップグレード可能なモジュール設計
正解: **(正解を表示します)**
Answer A,C is correct: A. REST APIs that allow for external applications to interact natively; C. SDKs that support interaction with third-party network equipment. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **168**
展示資料を参照してください。

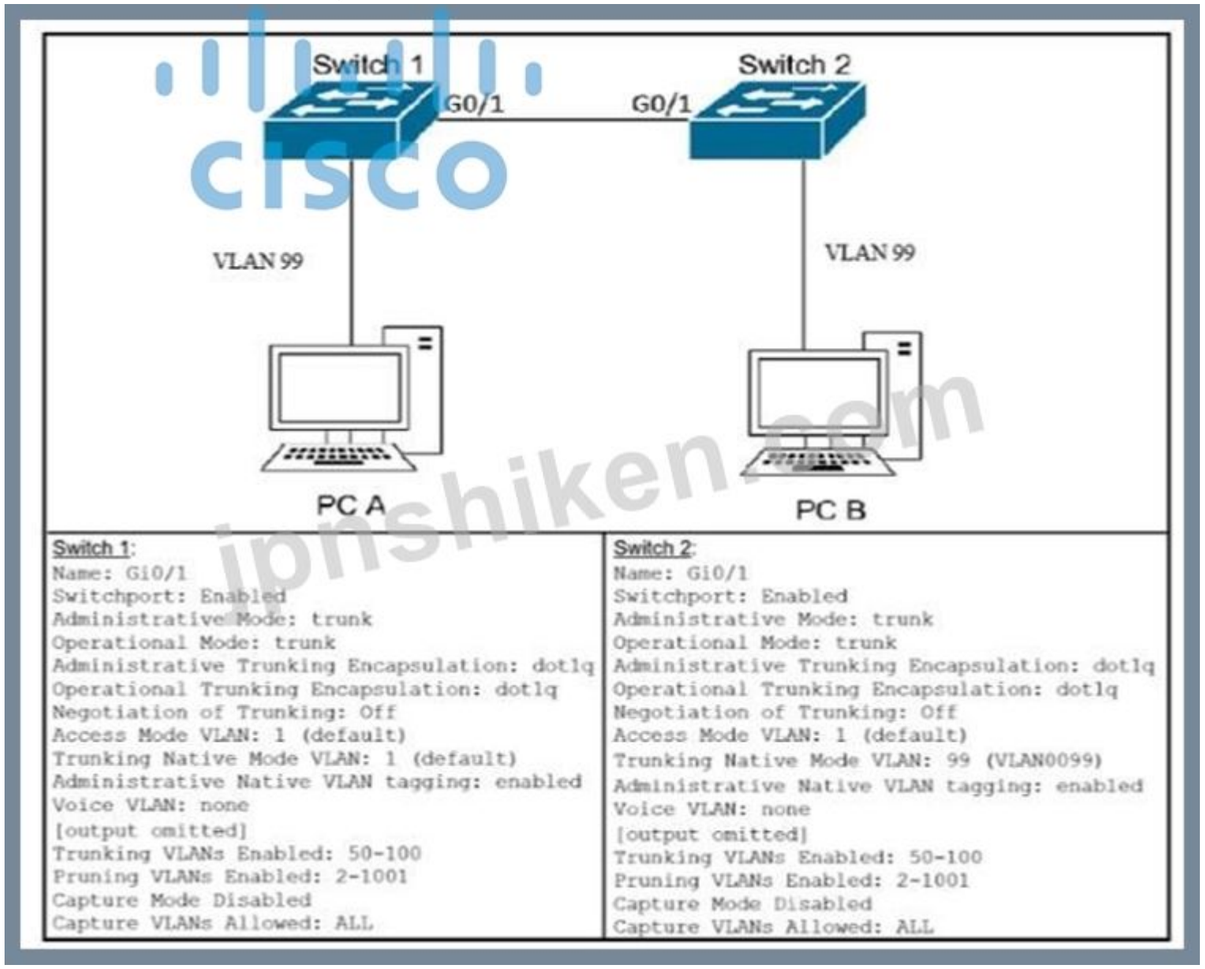
```
R2#show ip ospf interface
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 192.168.1.2
  Backup Designated Router (ID) 192.168.1.1, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 2/2, flood queue length 0
   Neighbor Count is 1, Adjacent neighbor count is 2
```

ルーター OldR は、ネットワーク上の別のルーターと交換され、OldR と R2 がルートを交換するようにすることを目的としています。エンジニアが初期 OSPF 設定を適用した後も、両方のデバイスでルートが欠落していました。ネイバー関係を有効にするために clear IP ospf process コマンドを入力する前に、どのコマンドシーケンスを発行する必要がありますか？

- OldR(config)#interface g0/0/0
  OldR(config-if)#ip ospf dead-interval 15
- OldR(config)#router ospf 1
  OldR(config-router)#no router-id 192.168.1.1
- OldR(config)#router ospf 1
  OldR(config-router)#network 192.168.1.0 255.255.255.0 area 2
- OldR(config)#interface g0/0/0
  OldR(config-if)#ip ospf hello-interval 15

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: (正解を表示します)
Option C. Routing and redundancy questions are solved by applying longest-prefix match, administrative distance, metrics, and gateway-redundancy behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Incorrect choices point to the wrong next hop, choose the wrong route source, or confuse routing with Layer 2 behavior. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

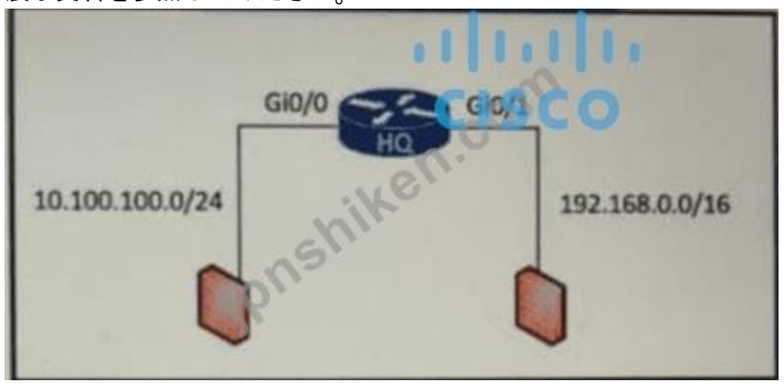
質問: **169**
添付資料を参照してください。



スイッチの設定後、スイッチ1の出力に基づくと、PC AとPC B間のpingテストが失敗します。
どのエラーを修正する必要がありますか？

A. ネイティブVLANの不一致があります
B. スイッチポートでアクセスモードが設定されています。
C. PCが間違ったVLANに接続されています
D. トランク上で全てのVLANが有効になっていません
正解: (正解を表示します)
The failure is caused by a native VLAN mismatch. On an 802.1Q trunk, traffic for the native VLAN is sent untagged by default. Both ends of the trunk must agree on which VLAN is native; otherwise, an untagged frame sent by one switch is placed into a different VLAN when it arrives on the other switch. That silently breaks traffic separation and can also create confusing reachability failures. Cisco switching guidance treats native VLAN consistency as a basic trunk requirement, and Cisco CCNA 200-301 v1.1 tests it as part of VLAN and trunk operation. Access-mode ports would be a different problem, but the exhibit points to a trunk inconsistency. The allowed VLAN list is also not the issue if the required VLANs are already carried. The fix is to configure the same native VLAN on both sides of the trunk, normally with switchport trunk native vlan < vlan-id > . The key clue is the mismatch between Switch 1 and Switch 2 native VLAN values.

質問: **170**
展示資料を参照してください。



インターフェース G0/0 上の任意のホストからのトラフィックを許可し、インターフェース G/0 からのトラフィックを拒否するには、アクセス リストが必要です。
/1. どのアクセスリストを適用する必要がありますか？

A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解: (正解を表示します)
The verified answer is A. The correct ACL option is the one that permits traffic arriving from G0/0 while denying traffic from G0/1 according to the exhibit direction. ACL placement and direction decide whether packets match at ingress or egress, so the selected list must be applied where the source interface condition is true. Cisco CCNA 200-301 v1.1 places this skill in Security Fundamentals, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. A list with reversed source logic or the wrong interface direction would either block valid

hosts or fail to block the unwanted traffic. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問**: 171**

図を参照してください。R1からISPへの接続にはIPv6を実装する必要があります。R1とISP間のアップリンクは手動割り当てで構成する必要があり、LANインターフェースは自己プロビジョニングする必要があります。両方の接続で、該当するIPv6ネットワークを使用する必要があります。R1に適用する必要がある2つの構成はどれですか？(2つ選択してください。)

A. インターフェース Gi0/1 ipv6 アドレス 2001:db8:0F1B:FCCB:ACCE:FCED:ABCD:FA02:/127
B. インターフェース Gi0/0ipv6 アドレス 2001:db8:1:AFFF::/64 eui-64
C. インターフェース Gi0/1ipv6 アドレス 2001:db8:0F1B:FCCB:ACCE:FCED:ABCD:FA00:/127
D. インターフェース Gi0/0ipv6 アドレス 2001:db8:0:AFFF::/64 eui-64
E. インターフェース Gi0/0ipv6 アドレス 2001:db8:0F1B:FCCB:ACCE:FCED:ABCD:FA03;/127

正解**: C,D (**コメントを発表する**)**

Answer C,D is correct: C. interface Gi0/1ipv6 addresss 2001:db8:0F1B:FCCB:ACCE:FCED:ABCD:FA00:
/127; D. interface Gi0/0ipv6 addresss 2001:db8:0:AFFF::/64 eui-64. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問**: 172**

どの出力がJSONデータ表現を表示しますか？

A.
```
{
  "response": {
  "taskId": {};
  "url": "string"
  };
  "version": "string"
}
```

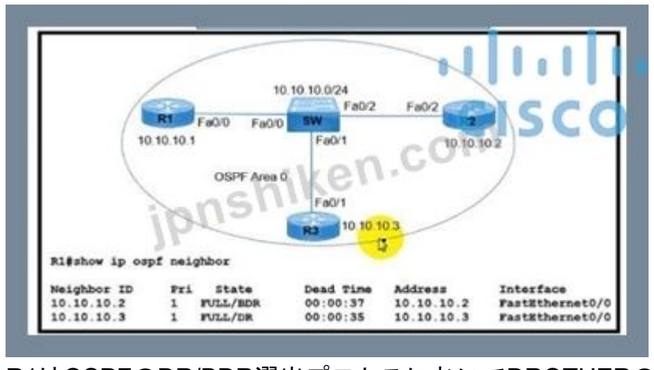
B.
```
{
  "response"- {
  "taskId"- {},
  "url"- "string"
  },
  "version"- "string"
}
```

C.
```
{
  "response": {
  "taskId": {},
  "url": "string"
  },
  "version": "string"
}
```

D.
```
{
  "response". {
  "taskId". {};
  "url". "string"
  };
  "version". "string"
}
```

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)
JSON represents data as structured name/value pairs, arrays, objects, strings, numbers, Booleans, and null values. In the exhibit, Option C is the output that follows JSON syntax: field names are enclosed in double quotes, values appear after colons, and objects or arrays are delimited with braces or brackets. XML would use opening and closing tags. YAML normally relies on indentation and key-value formatting without the same heavy brace structure. Plain text or CLI output does not follow a strict object model. Cisco CCNA v1.1 Automation and Programmability includes recognizing data formats used with APIs and automation tools.
That is the practical reason JSON appears so often in controller-based networking and REST APIs: it is compact, structured, and easy for software to parse. The key exam check is visual. If you see quoted keys, colons, braces, brackets, and comma-separated values arranged as objects or arrays, you are looking at JSON.

質問: **173**
展示資料を参照してください。



R1はOSPFのDR/BDR選出プロセスにおいてDROTHERの役割を担っています。R1がDRとして選出されるようにするには、エンジニアはどのような設定を実装する必要がありますか？

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

正解: (正解を表示します)

Option B. OSPF operation depends on area membership, network type, timers, router ID, priority, and whether a DR/BDR election occurs. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Incorrect choices either use the wrong OSPF role, omit a required adjacency condition, or apply a setting that does not affect the stated behavior. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **174**

キャンパス内の異なる建物内にそれぞれ設置された2つの独立したネットワークセグメントを無線で接続するには、どのアクセスポイントモードを使用すればよいですか？

A. メッシュ
B. ローカル
C. ブリッジ
D. ポイントツーポイント

正解: (正解を表示します)

bridge. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

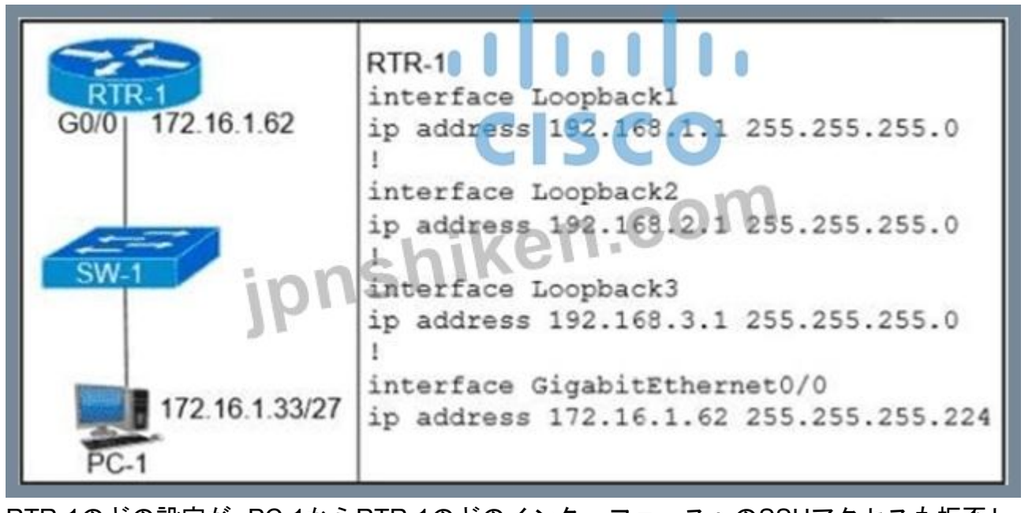
質問: **175**
ローカルAPモードとFlexConnect APモードの違いは何ですか？
A. ローカルAPモードでは、APごとにWLCへのCAPWAPトンネルが2つ作成されます。
B. APがWLCとの接続を失うと、FlexConnect APモードは機能しなくなります。
C. FlexConnect AP モードは、ローカルスイッチングが構成されている場合に、AP から WLC へのトラフィックをブリッジします。
D. ローカルAPモードでは、APは自律型APであるかのように動作します。
正解: **(**正解を表示します**)**
In local AP mode, a lightweight access point builds CAPWAP connectivity to the wireless LAN controller and normally sends both control and client data traffic through the controller. Cisco commonly describes this as separate CAPWAP control and data tunnels. FlexConnect mode is different because it is designed for remote or branch deployments where the AP may locally switch client data traffic instead of backhauling it all through the WLC. That is why option C is wrong: with local switching, FlexConnect bridges traffic locally, not from the AP to the WLC. FlexConnect can also continue serving clients during a WAN or controller outage, depending on configuration and authentication method, so option B is wrong. Local mode does not turn the AP into an autonomous AP; it remains controller-based. Cisco CCNA 200-301 v1.1 Network Access expects the distinction between centralized WLC forwarding and branch-friendly FlexConnect operation. The clearly correct difference in the options is A.

質問: **176**
エンドポイントの関数とは何ですか？
A. 個々のユーザーがネットワークサービスに直接アクセスするために使用します。
B. ネットワーク内のホスト間でユニキャスト通信を転送します。
C. 同じ VLAN 内のデバイス間でブロードキャスト トラフィックを送信します
D. ネットワークの信頼できるセクションと信頼できないセクション間のセキュリティを提供します。
正解: **A (**コメントを発表する**)**
It is used directly by an individual user to access network services. Security questions require distinguishing authentication, authorization, encryption, secure management, malware protection, and physical controls.
Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The wrong options apply the right security vocabulary to the wrong control or use weaker/deprecated protection. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **177**
Wi-Fiにおけるノイズはどのように定義されますか？
A. 無線機器から得られる信号対雑音比
B. ローカル信号に干渉する他のWi-Fiネットワークからの信号
C. 目的のWi-Fi信号と干渉するWi-Fi信号との差を測定した値
D. Wi-Fiトラフィック以外の干渉で、目的の信号を劣化させるもの
正解: **A (**コメントを発表する**)**
ratio of signal-to-noise rating supplied by the wirelesss device. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco- consistent configuration or behavior for this wireless scenario.

質問: **178**
3層ネットワークトポロジーを説明する2つの例を挙げてください。(2つ選択してください)
A. コア層とディストリビューション層は同じ機能を実行します
B. アクセス層は、異なるドメイン内のデバイス間のルーティングを管理します。
C. ネットワークコアは、デバイスが故障した場合でも継続的な接続を維持するように設計されています。
D. コア層は各ホストの有線接続を維持します
E. ディストリビューション層は、レイヤ2およびレイヤ3の技術を実行します。
正解: **(**正解を表示します**)**
Answer C,E is correct: C. The network core is designed to maintain continuous connectivity when devices fail.; E. The distribution layer runs Layer 2 and Layer 3 technologies. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Network Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **179**
展示資料を参照してください。

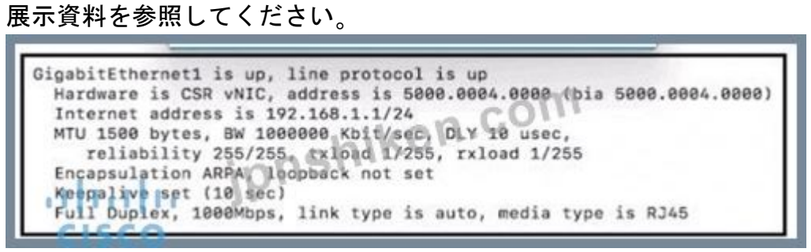


RTR-1のどの設定が、PC-1からRTR-1のどのインターフェースへのSSHアクセスも拒否し、その他のすべてのトラフィックを許可するのでしょうか？
A. access-list 100 deny tcp host 172.16.1.33 any eq 22 access-list 100 permit ip any anyinterface GigabitEthernet0/0 ip access-group 100 in
B. access-list 100 deny tcp host 172.16.1.33 any eq 22 access-list 100 permit ip any anyline vty 0 15 ip access-group 100 in
C. access-list 100 deny tcp host 172.16.1.33 any eq 23 access-list 100 permit ip any anyinterface GigabitEthernet0/0 ip access-group 100 in
D. access-list 100 deny tcp host 172.16.1.33 any eq 23 access-list 100 permit ip any anyline vty 0 15 ip access-group 100 in
正解: **B (**コメントを発表する**)**
The requirement is to block SSH management access from PC-1 to any RTR-1 interface while allowing other traffic. Applying the control to the VTY lines targets management sessions to the router itself. That is cleaner than placing an interface ACL on only one routed interface, because the question says any RTR-1 interface.
SSH uses TCP port 22, so the deny statement must match tcp host 172.16.1.33 any eq 22, followed by permit ip any any to avoid an implicit deny blocking everyone else. Telnet would use TCP port 23, so options that deny port 23 do not satisfy an SSH requirement. Cisco CCNA 200-301 v1.1 Security Fundamentals expects candidates to know the difference between filtering transit traffic on interfaces and

restricting administrative access through VTY lines. The correct design is an ACL that denies PC-1 SSH to any router address and then permits other traffic, applied inbound to the VTY access path. That matches option B.

質問: **180**
スイッチにおけるフレーム切り替えはどのように機能するのですか？
A. CDPを使用してフレームを隣接ポートに転送します
B. 既知の送信元 VLAN を含むフレームを変更します
C. 未知の送信元からのフレームを検査して破棄します
D. 既知の宛先を宛先ポートに転送します
正解: **D** (コメントを発表する)
forwards known destinations to the destination port. Switching questions depend on MAC learning, VLAN membership, trunking, STP election, and EtherChannel behavior. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong answers misapply a Layer 2 rule or configure the wrong logical interface. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

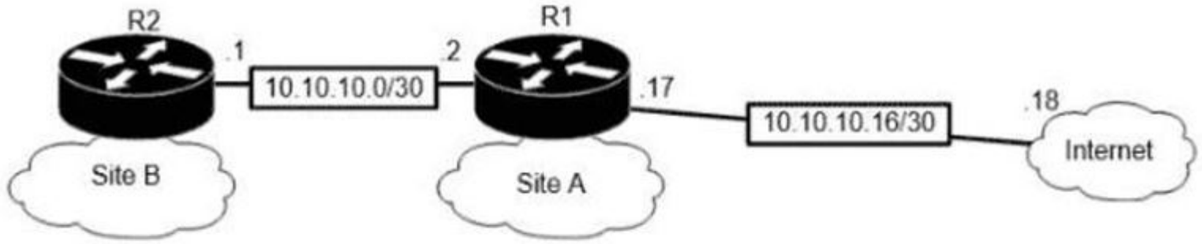
質問: **181**
展示資料を参照してください。



ネットワーク2001:db8::/64の修正EUI-64 IPv6インターフェースアドレスに一致するフォーマットはどれですか？
A. 2001 :db8::5000:0004:5678:0090/64
B. 2001 :db8:4425:5400:77ft:fe07:/64
C. 2001 :db8::5000:00ff:fe04 0000/64
D. 2001 :db8::5200:00ff:fe04:0000/64
正解: **C** (コメントを発表する)
2001 :db8::5000:00ff:fe04 0000/64. Network fundamentals questions require recognizing address structure, media characteristics, virtualization roles, frequency units, and topology tradeoffs. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. The incorrect choices may sound plausible but do not match the physical, logical, or mathematical property being tested. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **182**
展示資料を参照してください。



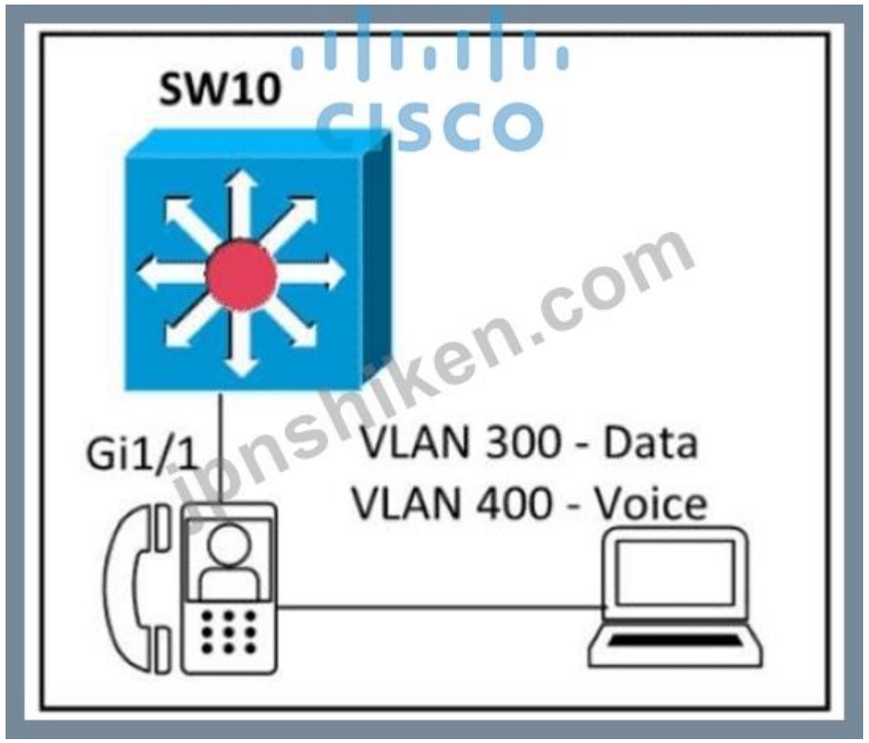

```
R2#sh run | b router ospf
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 network 10.10.10.1 0.0.0.0 area 0
 network 10.10.13.1 0.0.0.0 area 0

R2#show ip route
Gateway of last resort is not set
 10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C     10.10.10.0/30 is directly connected
C     10.10.13.0/25 is directly connected, Vlan20
C     10.10.13.144/28 is directly connected, Vlan40
```

```
R1#show ip route
Gateway of last resort is not set
 10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C     10.10.10.0/30 is directly connected, FastEthernet0/1
O     10.10.13.0/25 [110/6576] via 10.10.10.1, 01:37:03
C     10.10.10.16/30 is directly connected, FastEthernet0/24
O     10.10.13.144/28 [110/110] via 10.10.10.1, 01:37:03

R1#sh run | b router ospf
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 network 10.10.10.2 0.0.0.0 area 0
 default-information originate
```

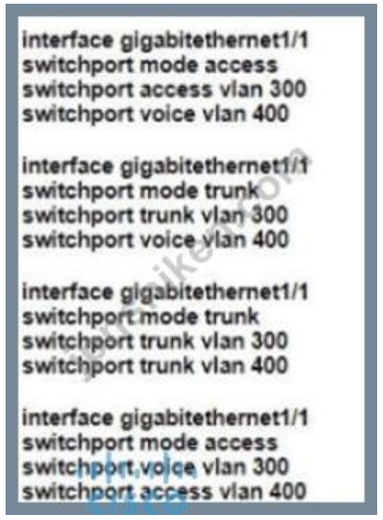
R1 OSPF 設定で default-information originate コマンドが設定されています。テスト後、サイト B の VLAN 20 上のワークステーションがインターネット上の DNS サーバーに到達できません。どの操作で設定の問題を修正できますか？

A. R2 に default-information originate コマンドを追加します
B. R1でip route 0.0.0.0 0.0.0.0 10.10.10.18コマンドを設定します。
C. R2でip route 0.0.0.0 0.0.0.0 10.10.10.2コマンドを設定します。
D. R1 の default-information originate コマンドに always キーワードを追加します
正解: **(**正解を表示します**)**
Configure the ip route 0.0.0.0 0.0.0.0 10.10.10.18 command on R1. OSPF behavior is controlled by interface state, area, timers, network type, cost, priority, router ID, and neighbor/adjacency rules. Cisco CCNA 200-301 v1.1 includes this under IP Services, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The distractors confuse OSPF with unrelated metrics, local-only process values, or parameters that do not satisfy the adjacency or route-selection requirement. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **183**
展示資料を参照してください。



エンジニアは、音声およびデータトラフィックに対応するためにGigabitEthernet1/1を構成する必要があります。このタスクを実行する構成はどれですか？



```
interface gigabitethernet1/1
switchport mode access
switchport access vlan 300
switchport voice vlan 400

interface gigabitethernet1/1
switchport mode trunk
switchport trunk vlan 300
switchport voice vlan 400

interface gigabitethernet1/1
switchport mode trunk
switchport trunk vlan 300
switchport trunk vlan 400

interface gigabitethernet1/1
switchport mode access
switchport voice vlan 300
switchport access vlan 400
```

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: (正解を表示します)

Option A. The answer follows directly from normal Cisco device behavior and the wording of the scenario.

Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **184**
展示資料を参照してください。

管理者は音声VLANの設定を担当しています。Cisco電話機をスイッチのGigabitEthernet3/1/4ポートに接続した場合、どのような結果が予想されますか？
A. 電話機と、電話機に接続されているワークステーションは、VLAN接続がありません。
B. 電話機と電話機に接続されたワークステーションは、VLAN 50でデータを送受信します。
C. 電話機はVLAN 50でデータの送受信を行いますが、電話機に接続されているワークステーションにはVLAN接続がありません。
D. 電話機はVLAN 50でデータを送受信しますが、電話機に接続されたワークステーションはVLAN 1でデータを送受信します。
正解: **(正解を表示します)**
The phone sends and receives data in VLAN 50, but a workstation connected to the phone sends and receives data in VLAN 1. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

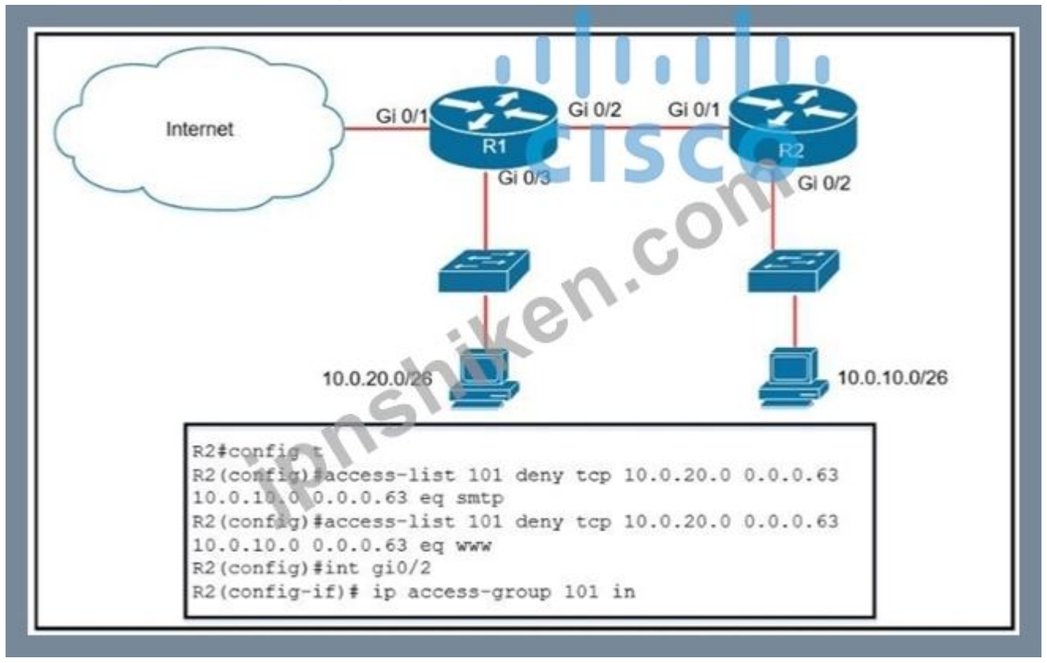
質問: **185**
2 つのレイヤ 2 スイッチ間には物理的な接続が実装されています。
また、両者間のネットワーク接続を設定する必要があります。
I. LACP EtherChannel を設定し、番号を 44 とします。
スイッチ SWI と SW2 間で EthernetO/O インターフェースを使用し、
両端ともEthernet0/1ポートを使用している。LACPモードは両端で一致している必要がある。
2. EtherChannelをトランクリンクとして設定します。
3. トランクリンクを 802.lq タグで構成します。
4. VLAN「MONITORING」をタグなしVLANとして設定します。
イーサチャネル。
ガイドライン
これは、仮想デバイス上でタスクを実行する実験課題です。
* この実験項目のタスクを確認するには、「タスク」タブを参照してください。
* デバイスコンソールにアクセスしてタスクを実行するには、「トポロジー」タブを参照してください。

* コンソールへのアクセスは、デバイスアイコンをクリックするか、コンソールウィンドウの上にあるタブを使用することで、必要なすべてのデバイスで利用できます。
必要な事前設定はすべて完了しました。
* デバイスの有効化パスワードやホスト名を変更しないでください。
次の項目に進む前に、設定をNVRAMに保存してください。
* 画面下部の 「次へ」をクリックして、この実験を提出し、次の問題に進んでください。
* 「次へ」をクリックすると、ラボが閉じられ、再度開くことはできません。

正解:
Solution is given below explanation.
Explanation:
To configure an LACP EtherChannel and number it as 44, configure it between switches SW1 and SW2 using interfaces Ethernet0/0 and Ethernet0/1 on both sides, configure the EtherChannel as a trunk link, configure the trunk link with 802.1q tags, and configure VLAN 'MONITORING' as the untagged VLAN of the EtherChannel, you need to follow these steps:
On both SW1 and SW2, enter the global configuration mode by using the configure terminal command.
On both SW1 and SW2, select the two interfaces that will form the EtherChannel by using the interface range ethernet 0/0 - 1 command. This will enter the interface range configuration mode.
On both SW1 and SW2, set the protocol to LACP by using the channel-protocol lacp command.
On both SW1 and SW2, assign the interfaces to an EtherChannel group number 44 by using the channel- group 44 mode active command. This will create a logical interface named Port-channel44 and set the LACP mode to active on both ends. The LACP mode must match on both ends for the EtherChannel to form.
On both SW1 and SW2, exit the interface range configuration mode by using the exit command.
On both SW1 and SW2, enter the Port-channel interface configuration mode by using the interface port- channel 44 command.

On both SW1 and SW2, configure the Port-channel interface as a trunk link by using the switchport mode trunk command.
On both SW1 and SW2, configure the Port-channel interface to use 802.1q tags for VLAN identification by using the switchport trunk encapsulation dot1q command.
On both SW1 and SW2, configure VLAN 'MONITORING' as the untagged VLAN of the Port-channel interface by using the switchport trunk native vlan MONITORING command.
On both SW1 and SW2, exit the Port-channel interface configuration mode by using the exit command.
On both SW1 and SW2, save the configuration to NVRAM by using the copy running-config startup-config command.

質問: **186**
SDN 環境でのネットワーク管理の自動化によってもたらされる 2 つの改善点は何ですか? (2つ選んでください)
A. データ収集および分析ツールは、ネットワークのベースラインを確立します
B. 人工知能は、潜在的な設計の失敗を特定して防止します。
C. 機械学習は、トラブルシューティング プロセスを自動化する際の全体的なエラー率を最小限に抑えます
D. 最小限の労力で新しいデバイスをオンボーディング
E. シスコ独自の API は、複数のネットワーク管理ツールを活用します。
正解: **(正解を表示します)**
The verified answer is A and D. Automation improves network management by collecting data for baselines and onboarding new devices with less manual work. In SDN and controller-based environments, telemetry and automated workflows reduce repetitive CLI work and improve consistency. Cisco CCNA 200-301 v1.1 places this skill in Automation and Programmability, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. The answer set overstates AI prevention and proprietary APIs; useful automation is mainly repeatable provisioning, validation, telemetry, and analysis. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **187**
展示資料を参照してください。


拡張ACLがルーターR2に設定され、適用されました。設定は意図どおりに機能しませんでした。10.0.10 0/26サブネットから10.0.20 0 26へのTCPポート25と80の送信トラフィックを停止しつつ、他のすべてのトラフィックを許可する2つの変更はどれですか？(2つ選択してください)

A. 許可されたトラフィックのために、ACL 101 の先頭に 「permit ip any any」ステートメントを追加します。

B. 許可されたトラフィックのために、ACL 101 の末尾に 「permit ip any any」ステートメントを追加します。

C. ACL 101では送信元IPアドレスと宛先IPアドレスを入れ替える必要があります

D. ACLはR1のGi0/2インターフェースのインバウンドに設定する必要があります。

E. ACL を R2 の Gi0/1 インターフェイスのアウトバウンドに移動する必要があります

正解: **(**正解を表示します**)**

The ACL failed because the packet direction and address roles were wrong, and because an explicit permit is needed after the deny statements. Extended ACL syntax follows source first, then destination. To block traffic from 10.0.10.0/26 going to 10.0.20.0/26 on TCP ports 25 and 80, the source must be the 10.0.10.0 subnet and the destination must be the 10.0.20.0 subnet. If those are reversed, the ACL is matching return traffic or the wrong flow. After the denies, a permit ip any any statement is required at the end; otherwise the implicit deny at the end of every ACL blocks all remaining traffic. The permit must not be placed at the beginning, because ACLs are processed top-down and an early permit would bypass the intended denies. Cisco CCNA v1.1 Security Fundamentals includes ACL behavior, direction, and ordering. The operational fix is therefore to swap source/destination and add the final permit.

質問: **188**

SSIDS の仕様は何ですか?

A. これらはシスコ独自のセキュリティ機能です。

B. 1 つの数字と 1 つの文字を含める必要があります。

C. スイッチ上で VLAN を定義します。

D. 大文字と小文字が区別されます。

正解: **D (**コメントを発表する**)**

They are case sensitive.. Wireless questions require separating client association, RF design, AP mode, WLAN security, and controller policy. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Incorrect answers usually confuse an encryption method with authentication, or a controller feature with a switchport feature. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **189**

仮想マシンの操作を説明するものは何ですか?

A. 仮想マシンは、ホスト ハードウェア リソースの管理と割り当てを担当します。

B. 仮想マシン環境では、物理サーバーは一度に 1 つのオペレーティング システムを実行する必要があります。

C. 仮想マシンは、仮想環境をサポートする物理ハードウェアです。

D. 仮想マシンは、サーバー ハードウェアから切り離されたオペレーティング システム インスタンスです。

正解: **(**正解を表示します**)**

Answer D is the technically correct selection. Virtual machines are operating system instances decoupled from the physical server hardware. The hypervisor presents virtual CPU, memory, disk, and NIC resources so multiple VMs can run on one host. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. The VM does not manage host resources itself, and the physical server can run multiple OS instances concurrently through virtualization. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

質問: **190**
FHRPを使用するメリットは何ですか？
A. ネットワークルーターの管理オーバーヘッドを削減
B. 複数のゲートウェイ間でトラフィックを負荷に応じて分散する
C. 可用性の度合いが高い
D. ネットワーク上のARPトラフィックを削減
正解: (正解を表示します)
The correct response is C. FHRPs improve availability by providing automatic default-gateway redundancy.
If the active gateway fails, another router can take over the virtual IP and MAC so hosts keep using the same default gateway. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. They do not primarily reduce management overhead, reduce ARP, or perform proportional load balancing in every implementation. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

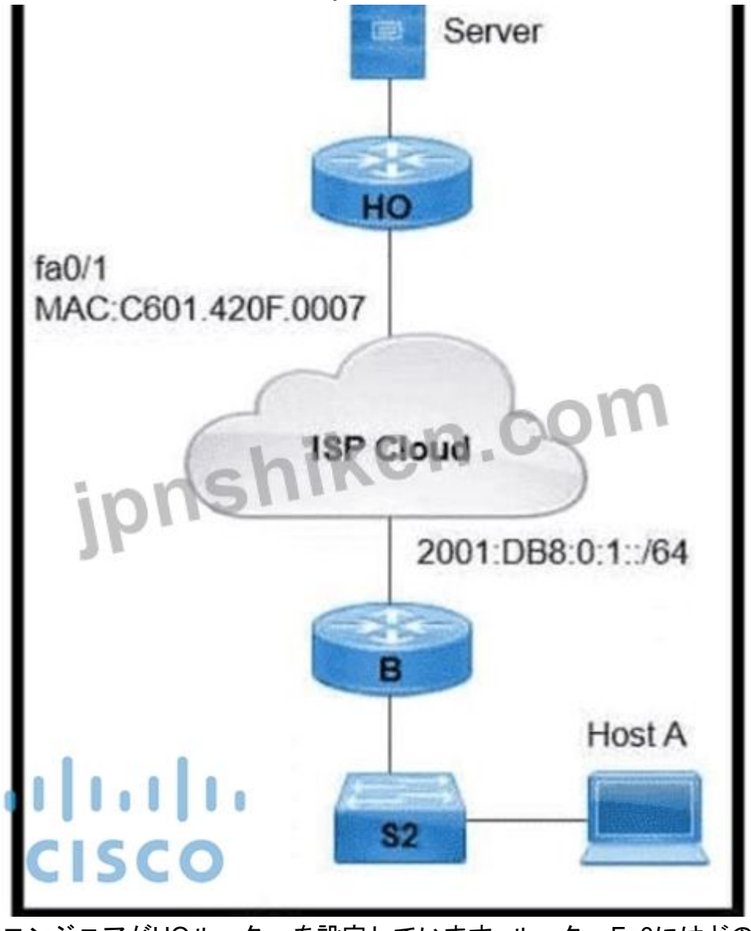
質問: **191**
次世代 IPS 向け Cisco Advanced Malware Protection の機能は何ですか?
A. 侵害された可能性のあるワイヤレス トラフィックの承認
B. 特定のファイルとファイル タイプのマルウェアの検査
C. エンド ユーザーの認証
D. URL フィルタリング
正解: (正解を表示します)
inspecting specific files and file types for malware. Wireless design and security require separating AP mode, WLAN identity, RF behavior, authentication, and encryption. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The distractors confuse wireless standards, security mechanisms, controller settings, or RF design practices. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **192**
スイッチは DHCP スヌーピング情報をどこに維持しますか?
A. MAC アドレス テーブル内
B. CAM テーブル内
C. 結合データベース内
D. フレーム転送データベース内
正解: (正解を表示します)
in the binding database. IP services questions test the exact function of infrastructure services such as addressing, name resolution, time synchronization, logging, monitoring, and secure management. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces.
The distractors name valid services, but they provide a different service function from the one required in the prompt. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **193**

WLCで使用した場合、どの機能を使用すると、WLCの配信システムポートを1つの802.3adグループにまとめることができますか？
A. QinQ
B. ISL
C. PAgP
D. ラグ
正解: **D** (コメントを発表する)
LAG. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **194**
展示資料を参照してください。

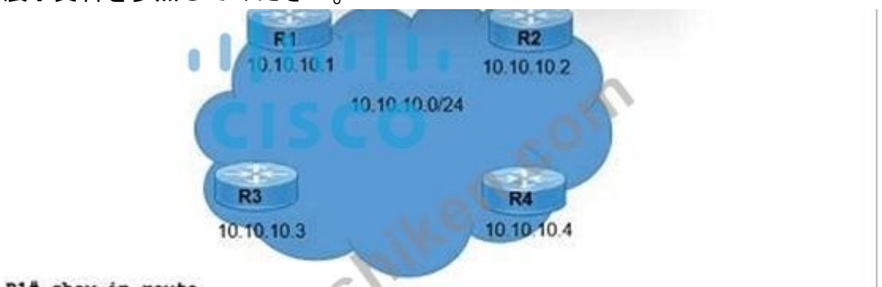


jpnshiken.com

エンジニアがHOルーターを設定しています。ルーターFa0にはどのIPv6アドレス設定を適用する必要がありますか？
ルーターが自身に固有の64-brt IPv6アドレスを割り当てるための/1インターフェース？
A. IPv6アドレス 2001:DB8:0:1:C601:42FF:FE0F:7/64

B. IPv6アドレス 2001:DB8:0:1:C601:42FE:800F:7/64
C. IPv6アドレス 2001 :DB8:0:1:FFFF:C601:420F:7/64
D. iov6 アドレス 2001 :DB8:0:1:FE80:C601:420F:7/64
正解: (正解を表示します)
ipv6 address 2001:DB8:0:1:C601:42FF:FE0F:7/64. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

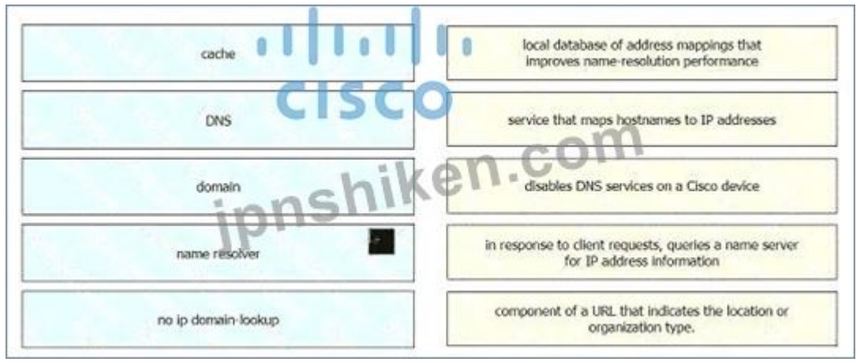
質問: **195**
展示資料を参照してください。



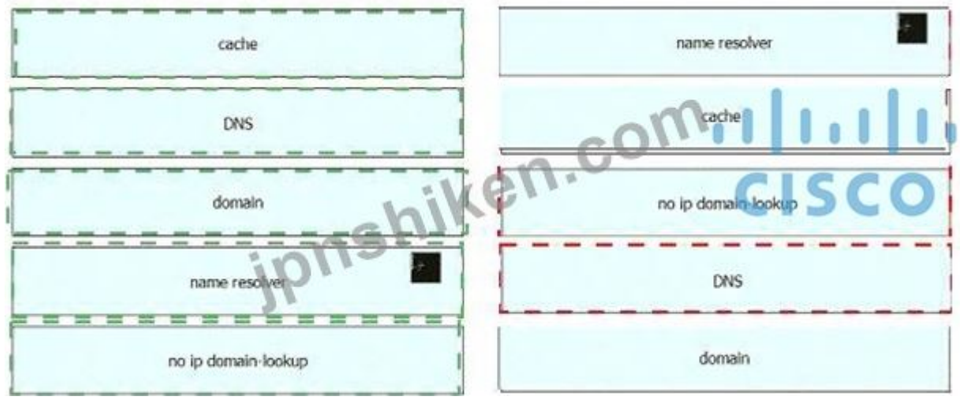

```
R1# show ip route
C    1.0.0.0/8 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O       10.10.10.3/32 [110/100] via 10.10.10.3, 00:39:08, Gigabitethernet0/3
C       10.10.10.0/24 is directly connected, Gigabitethernet0/0
O       10.10.10.2/32 [110/5] via 10.10.10.2, 00:39:08, Gigabitethernet0/2
R       10.10.10.4/32 [120/10] via 10.10.10.4, 00:39:08, Gigabitethernet0/4
```

R1から送信された場合、次ホップIPアドレスのうち、最も望ましくないメトリックを持つものはどれですか？
A. 10.10.10.5
B. 10.10.10.3
C. 10.10.10.4
D. 10.10.10.2
正解: **C** (コメントを発表する)
10.10.10.4. The answer follows from standard Cisco behavior and the operational clue in the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The other choices describe related terms, but they do not satisfy the requirement stated in the prompt. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **196**
左側のDNSルックアップコンポーネントを、右側の関数にドラッグアンドドロップしてください。

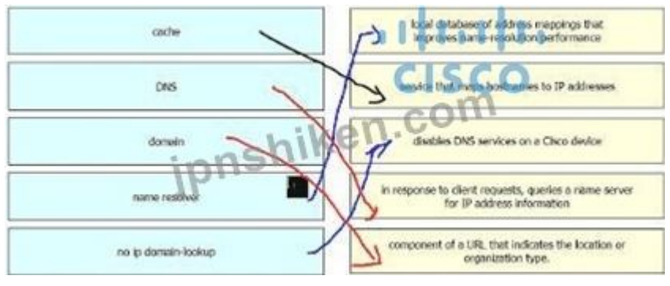


正解:



Explanation:

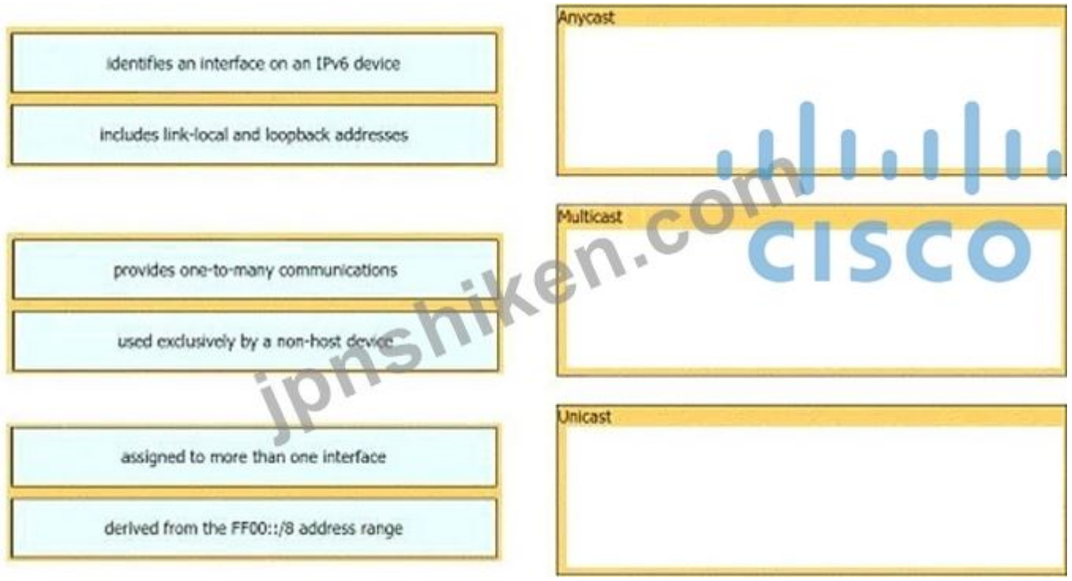
The verified answer is the displayed drag-and-drop mapping. DNS lookup components include the client resolver, recursive resolver, authoritative servers, record types, and query/response flow. Each component has a distinct function in translating names into usable addressing information. Cisco CCNA 200-301 v1.1 places this skill in IP Services, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. The usual mistake is treating every DNS server as authoritative for every name; recursive and authoritative roles are different. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.



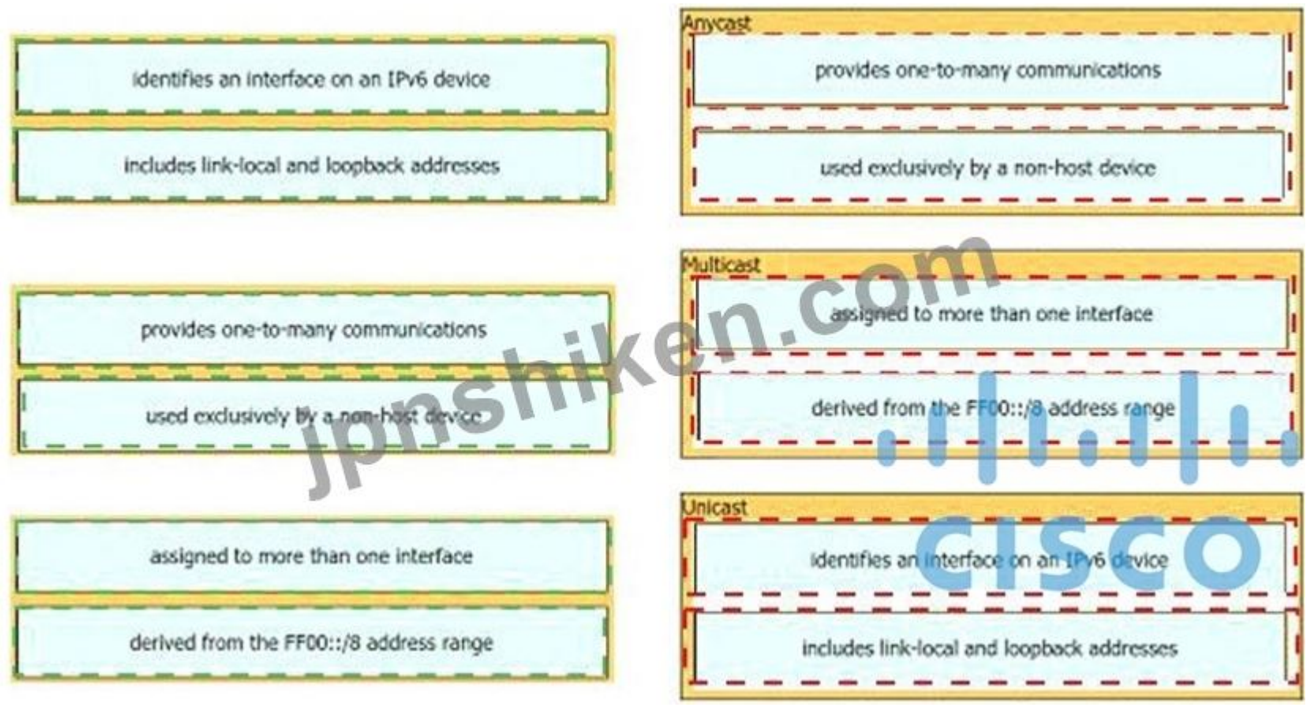
有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **197**

左側のIPv6アドレスの詳細を、右側の対応するタイプにドラッグアンドドロップしてください。



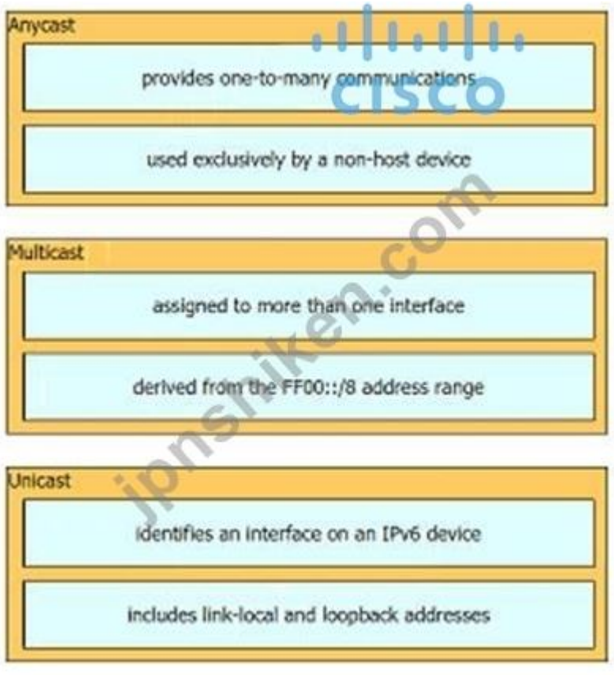
正解:



Explanation:

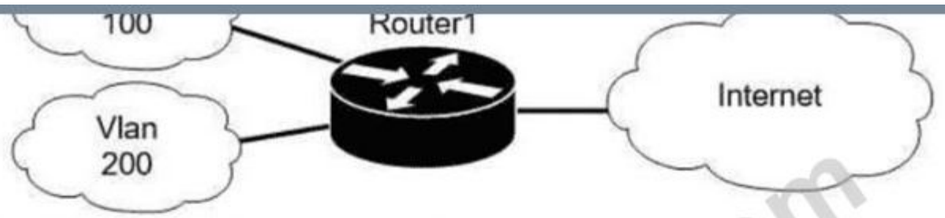
Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and

automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.



質問: **198**
リモートアクセスVPNの機能は何ですか？
A. 暗号化トンネリングを使用して複数のユーザーのデータのプライバシーを同時に保護
B. ユーザーが会社の内部ネットワークに接続している場合にのみ使用されます
C. 2つのブランチサイト間に安全なトンネルを確立します
D. ユーザーが安全なトンネルを介して社内ネットワークリソースにアクセスできるようにします
正解: **(**正解を表示します**)**
A remote access VPN allows individual users to connect securely to internal company resources over an untrusted network such as the Internet. The user runs a VPN client or uses a supported remote-access method, authenticates, and receives encrypted tunnel access to permitted internal services. That is different from a site- to-site VPN, which connects two networks such as branch and headquarters. The answer choice about multiple users simultaneously is too vague and does not identify the remote-access purpose. The option saying it is used exclusively while already on the internal network is wrong; the point is remote connectivity. Cisco CCNA 200-301 v1.1 Security Fundamentals covers VPN concepts because engineers must distinguish remote- access VPNs, site-to-site VPNs, IPsec, and tunneling behavior. The best definition is that remote access VPN allows users to access internal company network resources through a secure tunnel. The correct answer is D.

質問: **199**
展示資料を参照してください。




```
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#ip address 209.165.200.225 255.255.255.224
Router1(config-if)#ip nat outside
Router1(config)#interface GigabitEthernet0/1
Router1(config-if)#ip nat inside
Router1(config)#interface GigabitEthernet0/1.100
Router1(config-if)#encapsulation dot1Q 100
Router1(config-if)#ip address 10.10.10.1 255.255.255.0
Router1(config)#interface GigabitEthernet0/1.200
Router1(config-if)#encapsulation dot1Q 200
Router1(config-if)#ip address 10.10.20.1 255.255.255.0
Router1(config)#ip access-list standard NAT_INSIDE_RANGES
Router1(config-std-nacl)#permit 10.10.10.0 0.0.0.255
Router1(config)#ip nat inside source list NAT_INSIDE_RANGES interface GigabitEthernet0/0 overload
```

既存のVLAN 100のユーザーはインターネット上のサイトにアクセスできます。VLAN 200のユーザーがインターネットに接続できるようにするには、管理者はどのような操作を行う必要がありますか？

A. ルーター上でNATプールを定義します。

B. VLAN 200 の静的 NAT 変換を設定します。

C. VLAN 200 用に別のインターフェースで ip nat outside コマンドを設定します。

D. NAT INSIDF RANGFS ACL を更新します

正解: **B (**コメントを発表する**)**

Configure static NAT translations for VLAN 200.. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **200**

図を参照してください。支店のユーザーが、アプリケーションのパフォーマンスの問題、VoIP音声品質の低下、ダウンロード速度の低下を経験しています。これらの問題の原因は何ですか？

A. ブロードキャストストーム

B. 過剰利用

C. インターフェース設定

D. QoSキューイング

正解: (正解を表示します)

QoS queuing. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

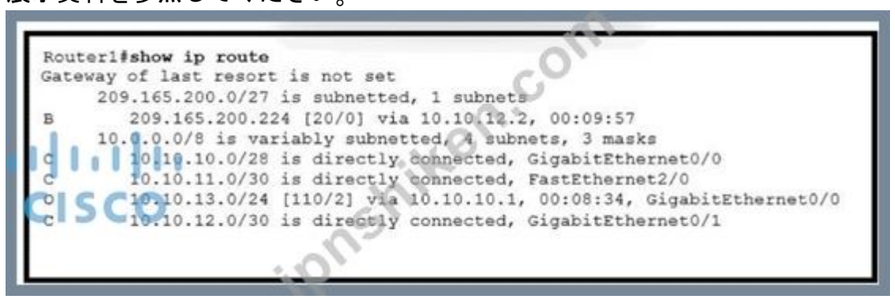
質問: **201**

左側のIPv6アドレスを、右側の対応するアドレスタイプにドラッグアンドドロップしてください。

正解:

Explanation:
Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.

質問: **202**
展示資料を参照してください。



パケットの送信元が10.10.10.2で、宛先が10.10.10.16の場合、ルーターはどのような動作をしますか？
A. 経路が学習されるのを待っているパケットをキューに入れます。
B. 学習したすべてのネクストホップにパケットをフラッディングします。
C. パケットを破棄します。
D. 宛先アドレスに似たルートを使用します。

正解: (正解を表示します)
It uses a route that is similar to the destination address.. IP services questions require matching the service to its exact operational role, such as logging, address assignment, file transfer, monitoring, redundancy, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The distractors are real technologies, but they solve different infrastructure problems. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **203**
添付資料を参照してください。

受信した設定エラーメッセージを説明しているのは、次のうちどれですか？
A. ブロードキャストIPアドレスです
B. ルーターは /28 マスクをサポートしていません。
C. プライベートIPアドレス範囲に属します。
D. これはネットワークIPアドレスです。
正解: (正解を表示します)
The configured address 192.168.16.143 with a /28 mask is the broadcast address of its subnet, so the router correctly rejects it with a bad-mask message. A /28 mask creates blocks of 16 addresses. In the 192.168.16.128
/28 subnet, the usable host range is 192.168.16.129 through 192.168.16.142, and 192.168.16.143 is the directed broadcast address. A broadcast address cannot be assigned to a router interface because it represents all hosts in that subnet, not one device. The issue is not that the router lacks /28 support, and it is not caused by private addressing. It is also not the network address; the network address would be 192.168.16.128.
CCNA 200-301 v1.1 Network Fundamentals requires precise subnet boundary recognition. The verified answer is A because the address shown in the exhibit is the subnet broadcast address. Reference: Cisco IPv4 subnetting fundamentals and interface address validation behavior.

質問: **204**
WPA3 で使用される暗号化方式はどれですか?
A. PSK
B. TKIP
C. さえ
D. AES
正解: (正解を表示します)
AES. Wireless design and security require separating AP mode, WLAN identity, RF behavior, authentication, and encryption. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command.
The distractors confuse wireless standards, security mechanisms, controller settings, or RF design practices.
In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **205**
クラウドベースのネットワーク トポロジの特徴は何ですか?
A. ワイヤレス接続は、サービスへの唯一のアクセス方法を提供します
B. オンサイト ネットワーク サービスは、物理的なレイヤー 2 およびレイヤー 3 コンポーネントで提供されます。
C. サービスは、パブリック、プライベート、またはハイブリッド展開によって提供されます
D. 物理ワークステーションはリソースを共有するように構成されています
正解: (正解を表示します)
Use C for this item. Cloud-based topology delivers services through public, private, or hybrid cloud deployment models. The defining characteristic is that compute, storage, applications, or network services are consumed from cloud infrastructure rather than only local physical equipment. In Cisco CCNA 200-301 v1.1, Network Fundamentals questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. Wireless access is not the sole method, and on-site Layer 2/Layer 3 components describe local infrastructure rather than cloud topology. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **206**
展示資料を参照してください。

10.0.1.5 をホストとするトラフィックの次のホップアドレスは何ですか？
A. 10.0.1.3
B. 10.0.1.50
C. 10.0.1.4
D. ループバック D
正解: (正解を表示します)
The router forwards traffic based on the best matching route in the routing table. For a destination host such as
10.0.1.5, the router compares available prefixes and selects the route with the longest matching prefix. After selecting the route, it forwards the packet to the next-hop address listed for that route, not necessarily to the final destination directly. In this exhibit, the route that includes 10.0.1.5 points to 10.0.1.50 as the next hop.
That makes 10.0.1.50 the Layer 3 neighbor to which the packet is sent next. Cisco CCNA 200-301 v1.1 IP Connectivity expects engineers to read routing output accurately: destination prefix, administrative distance, metric, next-hop address, outgoing interface, and route source all have separate meanings. A loopback label is not a next-hop IP address, and nearby addresses in the same range are not automatically correct. The next hop is the one installed in the matching route entry, so B is correct.

質問: **207**
ルーターが通知レベルのメッセージをsyslogサーバーに送信した場合、どのようなイベントが発生したことになりますか？
A. ICMP接続が確立されました
B. 証明書の有効期限が切れています
C. インターフェースラインの状態が変更されました
D. TCP接続が切断されました
正解: (正解を表示します)

An interface line has changed status. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol.
First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **208**
ピュア IPsec で送信されるトラフィックの種類は?
A. いくつかのリモート サイトの 1 つで MAC アドレスを見つけようとしているスイッチからのブロードキャスト パケット
B. あるサイトのサーバーから別の場所のホストへのマルチキャスト トラフィック
C. 2 つの異なるサイトにあるスイッチ間のスパニング ツリーの更新
D. リモート サイトのホストから本社のサーバーへのユニキャスト メッセージ
正解: (正解を表示します)
unicast messages from a host at a remote site to a server at headquarters. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Security Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **209**
単一のネットワーク デバイスでクライアント モードの信頼できるサーバーに NTP を構成するには、どの 2 つのタスクを実行する必要がありますか? (2つ選んでください)
A. NTP 認証を有効にします。
B. タイムゾーンを確認します。
C. NTP ブロードキャストを無効にします
D. NTPサーバーのIPアドレスを指定
E. NTP サーバーの秘密鍵を設定します
正解: (正解を表示します)
Answer A,D is correct: A. Enable NTP authentication.; D. Specify the IP address of the NTP server. IP services questions test the exact function of infrastructure services such as addressing, name resolution, time synchronization, logging, monitoring, and secure management. Cisco CCNA 200-301 v1.1 includes this topic under IP Services, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The distractors name valid services, but they provide a different service function from the one required in the prompt. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **210**
syslogメッセージを伝送するトランスポート層プロトコルはどれですか？(2つ選択してください。)
A. UDP

B. RTP
C. TCP
D. IP
E. ARP
正解: (正解を表示します)
Answer A,C is correct: A. UDP; C. TCP. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **211**

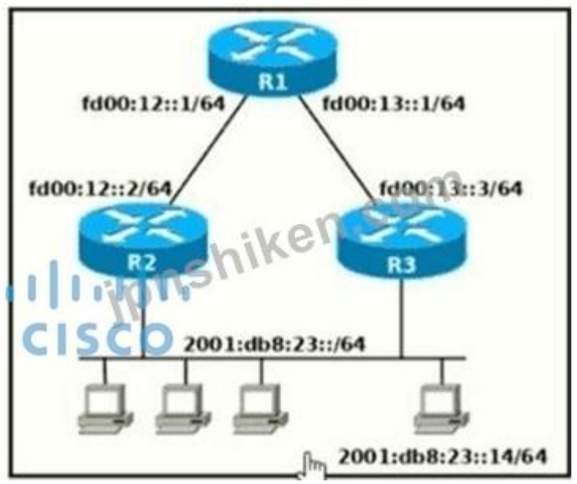
```
switchport mode trunk
switchport trunk allowed vlan 100,200,300
channel-group 1 mode active

SW1#show run interface fastEthernet 0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 100,200
channel-group 1 mode active

SW2#show run interface fastEthernet 0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 100,200,300
channel-group 1 mode active

SW2#show run interface fastEthernet 0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 100,200,300
channel-group 1 mode active
```

図を参照してください。エンジニアがSW1とSW2の間に新しいレイヤ2 LACP EtherChannelを構築しており、作業を確認するために指定されたshowコマンドを実行しました。スイッチがLACPポートチャネルで2番目のメンバーを正常にバンドルするために、他にどのようなタスクを実行する必要がありますか？
A. SW1ポートチャネル1でswitchport trunk allowed vlan 300コマンドを設定します。
B. SW1 のインターフェース Fa0/2 で switchport trunk allowed vlan 300 コマンドを設定します。
C. SW2 のインターフェース Fa0/2 で switchport trunk allowed vlan add 300 コマンドを設定します。
D. SW1 ポートチャネル 1 で switchport trunk allowed vlan add 300 コマンドを設定します。
正解: (正解を表示します)

Configure the switchport trunk allowed vlan add 300 command on SW1 port-channel 1. EtherChannel configuration should be applied to the logical port-channel interface for trunk VLAN policy after the bundle exists. Adding VLAN 300 to the port-channel preserves existing allowed VLANs and updates the logical link consistently. Applying the command only to a physical member interface can create inconsistent configuration between the member and the port-channel. Replacing the allowed list instead of using add could also remove existing VLANs and interrupt traffic. Cisco CCNA 200-301 v1.1 Network Access expects engineers to configure EtherChannel as one logical interface once the channel is formed. The corrected answer is to configure switchport trunk allowed vlan add 300 on SW1 port-channel 1. That updates the trunk safely and avoids per-member inconsistency.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **212**
展示資料を参照してください。



ルーター R1 で設定した場合、これらの要件を満たすコマンドはどれですか？(2 つ選択してください。)ネットワーク 2001:db8:2::/64 全体宛てのパケットは、ルーター R2 を経由して転送する必要があります。
ホスト2001:db8:23::14宛てのパケットは、できればR3を経由して転送する必要があります。

A. IPv6 ルート 2001:db8:23::/128 fd00:12::2
B. IPv6 ルート 2001:db8:23::14/128 fd00:13::3
C. IPv6 ルート 2001:db8:23::14/64 fd00:12::2
D. IPv6 ルート 2001:db8:23::/64 fd00:12::2
E. IPv6 ルート 2001:db8:23::14/64 fd00:12::2 200

正解: (正解を表示します)

Use D and E for this item. The route for the broader IPv6 network points traffic through R2, while a more specific or preferred host route can influence traffic for the individual host. Routers use longest-prefix match first, and administrative distance can make a route backup or less preferred when prefix length is equal. In Cisco CCNA 200-301 v1.1, IP Connectivity questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. The correct commands satisfy the network-wide path and the preferred host-specific path described in the exhibit. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

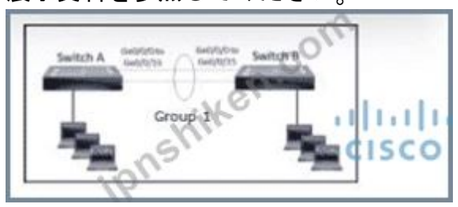
質問: **213**
特定のネットワークからの管理アクセスを制限する Cisco Wireless LAN Controller の機能はどれですか?
A. CPU ACL
B. TACACS
C. フレックス ACL
D. 半径
正解: (正解を表示します)
A CPU ACL on a Cisco Wireless LAN Controller restricts management-plane traffic destined to the controller itself. That is the feature used when management access must be limited to specific source networks. The CPU ACL is applied to traffic handled by the controller CPU, such as SSH, HTTPS, Telnet, SNMP, or other management access depending on platform support and configuration. TACACS+ and RADIUS are AAA services; they authenticate or authorize users but do not by themselves filter which source networks can reach the controller management plane. A Flex ACL applies to client data traffic in FlexConnect designs, not to controller management access. Cisco CCNA v1.1 Security Fundamentals expects the distinction between access control and authentication. If the requirement says restrict management access from specific networks, the security control must filter management-plane packets before login is even considered. On a WLC, that points to the CPU ACL.

質問: **214**
WLC で LAG を設定または削除する際の要件は何ですか?
A. LAG が有効な場合、トラフィック フローの受信ポートと送信ポートを指定する必要があります。
B. LAG を有効化または再構成した後、コントローラを再起動する必要があります。
C. LAG が無効になっている場合は、管理インターフェイスを再割り当てする必要があります。
D. 同じポートで複数のタグなしインターフェイスをサポートする必要があります。
正解: (正解を表示します)
The controller must be rebooted after enabling or reconfiguring LAG.. On Cisco Wireless LAN Controllers, Link Aggregation changes the way controller ports are bundled and used for client, AP, and management traffic. Enabling, disabling, or reconfiguring LAG is not merely a live interface command; the controller must be rebooted for the change to take effect. The management interface is not manually reassigned simply because LAG is removed, and LAG does not require the administrator to specify separate incoming and outgoing physical ports for each traffic flow. Cisco CCNA 200-301 v1.1 Network Access expects candidates to know that WLC LAG is a controller-level operational setting and that disruptive changes require a reboot window. The corrected answer is that the controller must be rebooted after enabling or reconfiguring LAG.
That is the requirement that prevents engineers from expecting the WLC to immediately change forwarding behavior without a restart.

質問: **215**
レイヤ3スイッチの機能は何ですか？
A. 異なるVLAN内のデバイス間でトラフィックをルーティングします。
B. MACアドレスのみを使用してVLAN間でイーサネットフレームを転送します。
C. これらは、IPアドレスに限定されたエンドポイント間でフレームを転送します。
D. レイヤ3モードで動作しているときは、ブロードキャストトラフィックのみを送信します。
正解: (正解を表示します)
They move frames between endpoints limited to IP addresssses.. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **216**
VLAN ホッピング攻撃はどのように軽減されますか?
A. 動的 ARP インスペクションを有効にします
B. 手動でトランク ポートを実装し、DTP を無効にします
C. すべてのポートをアクティブにして、デフォルトの VLAN に配置します。
D. 拡張 VLAN を構成する
正解: **(**正解を表示します**)**
Use B for this item. VLAN hopping is mitigated by manually configuring trunk ports and disabling Dynamic Trunking Protocol where trunks are not needed. This prevents an attacker from negotiating an unauthorized trunk from an access port. In Cisco CCNA 200-301 v1.1, Network Access questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. DAI protects ARP, activating unused default-VLAN ports is unsafe, and extended VLANs do not stop hopping attacks. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **217**
CiscoワイヤレスLANコントローラにリンクアグリゲーションを実装した場合について、正しい記述はどれですか？
A. クライアントトラフィックを通過させるには、2 つ以上のポートを設定する必要があります。
B. EtherChannelは 「アクティブモード」で構成する必要があります
C. 有効にすると、WLCの帯域幅は500Mbpsに低下します。
D. クライアントトラフィックを通過させるには、機能する物理ポートが1つ必要です。
正解: **D** (コメントを発表する)
One functional physical port is needed to pass client traffic. Switching features such as trunks and EtherChannels are controlled by negotiation mode, encapsulation, VLAN membership, and whether the selected protocol is Cisco proprietary or standards based. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The incorrect options either disable negotiation, select the wrong negotiation protocol, or configure a mode that cannot form the requested link under the stated conditions. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **218**
展示資料を参照してください。


LACP EtherChannelが設定され、最後の変更は、SwitchAのインターフェースが受信パケットに応答するものの、ネゴシエーションを開始しないようにすることです。interface range gigabitethernet0/0-15コマンドが入力されます。次に何を設定する必要がありますか？
A. SwitchA(config-if-range) #チャネルグループ1モード望ましい
B. SwitchA(config-if-range) #channel-group 1 mode auto
C. SwitchA(config-if-range) #チャネルグループ1モードアクティブ
D. SwitchA(config-if-range) #チャネルグループ1モードパッシブ

正解: **D** (コメントを発表する)
SwitchA(config-if-range) #channel-group 1 mode passive. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco- consistent configuration or behavior for this wireless scenario.

質問: **219**
無線LANコントローラでWPA2-PSK無線LANを設定する場合、ASCII形式で必要な最小文字数はいくつですか？
A. 6
B. 8
C. 12
D. 18
正解: (正解を表示します)
8. Wireless questions require separating client association, RF design, AP mode, WLAN security, and controller policy. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Incorrect answers usually confuse an encryption method with authentication, or a controller feature with a switchport feature. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **220**
軽量アクセスポイントがローカルモードで設定されている場合、有線ネットワークに接続するために使用するポートの種類はどれですか？
A. イーサチャネル
B. LAG
C. トランク
D. アクセス
正解: (正解を表示します)
access. A lightweight AP in local mode normally connects to the wired network through an access port for AP management connectivity, because client data is tunneled to the WLC through CAPWAP rather than locally switched onto multiple client VLANs at the AP switchport. Trunking is typically required for FlexConnect local switching or autonomous AP deployments that map multiple WLANs to VLANs locally. LAG and EtherChannel are link aggregation mechanisms and are not the default port type for a local-mode lightweight AP. Cisco CCNA 200-301 v1.1 Network Access expects engineers to distinguish local mode from FlexConnect mode. The corrected answer is access. Local mode centralizes client traffic at the controller, so the AP's wired switchport does not need to trunk client VLANs by default.

質問: **221**
ソフトウェア定義アーキテクチャでは、どのプレーンが分散され、トラフィックの転送を担当しますか?
A. 管理プレーン
B. コントロール プレーン
C. ポリシー プレーン
D. データプレーン
正解: (正解を表示します)

The data plane is responsible for forwarding traffic. In traditional devices, the data plane is distributed across the network devices themselves, even when the control and management functions are centralized or influenced by a controller. The control plane decides paths and builds tables; the data plane uses those tables to switch or route packets. The management plane handles configuration, monitoring, and administrative access. A policy plane may describe intent or business policy in some architectures, but it is not the forwarding plane. Cisco CCNA 200-301 v1.1 Automation and Programmability tests software-defined architecture at a conceptual level. The most important separation is that controller-based networking can centralize control while forwarding still occurs on the devices. The plane that is distributed and responsible for traffic forwarding is the data plane. Therefore, D is correct.

質問: **222**
スイッチで VLAN を構成する Ansible スクリプトを作成するために必要な 2 つのコンポーネントはどれですか? 2つ選んでください。）
A. クックブック
B. タスク
C. プレイブック
D. モデル
E. レシピ
正解: **(**正解を表示します**)**
Use B and C for this item. An Ansible automation uses playbooks and tasks to define work such as configuring a VLAN. The playbook organizes the automation, while tasks call modules or commands to produce the desired configuration on managed devices. In Cisco CCNA 200-301 v1.1, Automation and Programmability questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. Cookbooks and recipes are Chef terms, and a model is not the Ansible component required here. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **223**
展示資料を参照してください。

```
["red", "one"]
```

どのような種類のJSDNデータが表現されていますか？
A. 文字列
B. 配列
C. 番号
D. オブジェクト
正解: **B (**コメントを発表する**)**
array. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE. JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact with a controller, while southbound APIs allow the controller to communicate with network devices. NETCONF and RESTCONF are configuration
/management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to- device communication with application-to-controller communication or confuse a data format with a protocol.
Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers. The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

質問: **224**
ポイントツーマルチポイント ネットワーク トポロジでプライマリ ハブとして機能する AP モード。
A. フレックスコネクト

B. SEコネクト
C. ブリッジ
D. ローカル
正解: (正解を表示します)
bridge. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

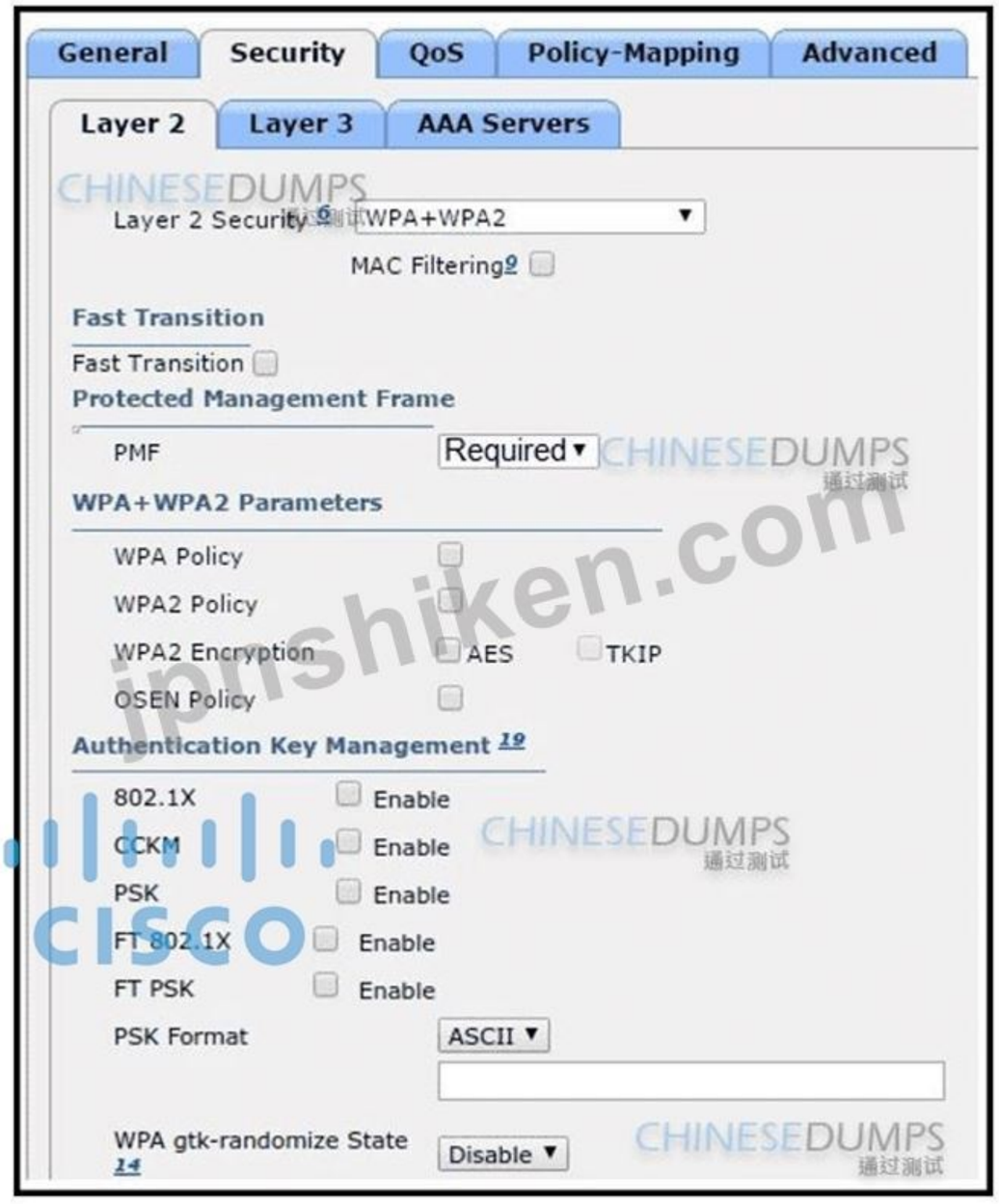
質問: **225**
HSRPグループ内のアクティブルーターが故障した場合、どのルーターがその役割を引き継ぎ、パケットを転送するのでしょうか？
A. バックアップ
B. スタンバイ
C. リスニング中
D. 転送
正解: (正解を表示します)
standby. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym.
The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **226**
Cisco WLC のコンソール接続によって提供される機能はどれですか?
A. 帯域外管理
B. デバイス管理用の安全な帯域内接続
C. ファイル転送用の暗号化されていない帯域内接続
D. HTTP ベースの GUI 接続
正解: (正解を表示します)
out-of-band management. Wireless questions require separating client association, RF design, AP mode, WLAN security, and controller policy. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Incorrect answers usually confuse an encryption method with authentication, or a controller feature with a switchport feature. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu **1813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **227**
サーバー仮想化でハイパーバイザーが各仮想マシンに提供する役割は何ですか?
A. サービスとしてのインフラストラクチャ。
B. サービスとしてのソフトウェア
C. 物理リソースの制御と配布
D. ハードウェア コントローラとして機能します。
正解: **C** (コメントを発表する)
control and distribution of physical resources. Automation questions require separating controller roles, API direction, data formats, HTTP behavior, and configuration-management tooling. Cisco CCNA 200-301 v1.1 includes this topic under Network Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The incorrect options mix northbound and southbound communication, confuse data serialization with transport, or describe traditional device-by-device management. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **228**
展示資料を参照してください。



ネットワークエンジニアは新しい無線LANを構成しており、RADIUSサーバーの代わりに事前共有キーを使用して認証を行うように指示されています。構成を完了するために、エンジニアは他にどのような作業を行う必要がありますか？

A. PMFを無効にする PSKを有効にする 802.1xを有効にする

B. WPAポリシーを選択 CCKMを有効にする PSKを有効にする

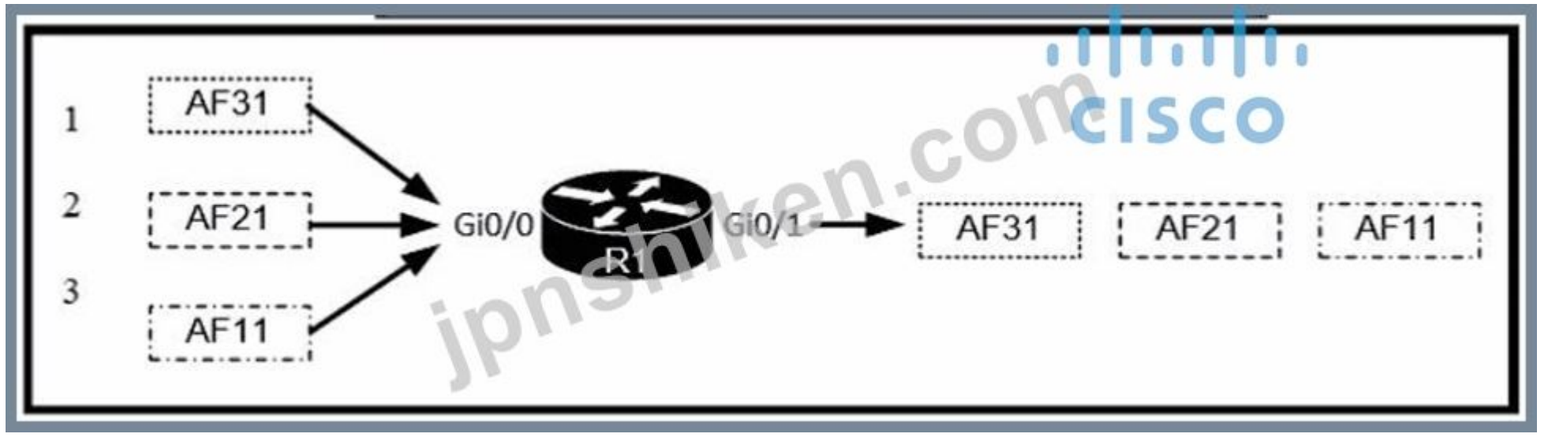
C. WPAポリシーを選択 WPA2ポリシーを選択 FT PSKを有効にする

D. WPA2ポリシーの選択 PMF無効化 PSK有効化

正解: **D** (コメントを発表する)

Select WPA2 Policy Disable PMF Enable PSK. Wireless questions depend on AP mode, WLAN security, RF band selection, controller interfaces, and client roaming or authentication behavior. Cisco CCNA 200-301 v1.
1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong options confuse encryption with authentication, local switching with tunneling, or controller management with client data handling. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco- consistent behavior for this item.

質問: 229
展示資料を参照してください。



R1は受信パケットに対して、どのホップごとのQoS動作を適用していますか？
A. キューイング
B. マーキング
C. シェーピング
D. 警察活動
正解: **(**正解を表示します**)**
policing. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic.
Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: 230
左側のIPv6アドレスを右側のタイプにドラッグアンドドロップしてください。

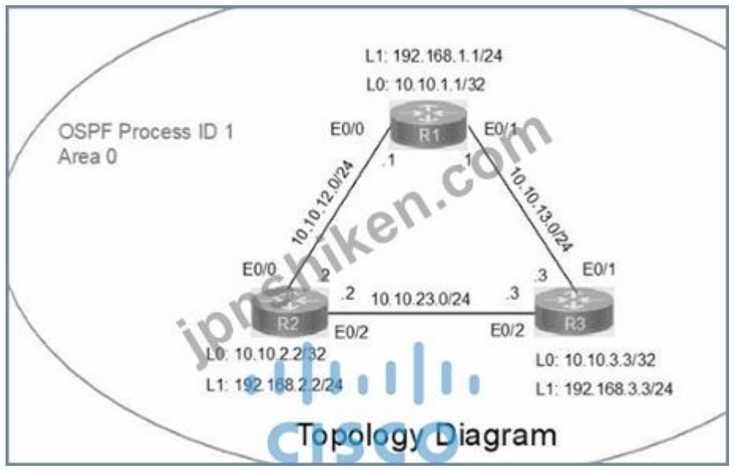
正解:

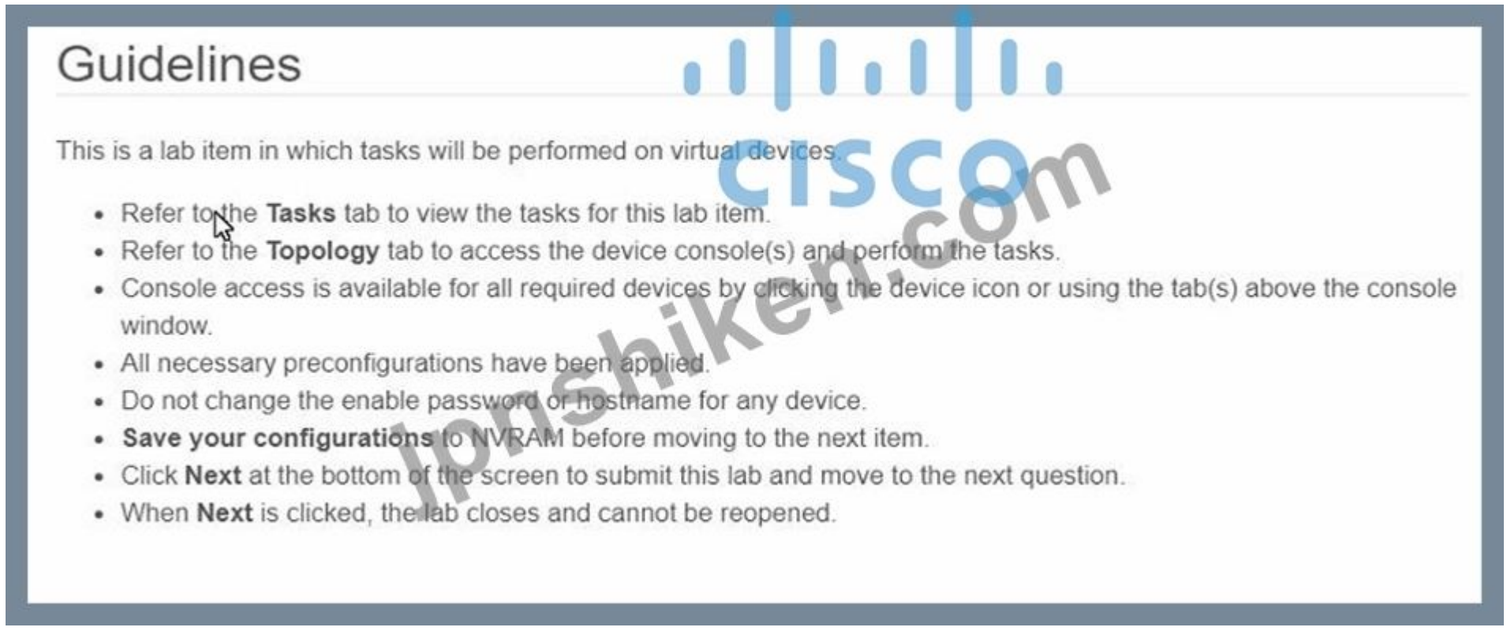
Explanation:

Cisco CCNA 200-301 v1.1 expects these items to be matched by function, protocol layer, scope, and operational role rather than by keyword similarity. The reliable method is to identify what each item actually does in a Cisco network: whether it forwards traffic, manages a device, secures access, assigns addressing, identifies a resource, or carries control information. Distractors in this format are usually valid networking terms placed under the wrong category. That is why the retained mapping is important; it keeps protocol behavior, device function, and service purpose aligned. In a real network, mixing these concepts leads to broken routing, failed wireless access, insecure management, or automation calls aimed at the wrong interface. The mapping shown in the document is therefore retained as the Cisco-consistent answer for this item.

2000:6a4f:74f8:f7b6:cb1a:934c:36ee:1
fe80:1e60:1f59:01b8:ece8:e962:4364:7
fc00:302d:1b26:dbe7:ce8b:17ae:be9f:3
ff00:45fc:709a:d439:62cb:cdad:0a15:12

質問: **231**


L1: 192.168.1.1/24
L0: 10.10.1.1/32
OSPF Process ID 1
Area 0
E0/0
E0/1
R1
.1
.1
10.10.12.0/24
10.10.13.0/24
E0/0
.2
.3
E0/1
10.10.23.0/24
.2
.3
R2
E0/2
E0/2
R3
L0: 10.10.2.2/32
L1: 192.168.2.2/24
L0: 10.10.3.3/32
L1: 192.168.3.3/24
Topology Diagram



3台のルーター間のIP接続は設定済みです。OSPF隣接関係を確立する必要があります。

1. R1とR2のルーターIDを、両者間で共有されているリンクのインターフェースIPアドレスを使用して設定します。
2. R1およびR3に面するR2リンクに最大値を設定します。R2はDR(指定リポジトリ)となる必要があります。R2に面するR1およびR3リンクは、DR選出のためのデフォルトのOSPF設定のままにしておく必要があります。OSPFプロセスをクリアした後、設定を確認してください。
3. ホストワイルドカードマスクを使用して、3つのルーターすべてがそれぞれのループバック1ネットワークをアドバタイズするように設定します。
4. R1とR3間のリンクを設定し、他のOSPFルーターを追加する機能を無効にします。

正解:

See the Explanation below.

Explanation:

Answer as below configuration:

on R1

```
conf terminal
interface Loopback0
ip address 10.10.1.1 255.255.255.255
!
interface Loopback1
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/0
no shut
ip address 10.10.12.1 255.255.255.0
ip ospf 1 area 0
duplex auto
!
```

interface Ethernet0/1
no shut
ip address 10.10.13.1 255.255.255.0
ip ospf 1 area 0
duplex auto
!
router ospf 1
router-id 10.10.12.1
network 10.10.1.1 0.0.0.0 area 0
network 192.168.1.0 0.0.0.255 area 0
!
copy run star

On R2
conf terminal
interface Loopback0
ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
ip address 192.168.2.2 255.255.255.0
!
interface Ethernet0/0
no shut
ip address 10.10.12.2 255.255.255.0
ip ospf priority 255
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/2
no shut
ip address 10.10.23.2 255.255.255.0
ip ospf priority 255
ip ospf 1 area 0
duplex auto
!
router ospf 1
network 10.10.2.2 0.0.0.0 area 0
network 192.168.2.0 0.0.0.255 area 0
!
copy runs start

On R3
conf ter
interface Loopback0
ip address 10.10.3.3 255.255.255.255
!
interface Loopback1
ip address 192.168.3.3 255.255.255.0
!
interface Ethernet0/1
no shut
ip address 10.10.13.3 255.255.255.0
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/2
no shut
ip address 10.10.23.3 255.255.255.0
ip ospf 1 area 0
duplex auto
!
router ospf 1
network 10.10.3.3 0.0.0.0 area 0
network 192.168.3.0 0.0.0.255 area 0
!
copy run start
!

質問: 232
展示資料を参照してください。

```
R1# sh ip ospf int gig0/0
Gig0/0 is up, line protocol is up
  Internet Address 10.201.24.8/28, Area 1, Attached via Network Statement
  Process ID 100, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no           Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 10.201.24.8
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07

R2#sh ip ospf int gig0/0
gig0/0 is up, line protocol is up
  Internet Address 10.201.24.1/28, Area 1
  Process ID 100, Router ID 172.16.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.1.1, Interface address 10.201.24.1
  No backup designated router on this network
  Timer intervals configured, Hello 20, Dead 80, Wait 80, Retransmit 5
```

cisco
jpnshiken.com

隣接関係を確立せずにOSPFネイバー関係を確立するには、どのような操作が必要ですか？

A. ヘルト間隔を変更する

B. プロセスIDを変更する

C. 優先度を変更する

D. ネットワークタイプを変更する

正解: **C (**コメントを発表する**)**

modify priority. OSPF neighbors can reach the 2-Way state without forming a full adjacency on a broadcast multiaccess segment when they are not required to become DR or BDR adjacencies. Changing OSPF priority is the mechanism that controls whether a router participates in the DR/BDR election. A priority of 0 prevents a router from becoming DR or BDR, so the neighbor relationship can be visible without the routers advancing to full adjacency with each other as DROTHER neighbors. Cisco CCNA 200-301 v1.1 IP Connectivity tests this because OSPF adjacency rules are not the same on all network types.
Matching hello timers is required to become neighbors at all, but it does not explain the deliberate ' without forming an adjacency ' behavior.
Process IDs are locally significant and do not have to match. The priority setting is the answer that changes the OSPF election role and therefore the adjacency outcome.

質問: **233**

エンジニアがNATを設定して、送信元サブネット10.10.0.0/24を3つのアドレスのいずれかに変換するようにしています。
192.168.30.1、192.168.3.2、192.168.3.3 のうち、どの設定を使用すべきですか？

enable
configure terminal
ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30
route-map permit 10.10.0.0 255.255.255.0
ip nat outside destination list 1 pool mypool
interface g1/1
ip nat inside
interface g1/2
ip nat outside

enable
configure terminal
ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30
access-list 1 permit 10.10.0.0 0.0.0.255
ip nat inside source list 1 pool mypool
interface g1/1
ip nat inside
interface g1/2
ip nat outside

enable
configure terminal
ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30
access-list 1 permit 10.10.0.0 0.0.0.255
ip nat outside destination list 1 pool mypool
interface g1/1
ip nat inside
interface g1/2
ip nat outside

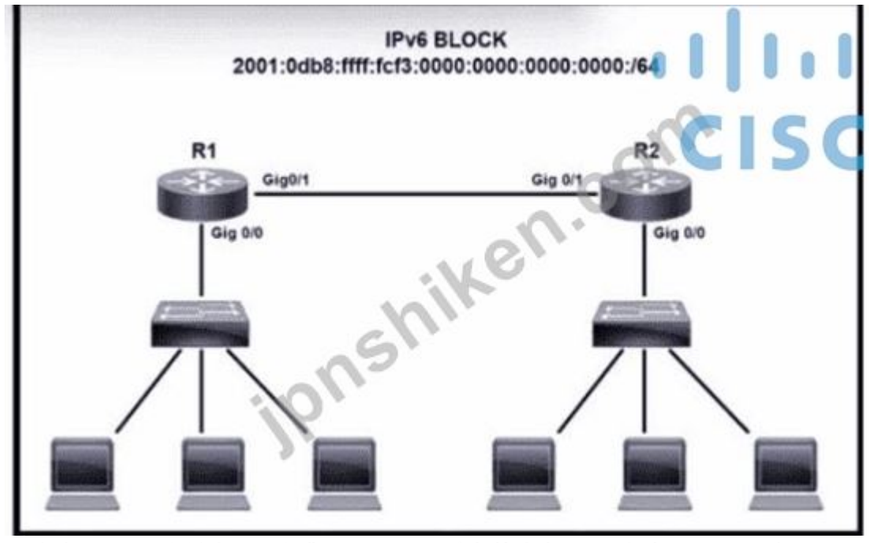
enable
configure terminal
ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30
access-list 1 permit 10.10.0.0 0.0.0.254
ip nat inside source list 1 pool mypool
interface g1/1
ip nat inside
interface g1/2
ip nat outside

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**)**
Option C. The answer follows directly from normal Cisco device behavior and the wording of the scenario.
Cisco CCNA 200-301 v1.1 includes this under IP Services, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **234**
ネゴシエーション プロトコルを使用せずに 2 つのスイッチ間で EtherChannel を構成するには、どのモードを使用する必要がありますか?
A. オン

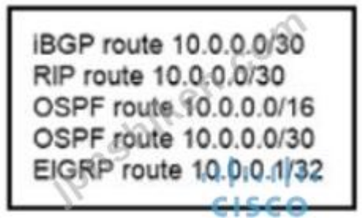
B. オート
C. アクティブ
D. 望ましい
正解: **A** (コメントを発表する)
EtherChannel mode on creates a static port channel without using a negotiation protocol. That means the switch bundles the selected physical interfaces unconditionally, provided the local interface parameters are compatible. No LACP or PAgP packets are exchanged. Mode active is LACP and actively attempts to negotiate. Mode auto is PAgP passive behavior, and desirable is PAgP active negotiation. The question says without using a negotiation protocol, so the only correct choice is on. Cisco CCNA v1.1 Network Access includes EtherChannel configuration and the difference between static, LACP, and PAgP modes. In production, static EtherChannel must be used carefully because the switch does not protect you from all mismatches the same way a negotiation protocol can. Both sides must be configured consistently. For exam purposes, the keyword is unconditional. If the bundle is formed manually and no LACP/PAgP negotiation is sent or received, the Cisco IOS command uses channel-group mode on.

質問: **235**



図を参照してください。企業内で IPv6 が実装されています。コマンド Ipv6 unlcast-routing が構成されます。R1 のインターレース GlgO/0 は、割り当てられた IPv6 ブロックを使用して動的割り当てを提供するように構成する必要があります。このタスクを実行するコマンドはどれですか?
A. IPv6アドレス 2001:DB8:FFFF:FCF3::1/64
B. IPv6 アドレス autoconfig 2001:DB8:FFFF:FCF2::/64
C. IPv6アドレス 2001:DB8:FFFF:FCF3::/64 eui-64
D. IPv6 アドレス 2001:DB8:FFFF:FCF3::/64 リンクローカル
正解: (正解を表示します)
ipv6 addresss 2001:DB8:FFFF:FCF3::/64 eui-64. Network fundamentals questions require careful attention to address scope, media type, cabling limits, topology design, virtualization, cloud service models, and the difference between TCP and UDP. The CCNA 200-301 v1.1 blueprint expects candidates to identify not only definitions but also the operational consequence of each choice. For example, public and private addressing have different routing behavior; fiber and copper use different physical media; TCP and UDP make different reliability tradeoffs; and virtualization abstracts physical resources through a hypervisor. The wrong answers are usually plausible terms from the same area, but they do not match the exact condition described in the question. The selected answer is correct because it is the only option that fits the stated network behavior, design requirement, or physical/logical property. That is the level of precision needed for Cisco troubleshooting and implementation work.

質問: **236**
展示資料を参照してください。



ルーターは、異なるルーティング情報ソースからこれら5つの経路を受信しました。
ルーターはルーティングテーブルにどの2つのルートをインストールしますか？(2つ選択してください)
A. RIPルート 10.0.0.0/30
B. iBGPルート 10.0.0.0/30
C. OSPFルート 10.0.0.0/30
D. EIGRPルート 10.0.0.1/32
E. OSPFルート 10.0.0.0/16
正解: **C,D (**コメントを発表する**)**
A router installs the best route by applying two major rules: longest prefix match and administrative distance.
Prefix length is considered first when routes describe different destination scopes; the more specific prefix wins for destinations inside that range. When routes have the same prefix length but come from different routing sources, the route with the lower administrative distance is preferred. In the answer set, the OSPF route to 10.0.0.0/30 is chosen over competing routes to the same /30 because OSPF has a better administrative distance than RIP and iBGP. The EIGRP host route to 10.0.0.1/32 is also installed because it is a more specific route to that single host. Cisco CCNA 200-301 v1.1 IP Connectivity requires engineers to interpret routing tables using these exact rules. The OSPF /16 is broader and does not replace a more specific /30 for matching destinations. The route table can contain both a network route and a host route when their prefixes differ.

質問: **237**
FHRP(ファーストホップ冗長プロトコル)を使用するメリットは何ですか？
A. ネットワーク上のARPトラフィックが減少
B. 複数のゲートウェイ間で、それぞれの負荷に応じてトラフィックを分散します。
C. ネットワークルーターの管理オーバーヘッドを削減
D. 可用性が高い
正解: **(**正解を表示します**)**
Higher degree of availability. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First- hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

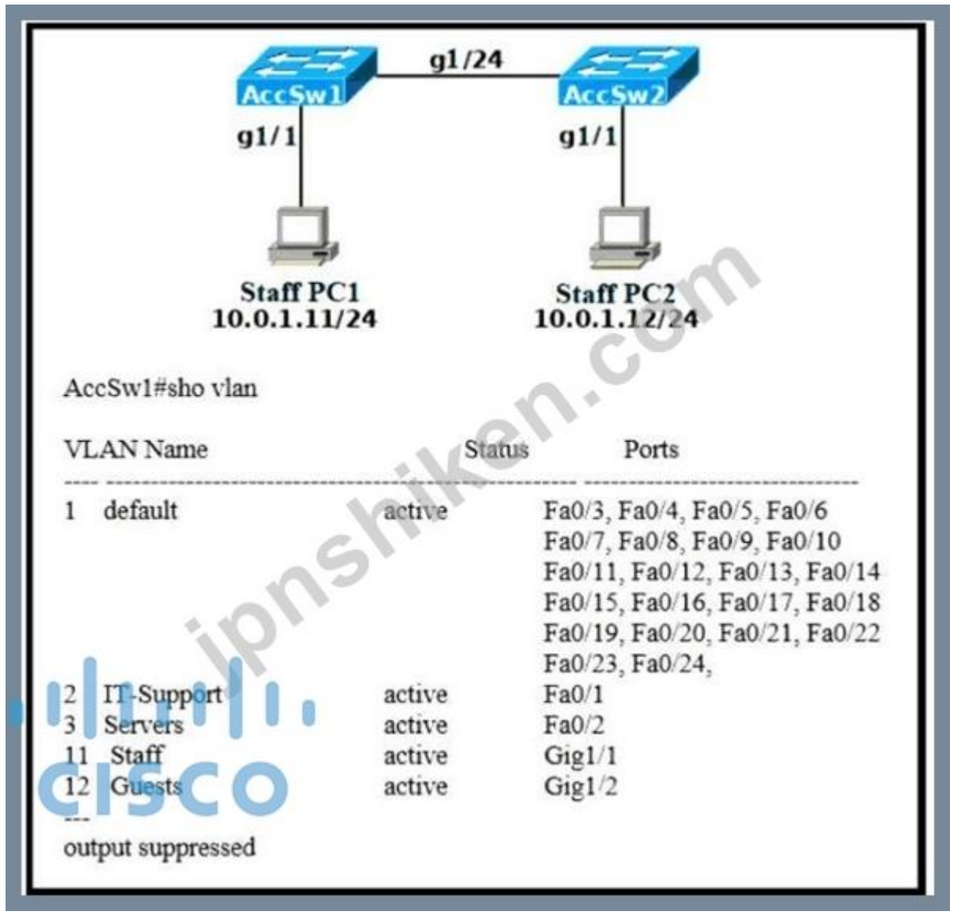
質問: **238**
セキュリティの観点から見て、SDN(ソフトウェア定義ネットワーク)を従来のネットワーク方式と比較して使用する利点は何ですか？
A. セキュリティは、ファイアウォール、VPN、IPSを使用してネットワークの境界付近で管理されます。
B. デバイス同士が通信してセキュリティポリシーを確立します。
C. 統一された制御ポイントを作成し、すべてのデバイスでセキュリティ ポリシーの一貫性を確保します。

D. デバイスごとにセキュリティポリシーをローカルで設定するためのAPIを公開します。
正解: **C** (コメントを発表する)
It creates a unified control point making security policies consistent across all devices.. Security questions in CCNA 200-301 v1.1 require matching the control to the threat or access requirement. Authentication proves identity, authorization controls what the user can do, and accounting records activity. Firewalls inspect and permit or deny traffic based on policy, while ACLs match packet fields in a defined order. VPN and IPsec questions require knowing whether the design protects unicast traffic, supports tunneling, or encrypts the original packet. Password and SSH questions depend on IOS behavior, including encrypted secrets, local users, domain names, and cryptographic images. The incorrect choices often use a valid technology in the wrong role or provide weaker protection. The selected answer is the Cisco-consistent control because it directly satisfies the access, confidentiality, or threat-mitigation requirement stated in the question.

質問: **239**
レイヤ2スイッチの特徴は何ですか？
A. ステートフルなトランザクション情報を保持します
B. 特定の順序でデータを送信する役割を担う
C. MACアドレスに基づいて転送決定を行います
D. トランスポート層プロトコルに基づくフィルタ
正解: **C** (コメントを発表する)
Makes forwarding decisions based on MAC addressses. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **240**
従来のキャンパスデバイス管理とCisco DNA Centerデバイス管理は、導入に関してどのような違いがありますか？
A. 従来のキャンパスデバイス管理方式は、通常、Cisco DNA Center デバイス管理よりもパッチやアップデートを迅速に展開します。
B. Cisco DNA Centerのデバイス管理は、従来のほとんどのキャンパスデバイス管理オプションよりも低コストで実装できます。
C. 従来のキャンパスデバイス管理では、Cisco DNA Centerデバイス管理を使用する場合よりもネットワークを迅速に拡張できます。
D. Cisco DNA Centerのデバイス管理は、従来のキャンパスデバイス管理よりも迅速にネットワークを展開します。
正解: (正解を表示します)
Cisco DNA Center device management deploys a network faster than traditional campus device management.. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable /auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **241**
展示資料を参照してください。



スイッチAccSw2がPC2とともにネットワークに追加されました。AccSw2にはすべてのVLANが実装されています。
PC1とPC2間のレイヤ2接続を確立するには、AccSw2のポートをどのように設定する必要がありますか？

A. インターフェース GigabitEthernet1/2
スイッチポートモードアクセス
switchport access vlan 2
!
インターフェース GigabitEthernet1/24
スイッチポートモード トランク

B. インターフェース GigabitEthernet1/1
スイッチポートモードアクセス
switchport access vlan 11
!
インターフェース GigabitEthernet1/24
スイッチポートモード トランク

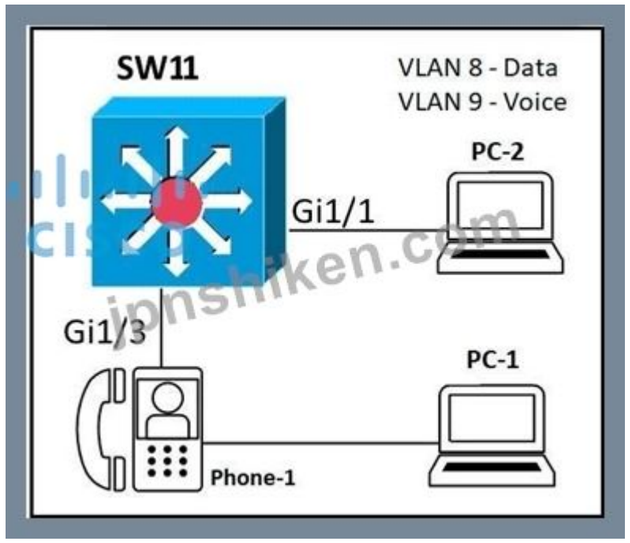
C. インターフェース GigabitEthernet1/24
スイッチポートモード トランク
switchport trunk allowed vlan 11, 12

!
インターフェース GigabitEthernet1/1
switchport access vlan 11
D. インターフェース GigabitEthernet1/2
スイッチポートモードアクセス
switchport access vlan 12
!
インターフェース GigabitEthernet1/24
スイッチポートモード トランク
switchport trunk allowed vlan 11, 12
正解**: B (**コメントを発表する**)**
Switching questions depend on MAC learning, VLAN membership, trunking, STP election, and EtherChannel behavior.
Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior.
The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong answers misapply a Layer 2 rule or configure the wrong logical interface.
In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface.
The selected answer is the Cisco- consistent behavior for this item.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問**: 242**
ID に基づいてセキュリティを提供するアクセス レイヤーの脅威軽減技術はどれですか?
A. ダイナミック ARP インスペクション
B. デフォルト以外のネイティブ VLAN を使用
C. 802.1x
D. DHCP スヌーピング
正解**: (**正解を表示します**)**
The verified answer is C. 802.1X provides identity-based access control at the access layer. A supplicant authenticates through the switch or AP to an authentication server before receiving network access.
Cisco CCNA 200-301 v1.1 places this skill in Security Fundamentals, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. DAI, DHCP snooping, and native VLAN changes protect Layer 2 infrastructure but do not authenticate user or device identity in the same way. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問**: 243**
展示資料を参照してください。



管理者は、スイッチ SW1 のインターフェース Gi1/1 と Gi1/3 を設定する必要があります。PC-1 と PC-2 はデータ VLAN に、Phone-1 は音声 VLAN に配置する必要があります。これらの要件を満たす構成はどれですか？

```
interface gigabitethernet1/1
 switchport mode access
 switchport access vlan 8
 !
interface gigabitethernet1/3
 switchport mode access
 switchport voice vlan 8
 switchport access vlan 9
```

```
interface gigabitethernet1/1
 switchport mode access
 switchport access vlan 9
 !
interface gigabitethernet1/3
 switchport mode trunk
 switchport trunk vlan 8
 switchport trunk vlan 9
```

```
interface gigabitethernet1/1
 switchport mode access
 switchport access vlan 8
 !
interface gigabitethernet1/3
 switchport mode access
 switchport access vlan 8
 switchport voice vlan 9
```

```
interface gigabitethernet1/1
 switchport mode access
 switchport access vlan 8
 !
interface gigabitethernet1/3
 switchport mode trunk
 switchport trunk vlan 8
 switchport voice vlan 9
```

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

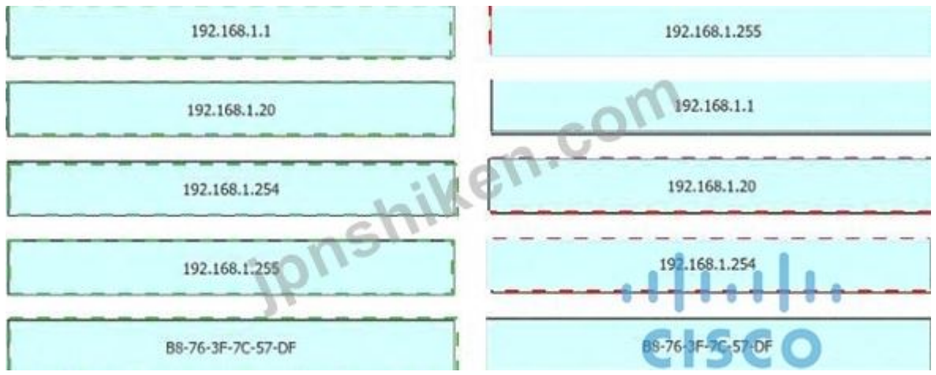
正解: **C** (コメントを発表する)

The verified answer is C. The correct switchport configuration assigns PCs to the data VLAN and the Cisco phone to the voice VLAN. A typical access port uses switchport access vlan for the attached data device and switchport voice vlan for the phone voice traffic. Cisco CCNA 200-301 v1.1 places this skill in Network Access, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. Configurations missing either data or voice VLAN assignment will fail the stated placement requirement. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **244**
展示資料を参照してください。

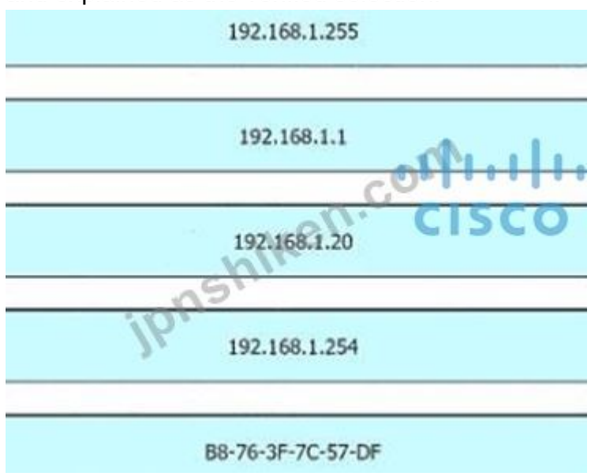
エンジニアは、クライアントワークステーションのネットワーク構成パラメータを検証し、チームリーダーに報告する任務を負っています。左側のノード識別子を右側のネットワークパラメータにドラッグアンドドロップしてください。

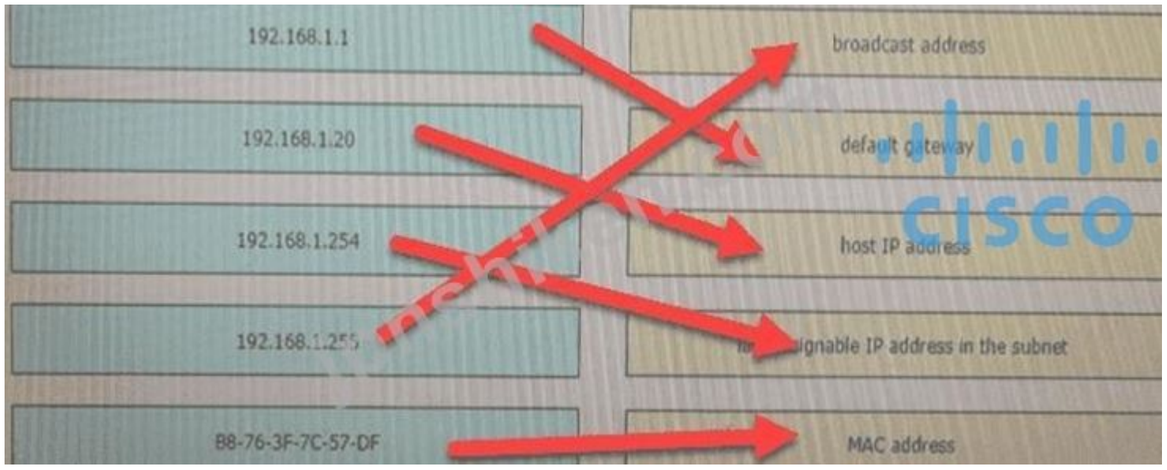
正解:



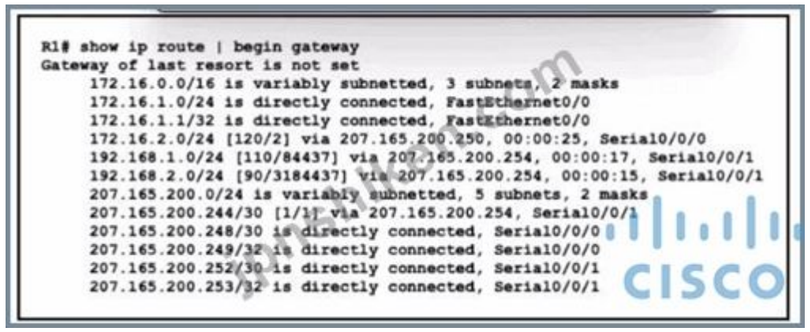
Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each protocol, component, address type, or management concept is matched to its correct operating role. The safe method is to classify every item by function: what it does, where it operates, and what problem it solves. Several distractors are usually valid networking terms, but they belong to a different layer or a different operational workflow. The shown mapping keeps those boundaries straight and avoids assigning a feature to the wrong technology. In practice, this same skill is required when troubleshooting because confusing a management- plane function with a forwarding-plane function, or a wireless security feature with an authentication feature, leads to incorrect fixes. The mapping shown in the file is therefore retained and explained as the verified selection.





質問: **245**



図を参照してください。左側の学習済み接頭辞を、右側の学習元となった優先ルーティング方法にドラッグアンドドロップしてください。

172.16.2.0/24	static
192.168.1.0/24	EIGRP
192.168.2.0/24	OSPF
207.165.200.244/30	RIP
207.165.200.248/30	

正解:

Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals drag-and-drop items test whether each protocol, address type, API action, or infrastructure component is matched to its real function. The correct way to solve these is to classify every item by layer, scope, and operational behavior before matching it. Several distractors are legitimate networking terms, but they are wrong when placed under the wrong protocol family or management model. The retained mapping preserves the Cisco distinctions between TCP and UDP behavior, AAA functions, IPv6 address scopes, device-management approaches, and REST operations. In implementation work, these distinctions matter because applying a feature at the wrong layer or associating a control with the wrong service creates broken configurations and wasted troubleshooting effort. The shown mapping is therefore retained as the verified response.

質問: 246

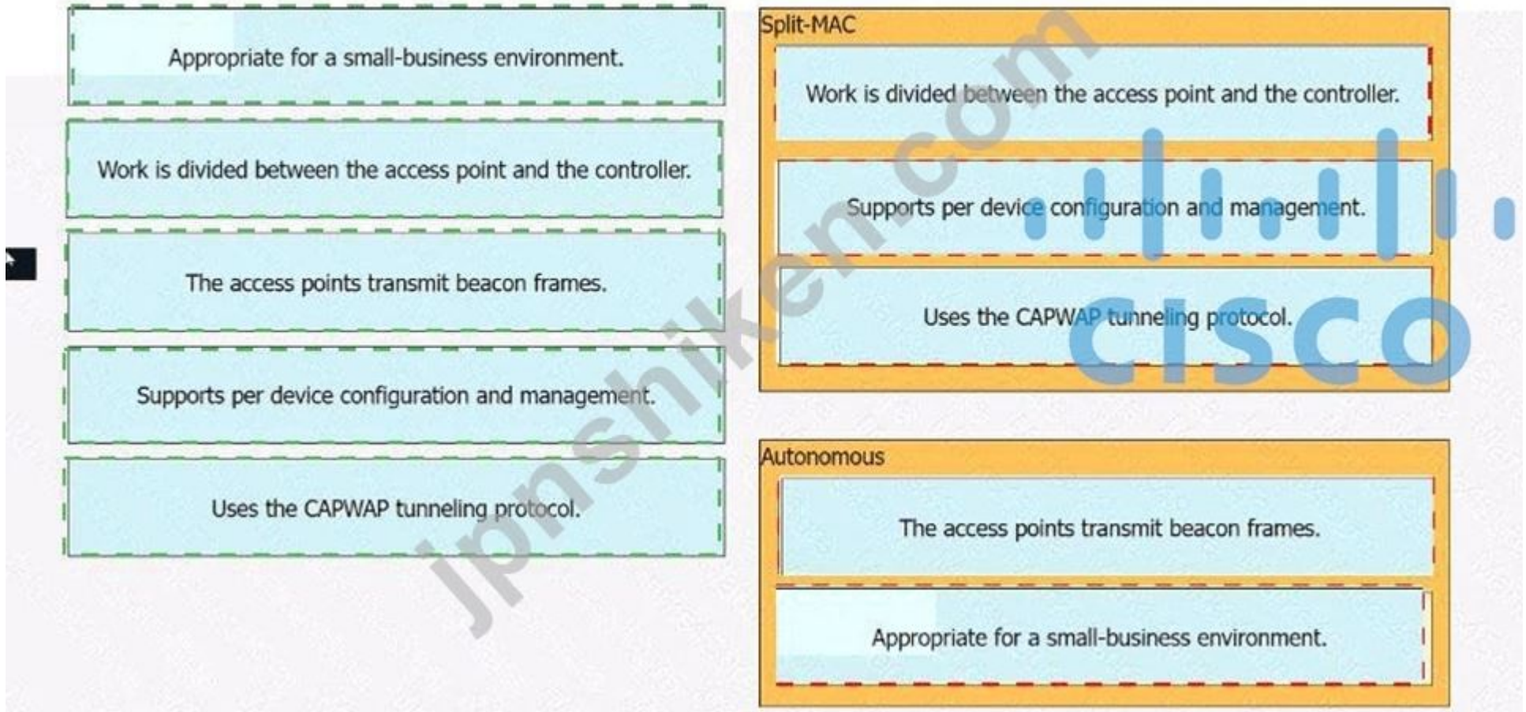
左側のワイヤレスアーキテクチャの利点を、右側のアーキテクチャの種類にドラッグアンドドロップしてください。

Drag and drop the wireless architecture benefits from the left onto the architecture types on the right.

cisco
ipnshiken.com

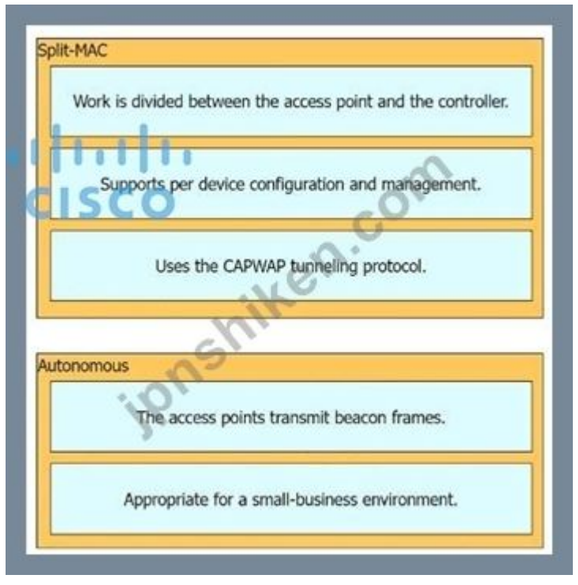
正解:

Drag and drop the wireless architecture benefits from the left onto the architecture types on the right.



Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this form test whether each protocol, command, service, or architecture term is placed with the function it actually performs. The safest approach is to classify each item by operating layer and purpose before matching it: routing behavior belongs to IP connectivity, wireless modes belong to access, REST methods belong to automation, and AAA functions belong to security services. Several distractors are valid networking terms, but they become wrong when mapped to the wrong plane or protocol. The retained mapping follows Cisco terminology and reflects how the features are used in implementation and troubleshooting. In practice, this prevents mixing up forwarding behavior with management behavior or authentication with authorization/accounting. The mapping shown in the file is therefore retained as the verified response.



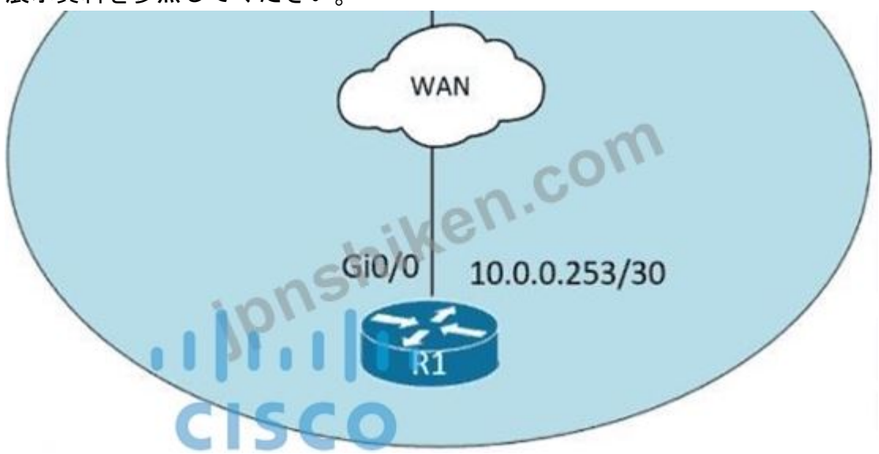
質問: **247**
Microsoft Windows を実行しているワークステーションで、デバイスのデフォルト ゲートウェイを提供するプロトコルはどれですか?
A. DHCP
B. STP
C. SNMP
D. DNS
正解: **(**正解を表示します**)**
The verified answer is A. DHCP can provide the default gateway to Windows workstations as part of the leased IP configuration. The router option tells the client which gateway to use for off-subnet destinations.
Cisco CCNA 200-301 v1.1 places this skill in IP Services, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. STP prevents switching loops, SNMP monitors devices, and DNS resolves names; none of those supplies the default gateway address to the host. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **248**
追加のアクセス ポートが必要な場合、スパイン アンド リーフ アーキテクチャがネットワークのスケーラビリティをどのように可能にしますか?
A. スパイン スイッチとリーフ スイッチを追加して、それらの間を冗長接続できます。
B. スパイン スイッチは、少なくとも 40 GB のアップリンクで追加できます。
C. コア スパイン スイッチへの 1 つの接続でリーフ スイッチを追加できます。
D. リーフ スイッチを追加して、すべてのスパイン スイッチに接続できます。
正解: **D (**コメントを発表する**)**
Spine-and-leaf networks scale access capacity by adding another leaf switch and connecting that leaf to every spine switch. That preserves the fabric's predictable any-leaf-to-any-leaf pathing and keeps oversubscription under control. A leaf switch is where servers, endpoints, or access-facing devices attach; spine switches provide the high-speed interconnection layer between leaves. Leaves do not connect to other leaves, and spines do not connect to other spines in the classic two-tier Clos design. Adding only a spine switch does not create additional access ports. Adding a leaf with a single uplink to one spine

would create a bottleneck and break the equal-cost multipath design principle. CCNA 200-301 v1.1 Network Access and Network Fundamentals include spine-leaf as a modern data-center architecture pattern. The verified answer is D: add a leaf switch with connections to every spine switch. Reference: Cisco spine-leaf/Clos architecture design guidance.

質問: **249**
デバイスをNTPサーバーとして設定する場合、どのコマンドを入力する必要がありますか？
A. ntp認証
B. NTPサーバー
C. NTPピア
D. ntpマスター
正解: **(**正解を表示します**)**
ntp master. IP services questions test the exact function of infrastructure services such as addressing, name resolution, time synchronization, logging, monitoring, and secure management. Cisco CCNA 200-301 v1.1 includes this topic under IP Services, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The distractors name valid services, but they provide a different service function from the one required in the prompt. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **250**
展示資料を参照してください。



管理者は、10.0.0.0/30サブネット内の最後に使用可能なアドレスが設定されているポートで、Cisco Discovery Protocolを無効にする必要があります。どのコマンドセットがこの要件を満たしますか？
A. インターフェース gi0/1 cdp 無効
B. インターフェース gi0/1 クリア CDP テーブル
C. インターフェース gi0/0no cdp advertise-v2
D. インターフェース gi0/0no cdp 実行
正解: **A (**コメントを発表する**)**
Answer A is the technically correct selection. CDP is disabled on a specific interface with the interface-level no cdp enable command. The requirement is to turn off CDP only on the port with the last usable address in the /30 subnet, so the correct interface must be selected and CDP disabled there. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. clear cdp table only clears learned neighbors, advertise- v2 changes advertisement format, and no cdp run is a global command rather than

an interface command in this context. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

質問: **251**
企業のセキュリティを向上させるために、組織はバッジ認証を実装してデータセンターへのアクセスを制限することを計画しています。セキュリティ プログラムのどの要素が展開されていますか?
A. ユーザートレーニング
B. ユーザーの意識
C. 脆弱性検証
D. 物理アクセス制御
正解: (正解を表示します)
physical access control. Security questions require distinguishing authentication, authorization, encryption, secure management, malware protection, and physical controls. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The wrong options apply the right security vocabulary to the wrong control or use weaker/deprecated protection.
In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **252**
PortFast機能を使用するメリットを2つ挙げてください。(2つ選択してください)
A. 有効化されたインターフェースは自動的にリスニング状態になります
B. 有効化されたインターフェースはすぐに起動し、転送状態に移行します。
C. 有効なインターフェースはトポロジー変更通知を生成しません。
D. 学習状態に移行した有効なインターフェースは、スイッチトポロジ変更通知を生成します。
E. 有効化されたインターフェースは、転送状態に移行する前に50秒間待機します。
正解: (正解を表示します)
Answer B,C is correct: B. Enabled interfaces come up and move to the forwarding state immediately; C.
Enabled interfaces never generate topology change notifications.. PortFast lets an access interface bypass the normal listening and learning delays and move directly to forwarding when the link comes up. That is valuable for end-user ports because DHCP, login scripts, and endpoint connectivity can fail or delay while classic STP converges. PortFast-enabled edge ports also do not create the same topology-change behavior expected from ordinary switch-to-switch links when end devices connect or disconnect. Cisco CCNA 200-301 v1.1 Network Access expects engineers to apply PortFast only to ports facing end hosts, not to ports that may create Layer 2 loops. The options saying the port is placed in listening state or waits 50 seconds are the opposite of PortFast behavior. The two correct benefits are immediate forwarding and avoiding unnecessary topology-change effects for edge connections.

質問: **253**
スイッチが、最近期限切れとなった宛先MACアドレスを含むフレームを受信した場合、何が起こるのでしょうか？
A. スイッチは、フレームを受信したポートの過去のアドレスについて、MACアドレスエージングテーブルを参照します。
B. スイッチは、フレームを受信したポートを除くすべての VLAN のすべてのポートにフレームをフラッディングします。
C. スイッチはフレームを破棄し、フレームを受信したポートから宛先MACアドレスを再度学習します。
D. スイッチは、フレームを受信したポートを除く、VLAN内のすべてのポートにフレームをフラッディングします。
正解: (正解を表示します)

The switch floods the frame to all ports in the VLAN except the port that received the frame.. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology.
The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **254**
MACアドレス学習の機能とは何ですか？
A. すべての VLAN とインターフェイスでデフォルトで有効になっています
B. MACアドレスフラッディングの可能性が高まります。
C. トランクに接続されているすべてのインターフェースで、デフォルトで無効になっています。
D. 管理VLANのセキュリティを強化します
正解: **(**正解を表示します**)**
It is enabled by default on all VLANs and interfaces. Security questions require distinguishing authentication, authorization, encryption, secure management, malware protection, and physical controls. Cisco CCNA 200-
301 v1.1 includes this under Network Access, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue:
a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The wrong options apply the right security vocabulary to the wrong control or use weaker /deprecated protection. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

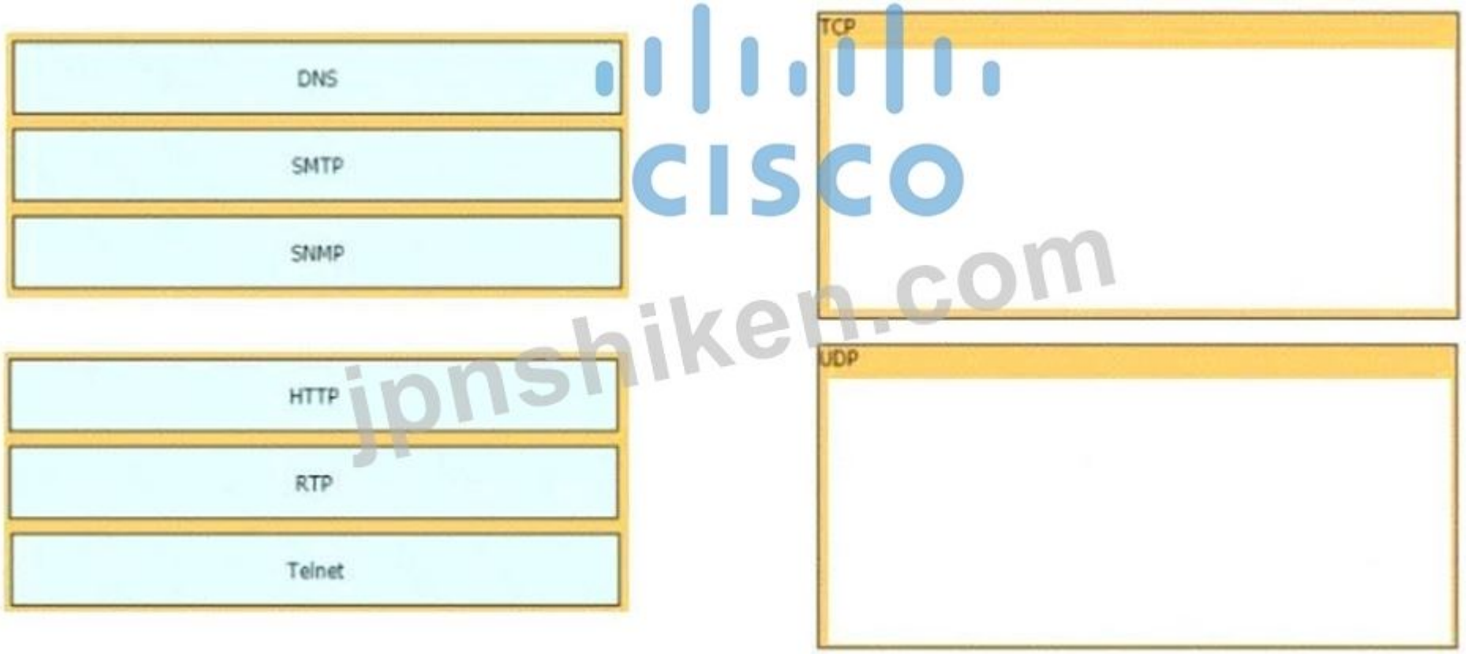
質問: **255**

```
    10.0.0.0/8 is variably subnetted, 15 subnets, 2 masks
O       10.0.12.0/24 [110/2] via 10.0.14.1, 00:17:46, GigabitEthernet0/2
C       10.0.14.0/24 is directly connected, GigabitEthernet0/2
L       10.0.14.4/32 is directly connected, GigabitEthernet0/2
O       10.0.23.0/24 [110/2] via 10.0.34.3, 00:17:46, GigabitEthernet0/0
C       10.0.34.0/24 is directly connected, GigabitEthernet0/0
L       10.0.34.4/32 is directly connected, GigabitEthernet0/0
C       10.0.45.0/24 is directly connected, GigabitEthernet0/1
L       10.0.45.4/32 is directly connected, GigabitEthernet0/1
O       10.1.0.1/32 [110/2] via 10.0.14.1, 00:17:46, GigabitEthernet0/2
R       10.2.0.0/24 [90/1] via 10.0.45.5, 00:00:13, GigabitEthernet0/1
O       10.255.1.1/32 [110/2] via 10.0.14.1, 00:17:46, GigabitEthernet0/2
O       10.255.2.2/32 [110/3] via 10.0.34.3, 00:17:46, GigabitEthernet0/0
                      [110/3] via 10.0.14.1, 00:17:46, GigabitEthernet0/2
O       10.255.3.3/32 [110/2] via 10.0.34.3, 00:17:46, GigabitEthernet0/0
C       10.255.4.4/32 is directly connected, Loopback0
R       10.255.5.5/32 [90/1] via 10.0.45.5, 00:00:13, GigabitEthernet0/1
```

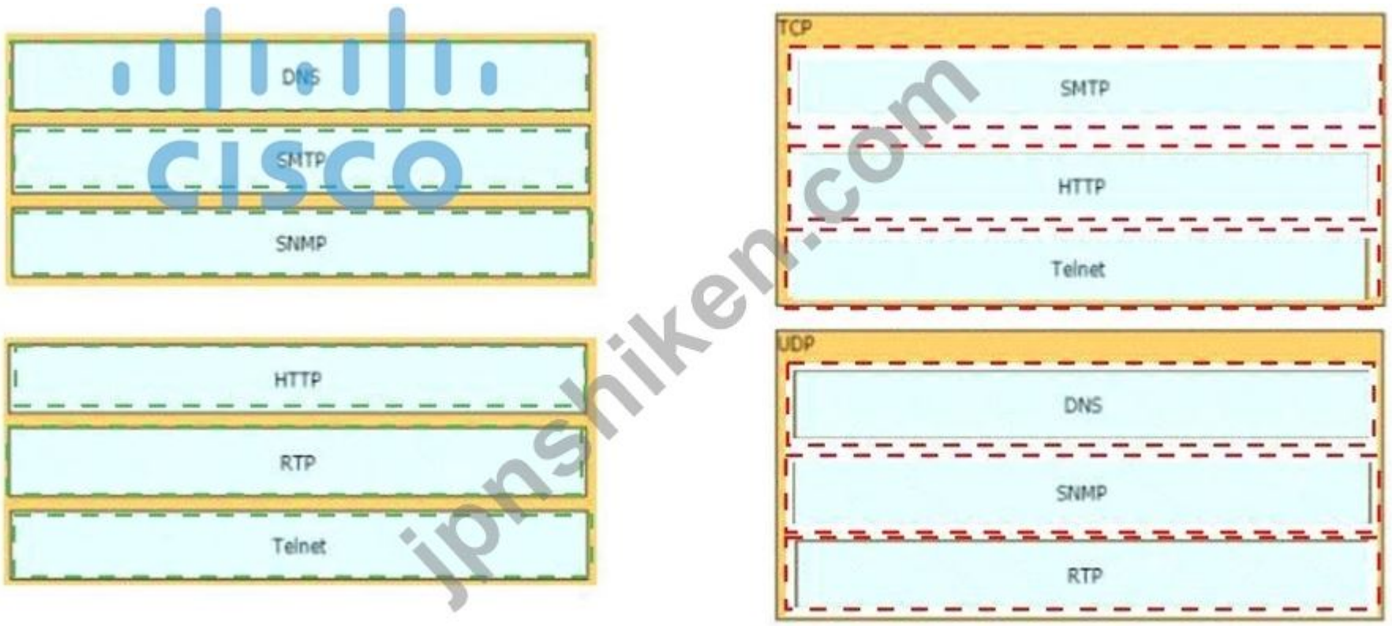
図を参照してください。どのルートがデフォルトの管理距離で設定されていますか？
A. EIGRP
B. OSPF
C. 安らかにお眠りください
D. ローカル

正解: (正解を表示します)
OSPF. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **256**
左側のTCP/IPプロトコルを右側の伝送プロトコルにドラッグアンドドロップしてください。

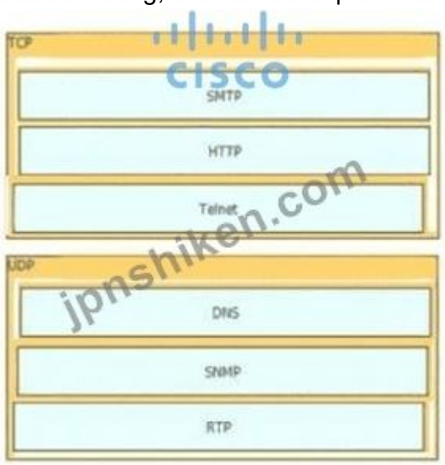


正解:



Explanation:

This item belongs to Cisco CCNA 200-301 v1.1 Network Fundamentals, where the exam measures whether the candidate can match a technology, field, protocol, or network behavior to its correct operational role. The important step is to classify each left-side item by what it actually does, not by a similar-sounding term. For example, management protocols, address types, QoS mechanisms, wireless settings, and topology terms all have strict meanings in Cisco documentation and IOS behavior. A wrong match usually places a function at the wrong layer or assigns a feature to the wrong control point. The shown mapping keeps those boundaries intact: the component that performs the function is paired with the matching description, while unrelated distractors are left unused or mapped elsewhere. In real troubleshooting, this same skill prevents engineers from applying a security, routing, switching, or automation feature in the wrong part of the design.

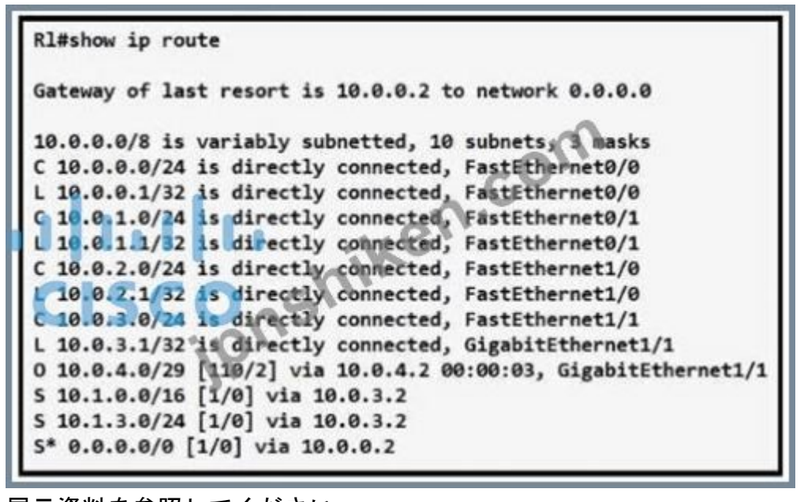


有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **257**
レイヤ 2 スイッチの 2 つの機能は何ですか? (2つ選んでください)
A. 関連付けおよび認証サーバーの中心点として機能します。
B. WAN 上のネットワーク間の最適なルートを選択します
C. VLAN 内でパケットを移動します
D. 異なる VLAN 間でパケットを移動します
E. パケットの MAC アドレスに基づいて転送の決定を行います
正解: **C,E (コメントを発表する)**
A Layer 2 switch forwards frames within a VLAN and makes forwarding decisions based on MAC addresses.
It learns source MAC addresses from ingress frames, records the associated port in the MAC address table, and forwards known destination frames out the matching port. If the destination is unknown, it floods within the VLAN. A Layer 2 switch does not select the best WAN route between networks; that is a router or Layer
3 switch function. It also does not normally move packets between different VLANs unless Layer 3 routing is involved. The existing answer that included a central point for association and authentication servers is not a Layer 2 switch function; that wording better resembles wireless or authentication infrastructure. Cisco CCNA
200-301 v1.1 Network Access expects a clean separation of switching and routing duties. The two valid Layer
2 switch functions are moving frames within a VLAN and forwarding based on MAC address.

質問: **258**
Cisco ワイヤレス LAN コントローラへの接続が失われた後もワイヤレス クライアントにサービスを提供し続けるユニファイド アクセス ポイントのモードはどれですか?
A. スニファ
B. メッシュ
C. フレックスコネクト
D. ローカル
正解: **(正解を表示します)**
Use C for this item. FlexConnect AP mode can continue serving local wireless clients when connectivity to the WLC is lost. It is designed for branch deployments where local switching and survivability are important during WAN outages. In Cisco CCNA 200-301 v1.1, Network Access questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. Local mode depends more heavily on the WLC for centralized traffic handling, while sniffer and mesh modes serve different purposes. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **259**



展示資料を参照してください。
ルーターR1は、10.0.4.10宛てのパケットをどのように転送しますか？
A. 10.0.4.2経由
B. 10.0.0.2経由
C. FastEthernet0/1経由
D. FastEthernet1/1経由
正解: **B** (コメントを発表する)
via 10.0.0.2. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **260**
仮想マシンの機能を識別するステートメントはどれですか?
A. 仮想化されたサーバーは、ハイパーバイザーとは別のスイッチに物理的に接続されている場合に最も効率的に実行されます。
B. ハイパーバイザーは、CPU、メモリ、ストレージなどの物理コンポーネントを仮想化できます
C. 各ハイパーバイザーは、1 つの仮想マシンと 1 つのソフトウェア スイッチをサポートできます。
D. ハイパーバイザーは、追加のリソースを必要とせずにレイヤー 3 で通信します
正解: (正解を表示します)
A hypervisor abstracts the physical server hardware and presents virtual hardware to each virtual machine.
That includes CPU, memory, storage, and virtual network interfaces. The virtual machine sees a logical machine, while the hypervisor schedules and allocates the real physical resources underneath it. This is the core function of server virtualization and is part of Cisco CCNA 200-301 v1.1 Network Fundamentals because modern network engineers must understand how servers connect through virtual switches and how traffic leaves a hypervisor toward the physical network. A hypervisor is not limited to one VM, and it does not magically communicate at Layer 3 without network resources. The idea that virtualized servers run best only when connected to a separate physical switch misunderstands virtualization; VM traffic can be switched inside the host through a virtual switch before reaching a physical NIC. The correct statement is that the hypervisor virtualizes physical components so multiple independent workloads can run on one host.

質問: **261**
SOHOネットワークの特徴は？
A. 各スイッチをネットワーク内の他のすべてのスイッチに接続します
B. 複数のユーザーが単一のブロードバンド接続を共有できるようにします
C. 1000 人以上のユーザーに高スループット アクセスを提供します。
D. 負荷分散と冗長性を提供するために、少なくとも 3 層のデバイスが含まれています。
正解: **(**正解を表示します**)**
Use B for this item. A SOHO network commonly lets multiple users share one broadband Internet connection.
Small office/home office designs emphasize low cost, simple management, wireless and wired access, and Internet edge services in a compact topology. In Cisco CCNA 200-301 v1.1, Network Fundamentals questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. Full-mesh switching, thousand-user capacity, and three-tier redundancy describe larger enterprise designs. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **262**
IPsecスイートに含まれるプロトコルを2つ挙げてください。(2つ選択してください)
A. AH
B. 3DES
C. ESP
D. TLS
E. AES
正解: **(**正解を表示します**)**
Answer A,C is correct: A. AH; C. ESP. AH and ESP are the two protocol headers that belong directly to the IPsec suite. Authentication Header provides integrity and authentication for IP packets, while Encapsulating Security Payload provides confidentiality and can also provide integrity and authentication depending on configuration. AES and 3DES are encryption algorithms used by security protocols, not IPsec protocols themselves. TLS is a separate transport/application security protocol used for services such as HTTPS, not an IPsec suite protocol. Cisco CCNA 200-301 v1.1 Security Fundamentals expects candidates to separate security protocols from cryptographic algorithms. The original AES/TLS answer was wrong because it selected one cipher and one non-IPsec protocol. The corrected answer is AH and ESP because those are the IPsec protocol components used to protect traffic at the IP layer.

質問: **263**
Aswitchは、宛先MACアドレス3C:5D:7E:9F:1A:2Bのフレームを受信します。
Switch# show ethernet-frame-and-mac-addresses-table

スイッチはフレームをどのように処理しますか？

A. MACアドレスが判明するまでフレームをエージングアウトします。

B. 不要なネットワーク混雑を避けるためにフレームを破棄します。

C. 設定に基づいて、フレームをあらかじめ決められたポートに切り替えます。

D. 受信ポートを除くすべてのポートにフレームをフラッディングします。

正解: **D** (コメントを発表する)

It floods the frame to all ports except the incoming port.. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **264**

ネットワーク管理者は、64 ビット アドレスを使用して新しい IPv6 ネットワークをセットアップしています。
2001:0EB8:00C1:2200:0001:0000:0000:0331/64. 構成を簡素化するために、管理者はアドレスを圧縮することにしました。管理者はどの IP アドレスを設定する必要がありますか?

A. ipv6 アドレス 21:EB8:C1:2200:1::331/64

B. ipv6 アドレス 2001:EB8:C1:22:1::331/64

C. ipv6 アドレス 2001:EB8:C1:2200:1::331/64

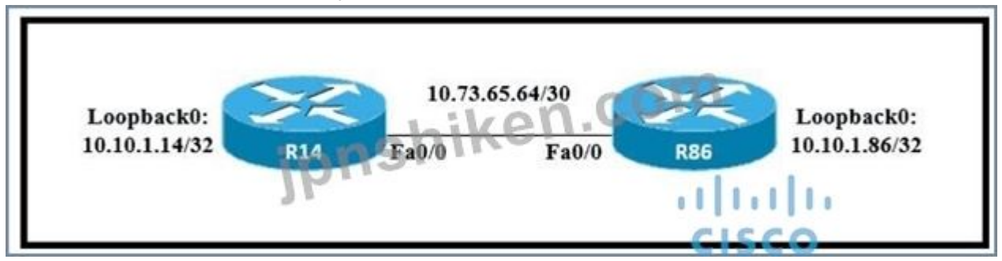
D. ipv6 アドレス 2001:EB8:C1:2200:1:0000:331/64

正解: (正解を表示します)

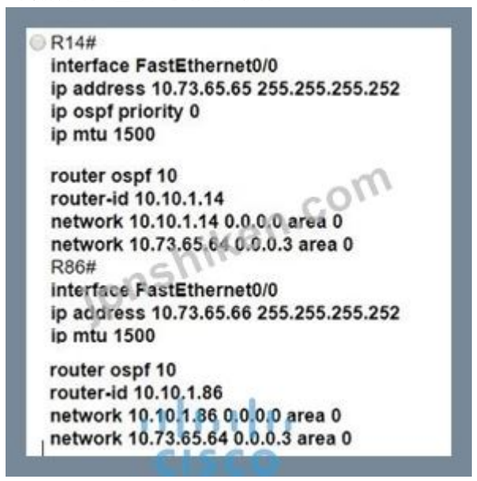
ipv6 address 2001:EB8:C1:2200:1::331/64. IPv6 questions depend on address scope, prefix representation, and whether the address is unicast, multicast, anycast, link-local, or global. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices represent a different IPv6 address behavior or an invalid compressed form. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **265**

展示資料を参照してください。



すべてのインターフェースは、duplex autoとip ospf network broadcastで設定されています。ルーターR14とR86がOSPFv2隣接関係を確立し、ルーター間でOSPF情報を交換する中心点として機能するには、どの設定が適切でしょうか？



R14#
interface Loopback0
ip ospf 10 area 0

interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip ospf priority 255
ip ospf 10 area 0
ip mtu 1500

router ospf 10
router-id 10.10.1.14

R86#
interface Loopback0
ip ospf 10 area 0
interface FastEthernet0/0
ip address 10.73.65.66 255.255.255.252
ip ospf 10 area 0
ip mtu 1500

router ospf 10
router-id 10.10.1.86
network 10.10.1.86 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0

R14#
interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip ospf priority 255
ip mtu 1500

router ospf 10
router-id 10.10.1.14
network 10.10.1.14 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0
R86#
interface FastEthernet0/0
ip address 10.73.65.66 255.255.255.252
ip mtu 1400

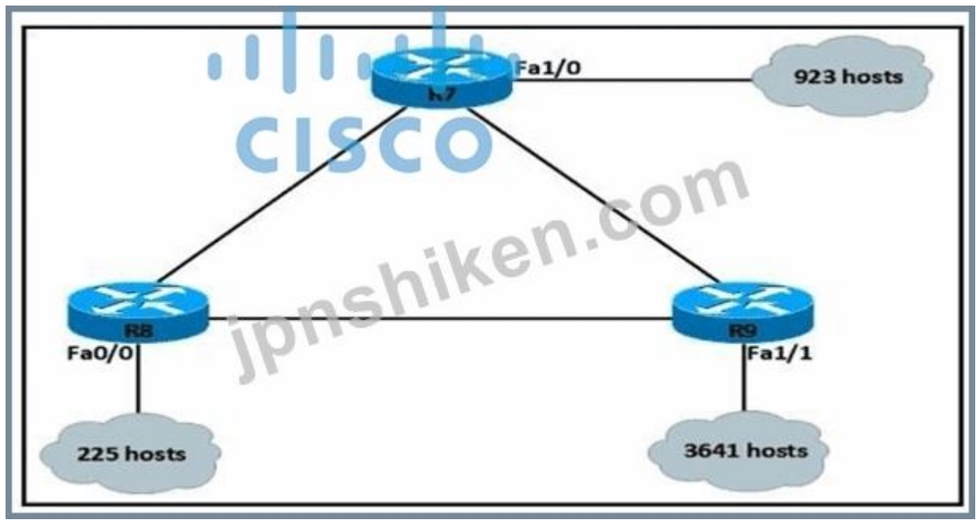
router ospf 10
router-id 10.10.1.86
network 10.10.1.86 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0

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

正解: (正解を表示します)

Option B. OSPF operation depends on area membership, network type, timers, router ID, priority, and whether a DR/BDR election occurs. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Incorrect choices either use the wrong OSPF role, omit a required adjacency condition, or apply a setting that does not affect the stated behavior. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: 266
展示資料を参照してください。



各ルータには、割り当てられたホスト数に見合う十分なIPアドレスを提供し、新規ホストの増加率が10%を超えないことを想定したIPサブネットを設定する必要があります。どの設定スクリプトを使用すべきでしょうか？

A.
```
R7#
configure terminal
interface Fa1/0
ip address 10.1.56.1 255.255.252.0
no shutdown

R8#
configure terminal
interface Fa0/0
ip address 10.9.32.1 255.255.255.0
no shutdown

R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1 255.255.240.0
no shutdown
```

B.
```
R7#
configure terminal
interface Fa1/0
ip address 10.1.56.1 255.255.248.0
no shutdown

R8#
configure terminal
interface Fa0/0
ip address 10.9.32.1 255.255.254.0
no shutdown

R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1 255.255.248.0
no shutdown
```

C.
```
R7#
configure terminal
interface Fa1/0
ip address 10.1.56.1 255.255.240.0
no shutdown

R8#
configure terminal
interface Fa0/0
ip address 10.9.32.1 255.255.224.0
no shutdown

R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1 255.255.192.0
no shutdown
```

D.
```
R7#
configure terminal
interface Fa1/0
ip address 10.1.56.1 255.255.192.0
no shutdown

R8#
configure terminal
interface Fa0/0
ip address 10.9.32.1 255.255.224.0
no shutdown

R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1 255.255.128.0
no shutdown
```

正解: (正解を表示します)

Option C. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **267**

エンジニアは、コア ルーターにバックアップ ルーターへのフローティング静的デフォルト ルートを設定する必要があります。
10.200.0.2. どのコマンドが要件を満たしていますか？

A. ip route 0.0.0.0 0.0.0.0 10.200.0.2 1
B. IPルート 0.0.0.0 0.0.0.0 10.200.0.2 フローティング
C. ip route 0.0.0.0 0.0.0.0 10.200.0.2
D. IPルート 0.0.0.0 0.0.0.0 10.200.0.2 10

正解: (正解を表示します)

Ip route 0.0.0.0 0.0.0.0 10.200.0.2 10. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol.
First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **268**

どのポートタイプが、追加設定なしでspanning-tree portfastコマンドをサポートしていますか？
A. アクセスポート
B. レイヤ3の主要インターフェース
C. レイヤー3サンインターフェース
D. トランクポート
正解: **(**正解を表示します**)**
access ports. Switching features such as trunks and EtherChannels are controlled by negotiation mode, encapsulation, VLAN membership, and whether the selected protocol is Cisco proprietary or standards based.
Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces.
The incorrect options either disable negotiation, select the wrong negotiation protocol, or configure a mode that cannot form the requested link under the stated conditions. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **269**
展示資料を参照してください。

```
R1# show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S* 0.0.0.0/0 is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.2.0/24 is directly connected, GigabitEthernet0/0
L        172.16.2.2/32 is directly connected, GigabitEthernet0/0
C        172.16.4.0/21 is directly connected, Serial0/0/1
L        172.16.8.2/26 is directly connected, Serial0/0/1
```

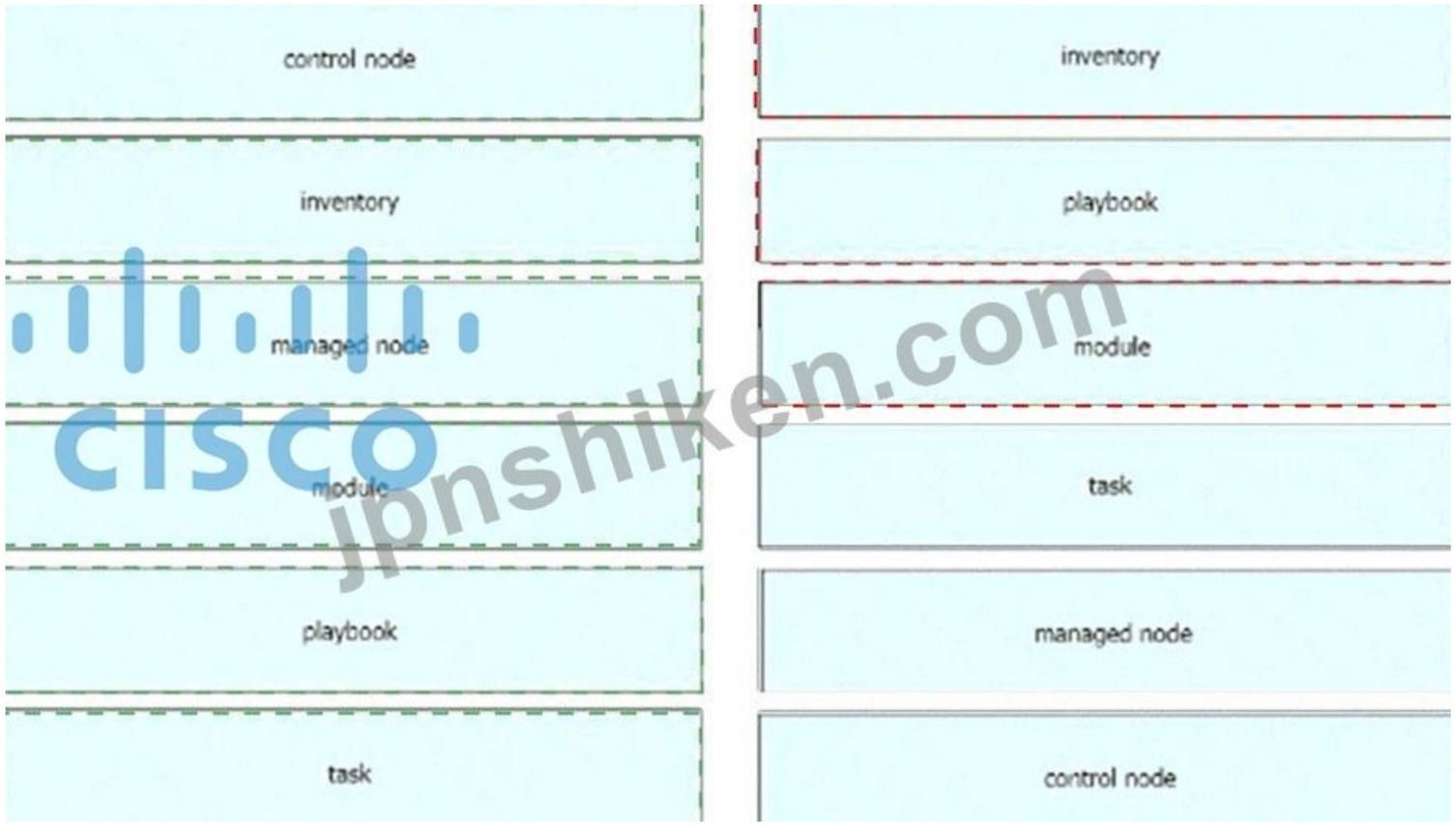
ルート172.16.4.0のサブネットマスクは何ですか？
A. 255.255.248.0
B. 255.255.254.0
C. 255.255.255.192
D. 255.255.240.0
正解: **A (**コメントを発表する**)**
255.255.248.0. Routing and redundancy questions are solved by applying longest-prefix match, administrative distance, metrics, and gateway-redundancy behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Incorrect choices point to the wrong next hop, choose the wrong route source, or confuse routing with Layer 2 behavior. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **270**
左側のAnsible用語を右側にドラッグアンドドロップしてください。

control node	collection of actions to perform on target devices, expressed in YAML format
inventory	device with Ansible installed that manages target devices
managed node	network device, without Ansible installed, upon which commands can be executed
module	specific action to be performed on one or more target devices
playbook	unit of Python code to be executed
task	Ansible file that defines the target devices upon which commands and tasks can be executed

cisco
ipnshiken.com

正解:

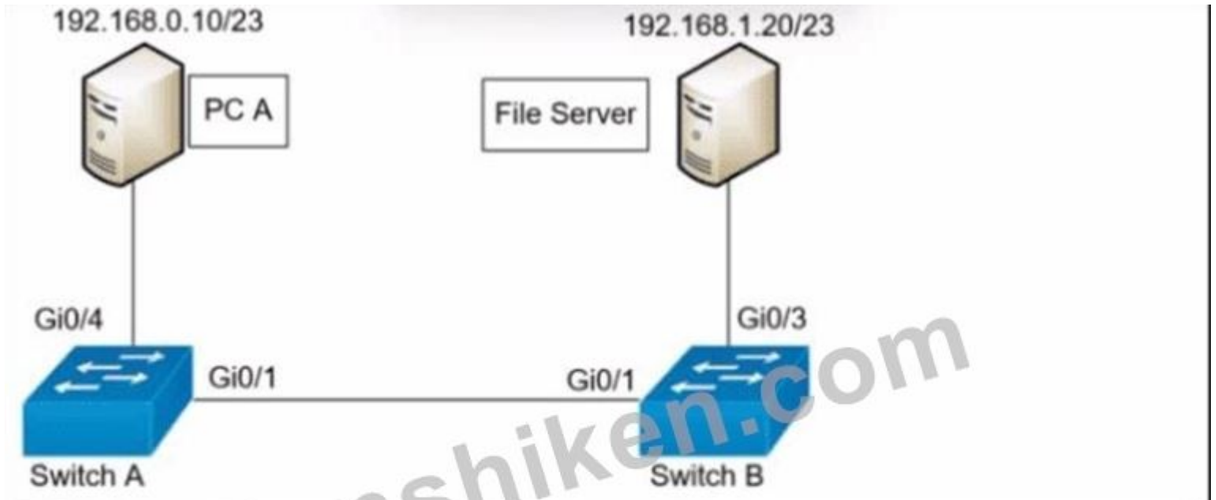


Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this form test whether each protocol, command, service, or architecture term is placed with the function it actually performs. The safest approach is to classify each item by operating layer and purpose before matching it: routing behavior belongs to IP connectivity, wireless modes belong to access, REST methods belong to automation, and AAA functions belong to security services. Several distractors are valid networking terms, but they become wrong when mapped to the wrong plane or protocol. The retained mapping follows Cisco terminology and reflects how the features are used in implementation and troubleshooting. In practice, this prevents mixing up forwarding behavior with management behavior or authentication with authorization/accounting. The mapping shown in the file is therefore retained as the verified response.

jpnshiken.com
cisco

質問: **271**
展示資料を参照してください。
PC Aとファイルサーバー。他の通信の中断を防ぐために、スイッチAで設定すべきコマンドはどれですか？



Switch A
Vlan 10,11,12,13

```
interface GigabitEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 10-12
!
interface GigabitEthernet0/4
 switchport access vlan 13
 switchport mode access
```

Switch B
Vlan 10,11,12,13

```
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/3
 switchport access vlan 13
 switchport mode access
```

A. スイッチポートトランクはVLAN 12を許可します
B. switchport trunk allowed vlan none
C. switchport trunk allowed vlan add 13
D. スイッチポートトランク許可VLAN削除10-11
正解: **(**正解を表示します**)**
switchport trunk allowed vlan add 13. Switching questions depend on MAC learning, VLAN membership, trunking, STP election, and EtherChannel behavior. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong answers misapply a Layer 2 rule or configure the wrong logical interface. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **272**

Perfect Forward Secrecy に依存するワイヤレス セキュリティ プロトコルはどれですか?
A. WPA3
B. WPA
C. WEP
D. WPA2
正解: (正解を表示します)
WPA3. WPA3 uses Simultaneous Authentication of Equals, or SAE, which improves password-based wireless authentication and provides protection associated with Perfect Forward Secrecy. WEP is obsolete and does not provide this property. WPA and WPA2 can use preshared keys or 802.1X methods, but WPA3 is the standard specifically associated with SAE and stronger protection against offline dictionary attacks. Cisco CCNA 200-301 v1.1 Network Access and Security Fundamentals require recognition of the difference between legacy WLAN security and WPA3 enhancements. Perfect Forward Secrecy means compromise of a long-term credential does not automatically expose earlier session keys. SAE is the mechanism that gives WPA3-Personal its major security improvement over WPA2-PSK. The original WEP answer was technically wrong and has been corrected to WPA3.

質問: **273**
RSAの特徴は何ですか？
A. 暗号化には事前共有鍵を使用します
B. 両方の側が同じ鍵を持っている必要があります
C. これは秘密鍵暗号化アルゴリズムです
D. これは公開鍵暗号システムです
正解: (正解を表示します)
It is a public-key cryptosystem. The answer follows from standard Cisco behavior and the operational clue in the scenario. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. The other choices are adjacent technologies or commands, but they do not meet the stated requirement.
In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco- consistent behavior for this item.

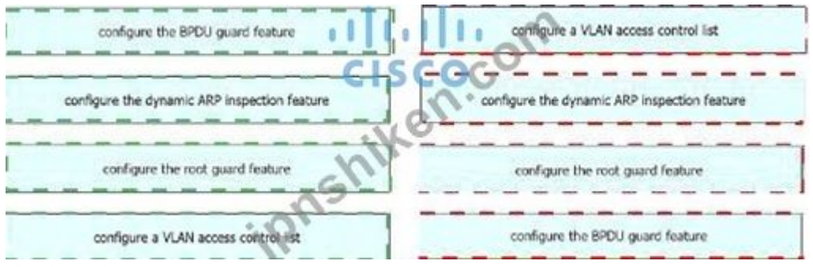
質問: **274**
パケットの状態をチェックして、パケットが正当かどうかを判断するネットワーク アプライアンスとは何ですか?
A. レイヤ 2 スイッチ
B. ロードバランサー
C. ファイアウォール
D. LAN コントローラー
正解: (正解を表示します)
The correct response is C. A firewall checks packets against security policy and, in stateful designs, connection state. It determines whether traffic is legitimate before allowing it between security zones or networks. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. Layer 2 switches forward frames, load balancers distribute sessions, and LAN controllers manage wireless infrastructure. When this appears in a network, the symptom normally confirms the answer:
the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **275**
OSPF は、ルーター R1 と R2 の間で構成する必要があります。

DR/BDR の選択を回避するために、ルーター R1 に適用する必要がある OSPF 構成はどれですか?
A. router ospf 1
network 192.168.1.1 0.0.0.0 area 0
interface e1/1
ip address 192.168.1.1 255.255.255.252
ip ospf network broadcast
B. router ospf 1
network 192.168.1.1 0.0.0.0 area 0
interface e1/1
ip address 192.168.1.1 255.255.255.252
ip ospf network point-to-point
C. router ospf 1
network 192.168.1.1 0.0.0.0 area 0
interface e1/1
ip address 192.168.1.1 255.255.255.252
ip ospf cost 0
D. router ospf 1
network 192.168.1.1 0.0.0.0 area 0
hello interval 15
interface e1/1
Ip address 192.168.1.1 255.255.255.252
正解: **B (コメントを発表する)**
router ospf 1network 192.168.1.1 0.0.0.0 area 0interface e1/1ip address 192.168.1.1 255.255.255.252ip ospf network point-to-point. OSPF operation depends on area membership, network type, timers, router ID, priority, and whether a DR/BDR election occurs. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Incorrect choices either use the wrong OSPF role, omit a required adjacency condition, or apply a setting that does not affect the stated behavior. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

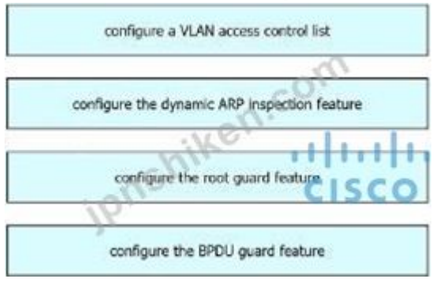
質問: **276**
左側の脅威軽減策を、右側のそれらが軽減する脅威または攻撃の種類にドラッグ＆ドロップしてください。

正解:



Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.



質問: **277**

2 層アーキテクチャの折りたたまれたコア レイヤによって実行される機能はどれですか?

A. ルーティング ポリシーの適用

B. データ ポリシーの対象トラフィックのマーキング

C. ユーザーをネットワークの端に接続する

D. セキュリティ ポリシーの適用

正解: **(**正解を表示します**)**

In a two-tier campus design, the core and distribution functions are collapsed into one layer. That collapsed core provides aggregation, Layer 3 boundaries, routing between access-layer blocks, and policy enforcement that would otherwise sit at the distribution layer. The access layer attaches users and endpoints; it is not the collapsed core ' s role. Marking interesting traffic can occur as part of QoS policy, but it is not the defining architectural function. Applying security policies may happen in some designs, but the answer that best describes collapsed-core responsibility is enforcing routing policies. Cisco CCNA 200-301 v1.1 Network Fundamentals expects candidates to compare two-tier and three-tier architectures. In small and medium campus networks, a collapsed core reduces complexity by combining distribution and core into the same devices. The key function in the answer set is routing-policy enforcement. Therefore, A is the best answer.

質問: **278**

ネットワーク管理者は、新しい無線ネットワークを構成する際に、アクセスポイントを自律モードで動作させるか、クラウドベースモードで動作させるかを決定する際に、どのような点を考慮すべきでしょうか？

自律モードのアクセスポイントは、クラウドベースモードのアクセスポイントに比べて、アンダーレイへの依存度は低いものの、メンテナンスがより複雑になります。

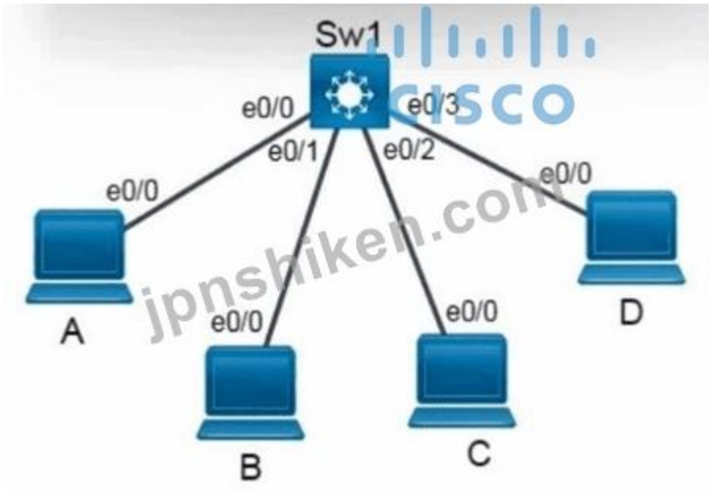
クラウドベースモードのアクセスポイントはアンダーレイに依存するため、自律モードのアクセスポイントよりも保守が複雑です。

A. クラウドベースモードのAPは導入は容易ですが、自律モードのAPよりも自動化が困難です。

B. 自律モードのアクセスポイントは、クラウドベースモードのアクセスポイントよりも簡単に展開および自動化できます。

正解: **A** (コメントを発表する)
Cloud-based mode APs are easy to deploy but harder to automate than APs in autonomous mode..
Wireless questions depend on AP mode, WLAN security, RF band selection, controller interfaces, and client roaming or authentication behavior. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong options confuse encryption with authentication, local switching with tunneling, or controller management with client data handling. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **279**
展示資料を参照してください。



ホストAのスイッチインターフェースはVLAN 2に設定されています。ホストDは、ホストAのIPアドレス宛てのユニキャストパケットを送信します。

```
Sw1#show mac-address table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
2       000c.859c.bb7b    DYNAMIC     e0/1
3       000c.859c.bb7b    DYNAMIC     e0/1
2       0010.11dc.3e91    DYNAMIC     e0/2
3       0010.11dc.3e91    DYNAMIC     e0/2
2       0043.49d4.c383    DYNAMIC     e0/3
Sw1#
```

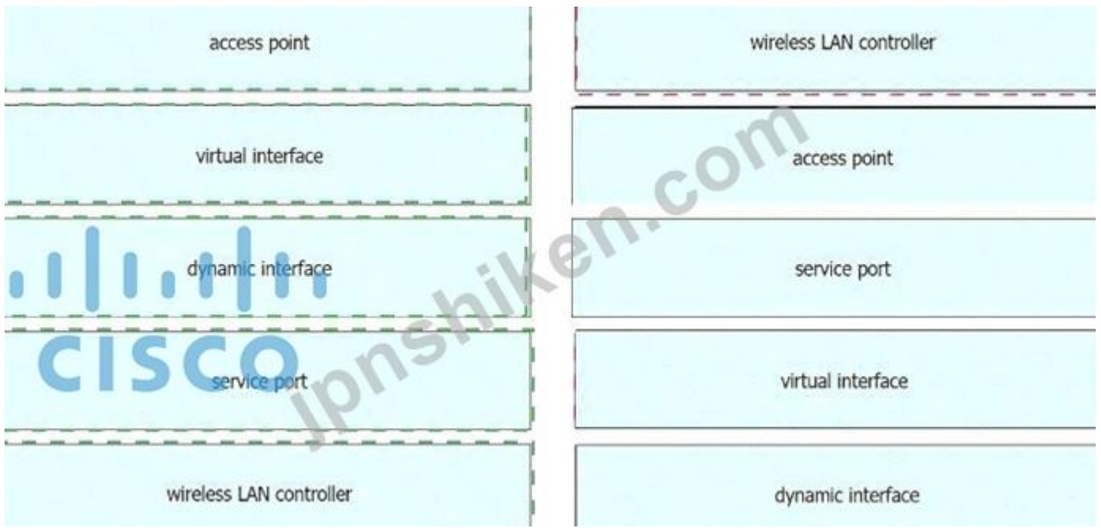
スイッチはホストDからフレームを受信すると、どのような動作をしますか？
A. 放送嵐を引き起こします。
B. スイッチのMACテーブルからフレームを削除します。
C. ソースポートをシャットダウンし、それをerr-disableモードにします。
D. 送信元ポートを除くすべてのポートからフレームをフラッディングします。
正解: (正解を表示します)
It floods the frame out of every port except the source port.. If the destination MAC address is missing from the switch MAC address table, the switch treats the frame as an unknown unicast. It floods the frame out ports in the same VLAN except the port on which it arrived. It does not err-disable the port, drop the frame from the table, or create a broadcast storm as the default behavior. Cisco CCNA 200-301 v1.1 Network Access expects candidates to know that VLAN boundaries still apply during flooding. Because host A is in VLAN 2, the switch floods only within VLAN 2, not through unrelated VLANs. The corrected answer is that the switch floods the frame out every eligible port except the source port.

質問: **280**
WLC上のどのインターフェースまたはポートが、インバンドデバイス管理およびコントローラとアクセスポイント間の通信のデフォルト設定になっていますか？
A. 仮想インターフェース
B. 管理インターフェース
C. コンソールポート
D. サービスポート
正解: **(**正解を表示します**)**
management interface. Wireless questions depend on AP mode, WLAN security, RF band selection, controller interfaces, and client roaming or authentication behavior. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong options confuse encryption with authentication, local switching with tunneling, or controller management with client data handling. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco- consistent behavior for this item.

質問: **281**
軽量モードの無線アクセスポイントの設定を変更するにはどうすればよいですか？
A. APの管理IPへのSSH接続
B. 親WLC経由のEoIP接続
C. 親WLC経由のCAPWAP/LWAPP接続
D. アクセスポイントの帯域外アドレスへのHTTPS接続
正解: **(**正解を表示します**)**
CAPWAP/LWAPP connection via the parent WLC. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco- consistent configuration or behavior for this wireless scenario.

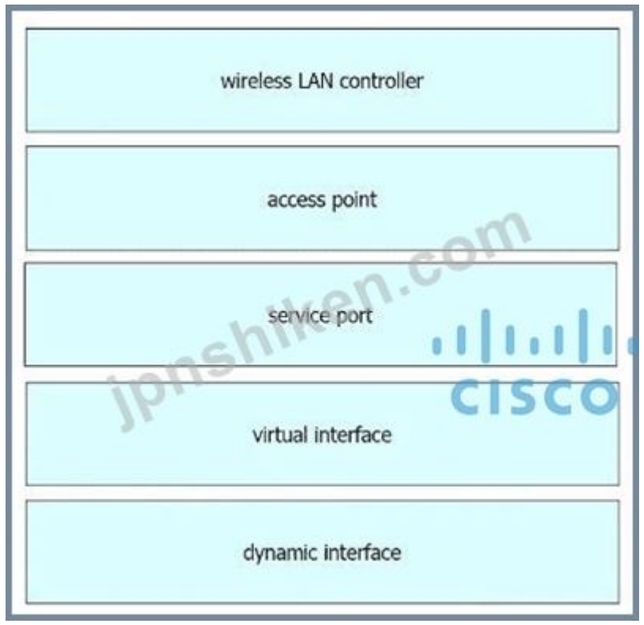
質問: **282**
左側のWLANコンポーネントを、右側のコンポーネント詳細にドラッグアンドドロップしてください。

正解:



Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this form test whether each protocol, command, service, or architecture term is placed with the function it actually performs. The safest approach is to classify each item by operating layer and purpose before matching it: routing behavior belongs to IP connectivity, wireless modes belong to access, REST methods belong to automation, and AAA functions belong to security services. Several distractors are valid networking terms, but they become wrong when mapped to the wrong plane or protocol. The retained mapping follows Cisco terminology and reflects how the features are used in implementation and troubleshooting. In practice, this prevents mixing up forwarding behavior with management behavior or authentication with authorization/accounting. The mapping shown in the file is therefore retained as the verified response.



質問: **283**

ネットワーク管理者は、ルーターR1へのリモートアクセス用にSSHを設定する必要があります。要件は、接続クライアントとの間で管理トラフィックを暗号化するために公開鍵と秘密鍵のペアを使用することです。

どの構成を適用すれば、要件を満たしますか？

```
t1#enable
t1#configure terminal
t1(config)#ip domain-name cisco.com
t1(config)#crypto key generate ec keysize 2048

t1#enable
t1#configure terminal
t1(config)#ip domain-name cisco.com
t1(config)#crypto key generate rsa modulus 1024

t1#enable
t1#configure terminal
t1(config)#ip domain-name cisco.com
t1(config)#crypto key generate ec keysize 1024

t1#enable
t1#configure terminal
t1(config)#ip domain-name cisco.com
t1(config)#crypto key encrypt rsa name myKey
```

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)

Option C. IP services questions test the exact function of infrastructure services such as addressing, name resolution, time synchronization, logging, monitoring, and secure management. Cisco CCNA 200-301 v1.1 includes this topic under IP Connectivity, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The distractors name valid services, but they provide a different service function from the one required in the

prompt. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **284**
宛先ネットワークへトラフィックを送信するために使用されるインターフェースはどれですか？
10.90.207.87/26 [110/1912] F0/7経由
10.90.207.87/26 [110/28968] F0/6経由
10.90.207.87/26 [120/14] F0/4経由
10.90.207.87/26 [120/11] F0/5経由
A. F0/7
B. F0/5
C. F0/4
D. F0/6
正解: **A (**コメントを発表する**)**
F0/7. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **285**
どのデバイスがトラフィックのステートフル検査を実行しますか？
A. ファイアウォール
B. スイッチ
C. アクセスポイント
D. ワイヤレスコントローラー
正解: **(**正解を表示します**)**
A firewall is the device class associated with stateful inspection. Stateful inspection tracks active sessions and uses connection state when deciding whether to permit return traffic or block unexpected packets. For example, if an internal host initiates a TCP session, the firewall can allow matching return traffic because it belongs to a known connection. A Layer 2 switch forwards frames based on MAC addresses and does not inspect transport-layer session state. An access point bridges wireless clients to the wired network, and a wireless controller manages AP behavior and WLAN policy, but neither is the generic stateful-inspection answer in this question. Cisco CCNA 200-301 v1.1 Security Fundamentals requires candidates to know common security device roles: firewall, WSA, AAA server, VPN headend, and access-layer controls. The key phrase is stateful inspection of traffic. That points directly to a firewall. The correct answer is A.

質問: **286**
DNS ルックアップ操作とは何ですか?
A. DNS サーバーは宛先に ping を送信して、宛先が使用可能であることを確認します。
B. 宛先ポート 53 経由でリクエストを処理します
C. プライマリ IP がダウンしている場合、DNS サーバーはクライアントを代替 IP アドレスに転送します。
D. IP アドレスから DNS サーバーへのドメイン名解決の要求に応答します。

正解: (正解を表示します)
Answer D is the technically correct selection. A DNS lookup resolves a name query or reverse query by asking DNS infrastructure for the matching value. In normal client use, DNS translates a hostname into an IP address so the application can connect to the destination. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. DNS does not ping the destination, act as an HA redirector by default, or merely define port 53 service behaviour. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **287**
SNMPv3 の使用を意味するコマンドはどれですか?
A. snmp サーバー ホスト
B. snmp-server コミュニティ
C. snmp-server enable トラップ
D. SNMP サーバー ユーザー
正解: **D** (コメントを発表する)
snmp-server user. SNMPv3 introduces user-based security, authentication, and optional encryption. The command snmp-server user is therefore the command that implies SNMPv3 because users are created for SNMPv3 security models. The snmp-server community command is associated with SNMPv1 and SNMPv2c community strings, which are weaker and do not provide the same authentication and privacy capabilities.
The snmp-server host and snmp-server enable traps commands can be used in broader SNMP configurations, but they do not by themselves identify SNMPv3. Cisco CCNA 200-301 v1.1 IP Services expects engineers to know that SNMPv3 is the secure version preferred for device monitoring. The original community-string answer was wrong and has been corrected to snmp-server user.

質問: **288**

図を参照してください。ルーターR1、R2、R3は、プロトコルを使用して、隣接ルーターのIPアドレス、ハードウェアプラットフォーム、およびソフトウェアバージョンを識別します。ネットワークエンジニアは、R2がR3と隣接ルーターの情報を共有しないように設定し、R1との関係を維持する必要があります。この要件を満たすアクションは何ですか？
A. gO/2 で no cdp enable コマンドを設定します。
B. no cdp run コマンドをグローバルに設定します。
C. no lldp run コマンドをグローバルに設定します。
D. gQV1 で no lldp receive コマンドを設定します。
正解: (正解を表示します)

Configure the no cdp enable command on gO/2.. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **289**

図を参照してください。WLAN上のクライアントは802.11rを使用する必要があります。この要件を満たすために、どのような対策を講じる必要がありますか？

A. 高速移行オプションを有効にし、認証キー管理でFT 802.1Xを有効にします。

B. 高速トランジションオプションとWPA gik-randomize Stateを無効にするように設定します。

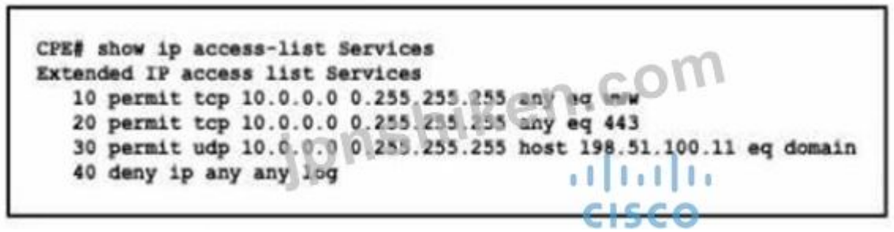
C. 保護管理フレームの下で、PMF オプションを 必須」に設定します。

D. 認証キー管理でCCKMを有効にする

正解: (正解を表示します)

Set the Fast Transition option to Enable and enable FT 802.1X under Authentication Key Management. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **290**



図を参照してください。このACLは、クライアントがHTTP、HTTPS、およびDNSサービスにUDP経由でのみアクセスできるように構成されています。新しい管理者は、DNSサービスへのTCPアクセスを追加したいと考えています。どの構成がACLを効率的に更新しますか？

A. ip access list extended Services35 permit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain

B. no ip access list extended Servicesip access list extended Services30 permit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain

C. ip access list extended Servicespermit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain

D. 拡張されたIPアクセスリストサービスはありません。拡張されたIPアクセスリストサービス。udpを許可 10.0.0.0 0.255.255.255 any eq 53。tcpを許可 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain。ipを拒否 任意の任意のログ

正解: **(**正解を表示します**)**

ip access list extended Services35 permit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **291**

図を参照してください。左側のサブネットマスクを、右側の対応するサブネットにドラッグアンドドロップしてください。
すべてのサブネットマスクが使用されているわけではありません。

正解:

Explanation:

Cisco CCNA 200-301 v1.1 expects these items to be matched by function, protocol layer, scope, and operational role rather than by keyword similarity. The reliable method is to identify what each item actually does in a Cisco network: whether it forwards traffic, manages a device, secures access, assigns addressing, identifies a resource, or carries control information. Distractors in this format are usually valid networking terms placed under the wrong category. That is why the retained mapping is important; it keeps protocol behavior, device function, and service purpose aligned. In a real network, mixing these concepts leads to broken routing, failed wireless access, insecure management, or automation calls aimed at the wrong interface. The mapping shown in the document is therefore retained as the Cisco-consistent answer for this item.

質問: **292**

Cisco Wireless LAN Controller を使用する利点は何ですか?

A. AP の集中管理には、より複雑な構成が必要です。

B. 一意の SSID は同じ認証方法を使用できません

C. 自律的で軽量な AP をサポート

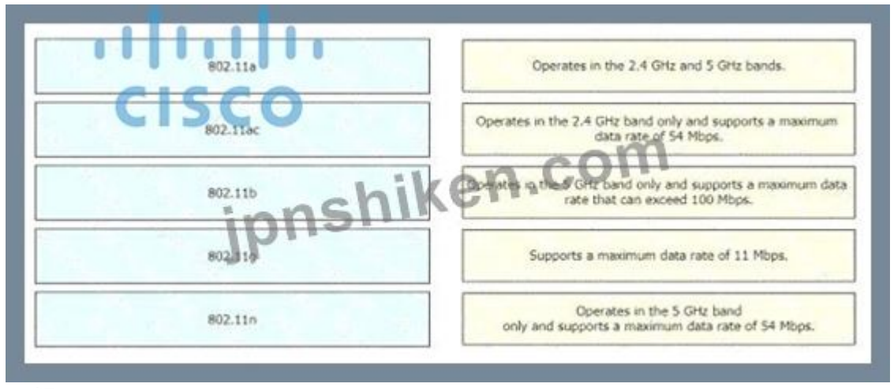
D. 各アクセス ポイントを個別に設定する必要がなくなります。

正解: **(**正解を表示します**)**

A Cisco Wireless LAN Controller centralizes access point management, which is the operational benefit described in option D. In a controller-based WLAN, lightweight APs join the WLC, download configuration, receive policy, and tunnel or switch client traffic according to the deployment model. That removes the need to configure every AP independently, which is exactly the pain point a WLC is designed to solve in enterprise wireless. Option A is backwards because central management normally reduces repeated per-AP configuration. Option B is false because multiple WLANs can use similar authentication methods while still using different SSIDs and policies. Option C is not the best answer because WLCs manage lightweight APs; autonomous APs are independently configured and do not rely on the same controller model. CCNA 200-301 v1.1 Network Access expects candidates to understand controller-based wireless architecture and the role of APs versus WLCs. Reference: Cisco wireless controller and lightweight AP deployment documentation.

質問: **293**
環境における Opportunistic Wireless Encryption の機能は何ですか?
A. 提供圧縮
B. WEP 接続を使用してセキュリティを強化する
C. 認証を提供する
D. オープン ネットワーク上のトラフィックを保護する
正解: **(**正解を表示します**)**
protect traffic on open networks. Wireless operation depends on WLAN identity, AP mode, RF management, client authentication, and controller-based policy enforcement. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The distractors confuse WLAN names, authentication, encryption, RF optimization, and controller management functions. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **294**
左側の802.11無線規格を右側の対応する説明文にドラッグアンドドロップしてください。



cisco
ipnshiken.com
正解:

Explanation:

Use the displayed drag-and-drop mapping for this item. 802.11 standards differ by frequency band, maximum theoretical rate, modulation, and channel width. The mapping should separate legacy 802.11b/g 2.4-GHz behaviour, 802.11a 5-GHz behaviour, and newer high-throughput standards such as 802.11n/ac. In Cisco CCNA 200-301 v1.1, Network Fundamentals questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. Confusing band support with throughput is the usual trap in this question type. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **295**

エンジニアがVoIPハンドセットに接続されているスイッチポートを設定しています。音声VLAN 4で手動で割り当てられたMACアドレスabcd.abcd.abcdを使用してポートセキュリティを有効にするには、エンジニアはどのコマンドを設定する必要がありますか？

A. スイッチポート ポートセキュリティ MACアドレス abcd.abcd.abcd

B. switchport port-security mac-address abed.abed.abed vlan 4

C. switchport port-security mac-address sticky abcd.abcd.abcd vlan 4

D. switchport port-security mac-address abcd.abcd.abcd vlan voice

正解: **D (**コメントを発表する**)**

switchport port-security mac-address abcd.abcd.abcd vlan voice. Cisco port security can bind a secure MAC address specifically to the access VLAN or to the voice VLAN. Because the handset is using voice VLAN 4, the manually assigned secure MAC must be applied with the vlan voice keyword. Adding only the MAC address does not identify the voice VLAN context. Using a numeric VLAN value in this syntax is

not the correct way to identify the voice VLAN for port-security binding. Sticky learning is also wrong because the question asks for a manually assigned MAC address. Cisco CCNA 200-301 v1.1 Network Access expects engineers to distinguish data VLAN and voice VLAN behavior on the same switch port. The corrected command is switchport port-security mac-address abcd.abcd.abcd vlan voice.

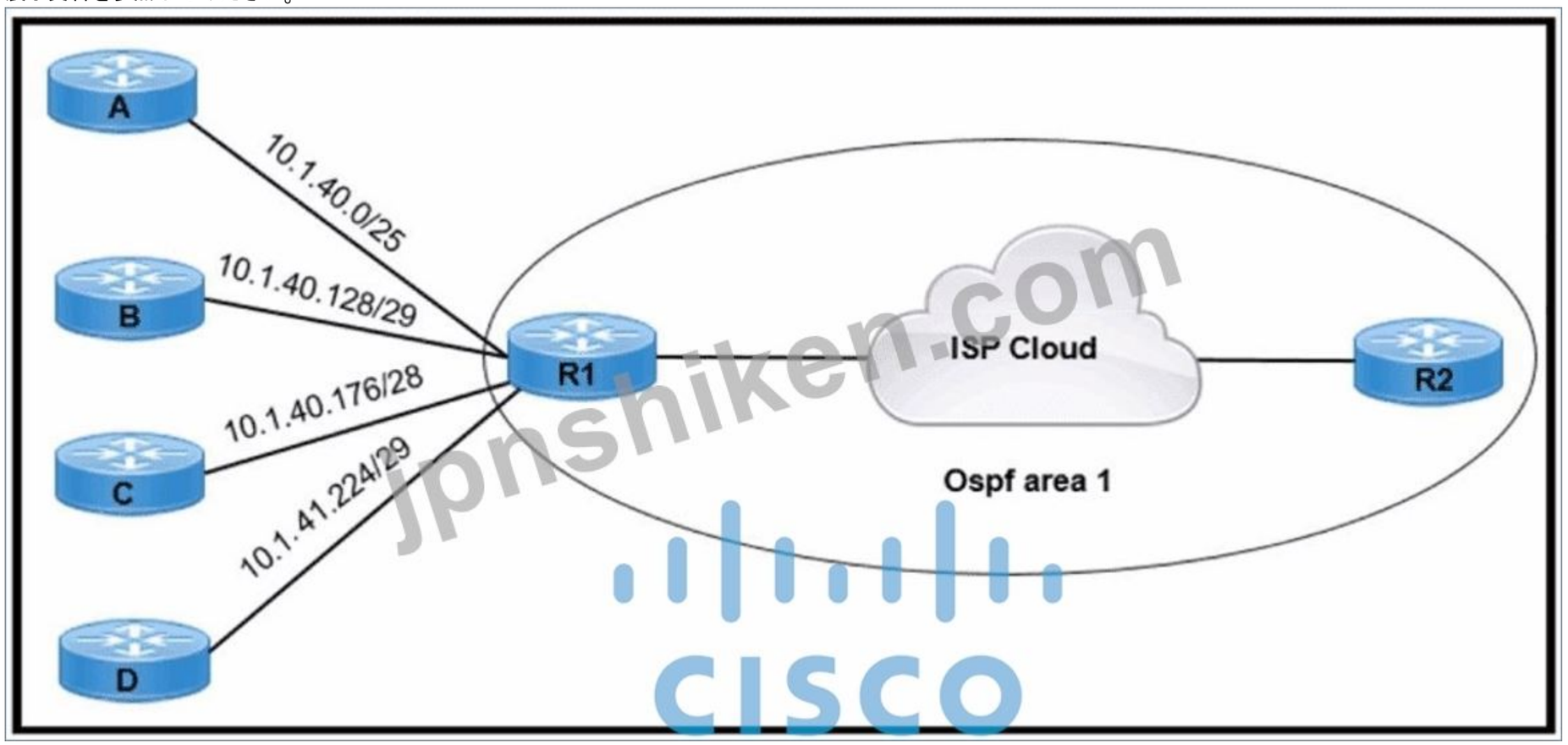
質問: **296**
AireOS GUIを使用する際に、コントローラー管理ページを同時に閲覧できるユーザーの総数はいくつですか？
A. 2
B. 5
C. 8
D. 9
正解: (正解を表示します)
8. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE. JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact with a controller, while southbound APIs allow the controller to communicate with network devices. NETCONF and RESTCONF are configuration/management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to-device communication with application-to-controller communication or confuse a data format with a protocol. Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers. The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

質問: **297**
エンジニアは、本社ルーターのシリアル 0/0 インターフェイスで IPv6 アドレス 2001:0db8:0000:0000:0700:0003:400F:572B を構成する必要があり、構成を容易にするために圧縮する必要があります。
ルーター インターフェイスで発行する必要があるコマンドはどれですか?
A. ipv6 アドレス 2001:db8::700:3:400F:572B
B. ipv6 アドレス 2001:db8:0::700:3:4F:572B
C. ipv6 アドレス 2001:Odb8::7:3:4F:572B
D. ipv6 アドレス 2001::db8:0000::700:3:400F:572B
正解: (正解を表示します)
Use A for this item. IPv6 compression removes leading zeros in each hextet and compresses one longest contiguous run of zero hextets with double colon. The address 2001:0db8:0000:0000:0700:0003:400F:572B becomes 2001:db8::700:3:400F:572B. In Cisco CCNA 200-301 v1.1, Network Fundamentals questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. The double colon cannot be used twice, and nonzero hextets such as 400F cannot be shortened to 4F. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **298**
Cisco ONA Center が従来のキャンパス管理よりも優れているのはどれですか?
A. Cisco DNA Center は暗号化された管理に SNMPv3 を活用し、従来のキャンパス管理は SNMPv2 を使用します。
B. Cisco DNA Center は安全な Web アクセスのために HTTPS を自動化し、従来のキャンパス管理では HTTP を使用します。
C. Cisco DNA Center は API を活用しており、従来のキャンパス管理では手動でデータを収集する必要があります。
D. Cisco DNA Center は暗号化されたエントリの SSH アクセスを自動化し、SSH は従来のキャンパス管理には存在しません。
正解: (正解を表示します)
Cisco DNA Center leverages APIs, and traditional campus management requires manual data gathering..
Cisco DNA Center provides a major advantage by exposing APIs and using a controller-based model to collect, analyze, and act on network information. Traditional campus management is often manual, device-by- device, and CLI-centered. The advantage is not merely HTTPS or SNMP version selection; those are individual management transport choices. Cisco CCNA 200-301 v1.1 Automation and

Programmability expects engineers to understand that DNA Center changes the management model by using software-defined workflows, APIs, automation, and assurance. The corrected answer is that Cisco DNA Center leverages APIs, while traditional campus management requires more manual data gathering. That is the clearest contrast between a controller-based management platform and conventional operations.

質問**: 299**
展示資料を参照してください。



ルータ R1 はルータ A、B、C、D から静的ルーティングアップデートを受信します。ネットワーク エンジニアは、R1 が OSPF エリア 1 で静的ルートをアドバタイズするようにしたいと考えています。OSPF でアドバタイズする必要がある nary アドレスはどれですか?

A. 10.1.40.0/25
B. 10.1.40.0/24
C. 10.1.40.0/23
D. 10.1.41.0/25

正解**: C (**コメントを発表する**)**

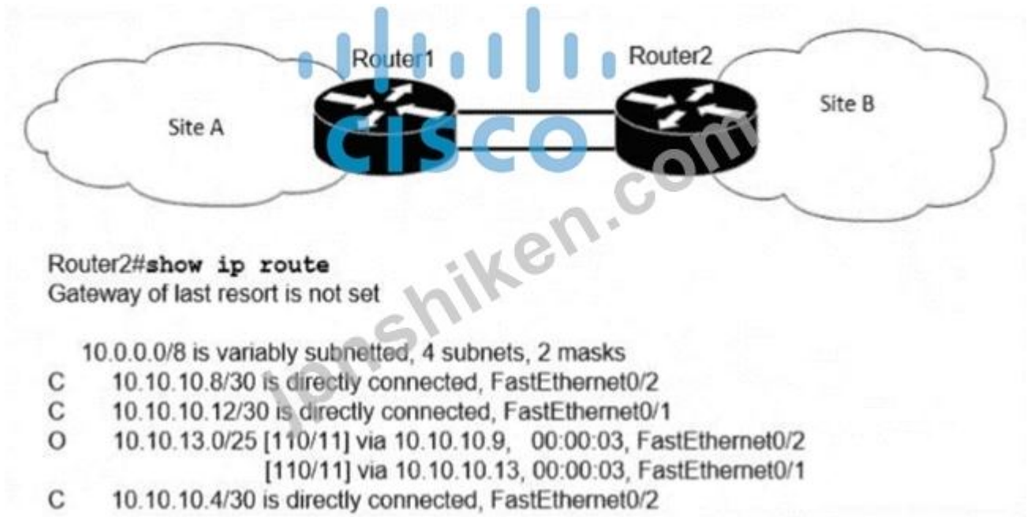
10.1.40.0/23. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.

The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **300**
展示資料を参照してください。

オブジェクト、キー、JSDNリストの値はそれぞれいくつ存在しますか？
A. 3つのオブジェクト、2つのキー、および3つのJSDNリスト値
B. 3つのオブジェクト、3つのキー、および2つのJSDN MI値
C. オブジェクト1つ、キー3つ、JSDNリスト値3つ
D. オブジェクト1つ、キー3つ、JSDNリスト値2つ
正解: **(正解を表示します)**
one object, three keys, and three JSDN list values. The answer follows from standard Cisco behavior and the operational clue in the scenario. Cisco CCNA 200-301 v1.1 includes this under Automation and Programmability, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. The other choices are adjacent technologies or commands, but they do not meet the stated requirement. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **301**
展示資料を参照してください。

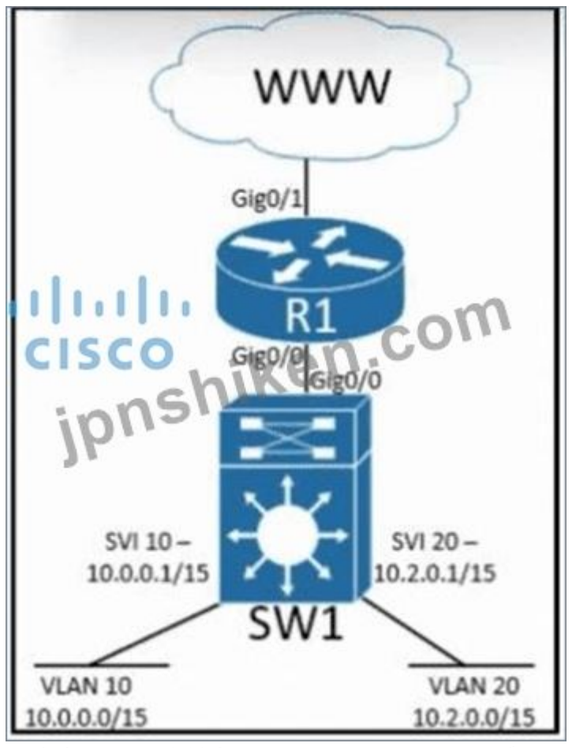


このネットワークでOSPFが動作している場合、ルーター2はサイトBからサイトAの10.10.13.128/25へのトラフィックをどのように処理しますか？

A. Fa0/1とFa0/2からのトラフィックを負荷分散します。
B. 到達不能であるため、トラフィックを破棄します。
C. インターフェース Fa0/2 からパケットを送信します。
D. インターフェース Fa0/1 からパケットを送信します。
正解: (正解を表示します)
The correct response is B. Router2 can forward only to networks that exist in its routing table or match a less- specific usable route. If the OSPF database and routing table contain 10.10.13.0/25 but not 10.10.13.128/25, traffic for the second half of that /24 has no valid match and is discarded. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. Load balancing requires equal- cost valid routes to the same prefix; forwarding out either interface would require a matching route that the scenario does not provide. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **302**



図を参照してください。VLAN間ルーティングはSW1で設定されています。クライアントAはVLAN内でLinuxをOSとして実行しています。
クライアントAはデフォルトゲートウェイIPアドレス10.0.0.1を使用していますが、Windowsを実行しているVLAN 20内のクライアントBにpingを実行できません。クライアントAのIP設定が正しいことを確認するには、どのような操作が必要ですか？

A. クライアント A で ipconfig コマンドを実行し、IP アドレスがホストの範囲内にあることを確認します。
10.0.0.1 - 10.0.255.254。
B. クライアント A で ifconfig コマンドを実行して、その IP アドレスとサブネット マスクが 255.254.0.0 の範囲内にあることを確認します。
C. クライアント A で ipconfig コマンドを実行して、正しい 10.0.0.1 デフォルト ゲートウェイが使用されていることを確認します。
D. クライアント A で ifconfig コマンドを実行して、サブネット マスクが 255.255.128.0 に設定されていることを確認します。
正解: **B (**コメントを発表する**)**
Run the ifconfig command on client A to confirm that its IP and subnet mask fall within 255.254.0.0.. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **303**
展示資料を参照してください。

```
{
    "SW1" : ["Ten-GigabitEthernet0/0", "Ten-GigabitEthernet0/1"],
    "SW2" : ["Ten-GigabitEthernet0/0", "Ten-GigabitEthernet0/1"],
    "SW3" : ["Ten-GigabitEthernet0/0", "Ten-GigabitEthernet0/1"],
    "SW4" : ["Ten-GigabitEthernet0/0", "Ten-GigabitEthernet0/1"]
}
```

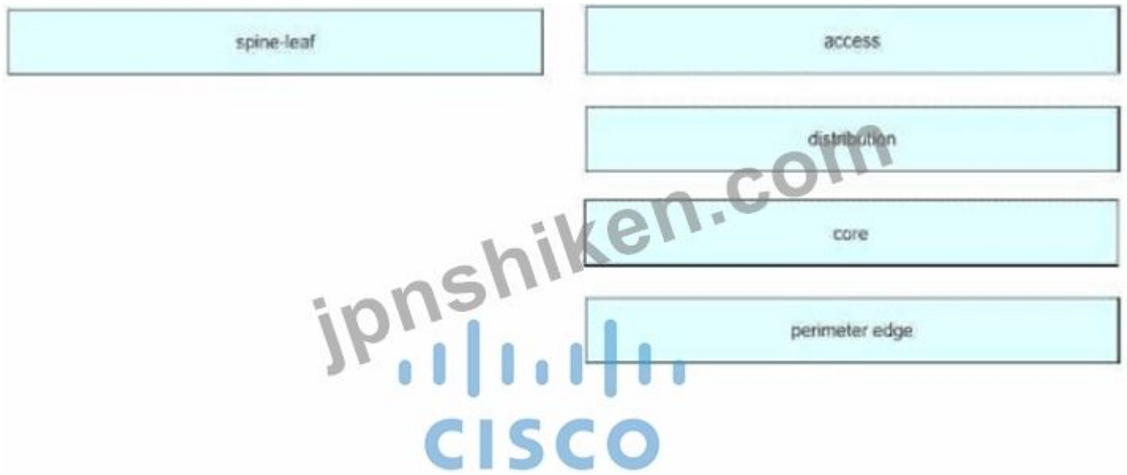
JSONオブジェクトはいくつ表示されますか？
A. 1
B. 2
C. 3
D. 4
正解: **(**正解を表示します**)**
4. Automation questions require recognizing data structures, HTTP methods, APIs, controllers, and the separation of northbound and southbound communication. Cisco CCNA 200-301 v1.1 includes this under Automation and Programmability, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function.
Distractors mix application-facing and device-facing roles or confuse values, keys, arrays, and objects. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **304**
左側のネットワークトポロジーアーキテクチャタイプを、右側の対応する機能にドラッグアンドドロップしてください。すべてのアーキテクチャタイプが使用されるわけではありません。

正解:

Explanation:

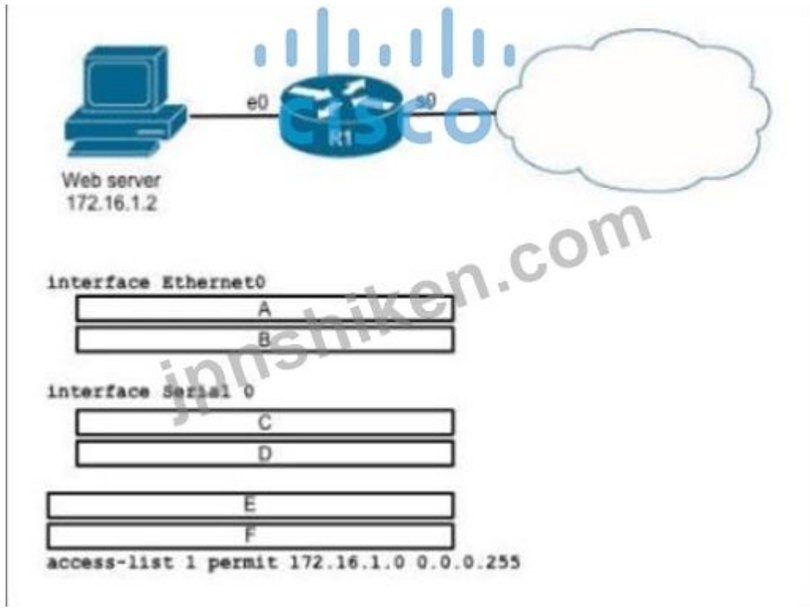
Cisco CCNA 200-301 v1.1 expects these items to be matched by function, protocol layer, scope, and operational role rather than by keyword similarity. The reliable method is to identify what each item actually does in a Cisco network: whether it forwards traffic, manages a device, secures access, assigns addressing, identifies a resource, or carries control information. Distractors in this format are usually valid networking terms placed under the wrong category. That is why the retained mapping is important; it keeps protocol behavior, device function, and service purpose aligned. In a real network, mixing these concepts leads to broken routing, failed wireless access, insecure management, or automation calls aimed at the wrong interface. The mapping shown in the document is therefore retained as the Cisco-consistent answer for this item.



jpnshiken.com
CISCO

質問: **305**
Cisco DNA Centerの総合健全性ダッシュボードの機能は何ですか？
A. 世界の主要10の課題の概要を提供します。
B. ネットワーク上の 10 台のデバイスとユーザーの詳細なアクティビティ ログを提供します。
C. ネットワーク上の各無線デバイスの動作状態を要約します。
D. ネットワーク内のサーバーとワークステーションの日次および週次のCPU使用率を要約します。
正解: **A** (コメントを発表する)
The correct response is A. Cisco DNA Center health dashboards summarize significant network issues so operators can prioritize remediation. The Overall Health view is meant to surface broad client, device, and network status information rather than raw host CPU charts. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. Detailed logging for only ten devices or wireless-only summaries does not describe the overall dashboard function. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **306**
展示資料を参照してください。



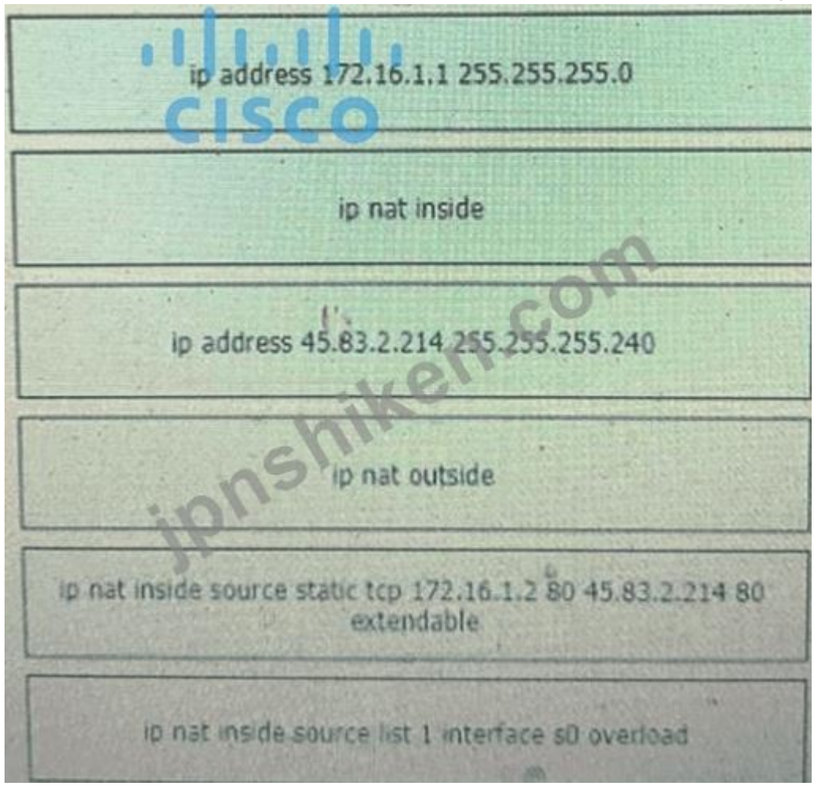
エンジニアがルーターを設定して、Webサーバーに静的NATを提供します。左側の設定コマンドを、右側の設定における対応する文字にドラッグアンドドロップしてください。

正解:

Explanation:

Use the displayed drag-and-drop mapping for this item. Static NAT creates a fixed one-to-one translation between an inside local address and an inside global address. The router must identify inside and outside interfaces and define the translation so the web server can be reached through the mapped address. In Cisco CCNA 200-301 v1.1, IP Services questions frequently test the practical boundary between similar features:

what the feature does, where it is configured, and what problem it is meant to solve. Dynamic NAT and PAT do not provide the same permanent server mapping unless configured specifically for static service translation. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.



質問: **307**
物理的な配線はすべて完了しています。ある企業は新たに32か所の拠点を展開する予定です。
これらのサイトでは、IPv4とIPv6の両方のネットワークが利用されます。
1. サブネット要件を満たし、最大化するためにサブネット172.25.0.0/16を使用する
ホストの数
2番目のサブネットを使用する
* Sw1O1のe0/0に最初の使用可能なIPアドレスを割り当てます。
* Sw102のe0/0に最後に使用可能なIPアドレスを割り当てます。
2. サブネット要件を満たし、最大限に活用するためのサブネット
ホストの数
c 2番目のサブネットを使用する
* 一意の64ビットインターフェイス識別子を使用してIPv6 GUAを割り当てます
Sw101のe0/0で
* 一意の64ビットインターフェイス識別子を使用してIPv6 GUAを割り当てます
swi02 の eO/O 上
ガイドライン
これは、仮想デバイス上でタスクを実行する実験課題です。
* この実験項目のタスクを確認するには、タスク」タブを参照してください。
* デバイスコンソールにアクセスしてタスクを実行するには、トポロジー」タブを参照してください。
* コンソールへのアクセスは、デバイスアイコンをクリックするか、コンソールウィンドウの上にあるタブを使用することで、必要なすべてのデバイスで利用できます。
必要な事前設定はすべて完了しました。
* デバイスの有効化パスワードやホスト名を変更しないでください。
次の項目に進む前に、設定をNVRAMに保存してください。
* 画面下部の 次へ」をクリックして、この実験を提出し、次の問題に進んでください。
* 次へ」をクリックすると、ラボが閉じられ、再度開くことはできません。

正解:
See the Explanation for the solution.
Explanation:
To subnet 172.25.0.0/16 to meet the subnet requirements and maximize the number of hosts, you need to determine how many bits you need to borrow from the host portion of the address to create enough subnets for 32 sites. Since 32 is 2^5, you need to borrow 5 bits, which means your new subnet mask will be /21 or

255.255.248.0. To find the second subnet, you need to add the value of the fifth bit (32) to the third octet of the network address (0), which gives you 172.25.32.0/21 as the second subnet. The first usable IP address in this subnet is 172.25.32.1, and the last usable IP address is 172.25.39.254.
To assign the first usable IP address to e0/0 on Sw101, you need to enter the following commands on the device console:
Sw101#configure terminal Sw101(config)#interface e0/0 Sw101(config-if)#ip address 172.25.32.1
255.255.248.0 Sw101(config-if)#no shutdown Sw101(config-if)#end
To assign the last usable IP address to e0/0 on Sw102, you need to enter the following commands on the device console:
Sw102#configure terminal Sw102(config)#interface e0/0 Sw102(config-if)#ip address 172.25.39.254
255.255.248.0 Sw102(config-if)#no shutdown Sw102(config-if)#end
To subnet an IPv6 GUA to meet the subnet requirements and maximize the number of hosts, you need to determine how many bits you need to borrow from the interface identifier portion of the address to create enough subnets for 32 sites. Since 32 is 2^5, you need to borrow 5 bits, which means your new prefix length will be /69 or ffff:ffff:ffff:fff8::/69 (assuming that your IPv6 GUA has a /64 prefix by default). To find the second subnet, you need to add the value of the fifth bit (32) to the fourth hextet of the network address (0000), which gives you xxxx:xxxx:xxxx:0020::/69 as the second subnet (where xxxx:xxxx:xxxx is your IPv6 GUA prefix). The first and last IPv6 addresses in this subnet are xxxx:xxxx:xxxx:0020::1 and xxxx:xxxx:
xxxx:0027:ffff:ffff:ffff:fffe respectively.
To assign an IPv6 GUA using a unique 64-bit interface identifier on e0/0 on Sw101, you need to enter the following commands on the device console (assuming that your IPv6 GUA prefix is 2001:db8::/64):
Sw101#configure terminal Sw101(config)#interface e0/0 Sw101(config-if)#ipv6 address 2001:db8::20::1/69 Sw101(config-if)#no shutdown Sw101(config-if)#end To assign an IPv6 GUA using a unique 64-bit interface identifier on e0/0 on Sw102, you need to enter the following commands on the device console (assuming that your IPv6 GUA prefix is 2001:db8::/64):
Sw102#configure terminal Sw102(config)#interface e0/0 Sw102(config-if)#ipv6 address 2001:db8::27::fffe
/69 Sw102(config-if)#no shutdown Sw102(config-if)#end

質問**: 308**
Rapid PVST+に おける共有LANセグメント上のバックアップポートの動作モードと役割は何ですか？
A. 転送モードであり、各 VLAN のルートブリッジへの最低コストパスを提供します。
B. 学習モードであり、LAN から離れたルートブリッジへの最短経路を提供し、トラフィックを処理します。
C. ブロッキングモードであり、指定されたブリッジへの代替パスを提供する。
D. リスニングモードであり、ルートブリッジへの代替パスを提供する
正解**: (**正解を表示します**)**
blocking mode and provides an alternate path toward the designated bridge. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation.
Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol:
LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

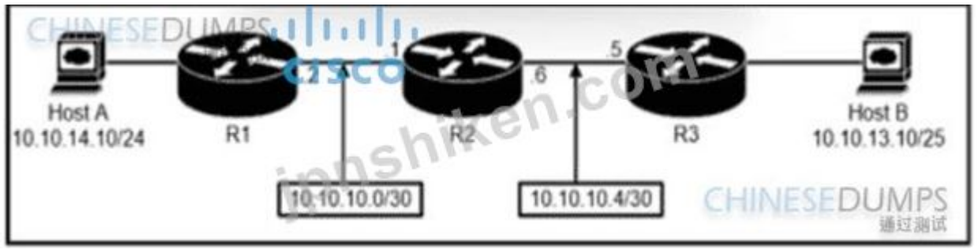
質問**: 309**
Cisco ワイヤレス LAN コントローラの GUI で WPA2 PSK を使用して WLAN を設定する場合、どの 2 つの形式を選択できますか? (2つ選んでください)
A. アスキー
B. base64
C. バイナリ
D. 10 進数

E. 16 進数
正解: (正解を表示します)
Cisco WLC WPA2-PSK configuration supports a pre-shared key entered either as ASCII text or as a hexadecimal key. ASCII is the human-readable passphrase format administrators normally use, while hexadecimal is the raw key representation. Base64, binary, and decimal are not the WLC PSK input formats for this configuration task. This question is easy to miss because it is asking about the selectable key formats in the Cisco Wireless LAN Controller GUI, not about the WPA2 cipher itself. Under CCNA 200-301 v1.1 Network Access, candidates are expected to recognize basic WLAN security configuration elements, including WPA2, PSK, SSID, and wireless controller settings. In practice, using ASCII simplifies administration, while hexadecimal is useful when a precise key value must be supplied. The verified choices are therefore A and E. Reference: Cisco Wireless LAN Controller WLAN security configuration guidance for WPA/WPA2 pre-shared keys.

質問: **310**
SDNコントローラによって集中管理されるのはどのプレーンですか？
A. 管理プレーン
B. 制御プレーン
C. データプレーン
D. サービスプレーン
正解: (正解を表示します)
control-plane. Automation and controller-based networking require separating APIs, management-plane actions, data formats, and centralized control from traditional device-by-device configuration. Cisco CCNA
200-301 v1.1 includes this under Automation and Programmability, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong options mix northbound and southbound roles, control and data plane functions, or automation outcomes with unrelated technologies. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control- plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **311**
ネットワーク操作における TFTP の機能は何ですか?
A. ユーザー名とパスワードを使用して、バックアップ構成ファイルをサーバーからスイッチに転送します。
B. ルーター上のファイル システム間でファイルを転送する
C. 輻輳したリンク上のサーバーからルーターに構成ファイルを転送します
D. ファームウェアのアップグレードのためにサーバーからルーターに IOS イメージを転送します。
正解: (正解を表示します)
transfers IOS images from a server to a router for firmware upgrades. Security fundamentals questions test the boundary between identity, authorization, accounting, encryption, inspection, and access-control functions.
Cisco CCNA 200-301 v1.1 includes this topic under IP Services, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces.
The other answers confuse identity checking with traffic filtering, or they assign the correct security idea to the wrong device or protocol. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **312**



図を参照してください。エンジニアは、ホストAとホストBが通信できるように、2つのネットワーク間に静的ネットワークルートを設定する必要があります。左側のコマンドを、右側の設定が必要なルーターにドラッグアンドドロップしてください。すべてのコマンドを使用するわけではありません。

正解:

Explanation:
Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this form test whether each protocol, command, service, or architecture term is placed with the function it actually performs. The safest approach is to classify each item by operating layer and purpose before matching it: routing behavior belongs to IP connectivity, wireless modes belong to access, REST methods belong to automation, and AAA functions belong to security services. Several distractors are valid networking terms, but they become wrong when mapped to the wrong plane or protocol. The retained mapping follows Cisco terminology and reflects how the features are used in implementation and troubleshooting. In practice, this prevents mixing up forwarding behavior with management behavior or authentication with authorization/accounting. The mapping shown in the file is therefore retained as the verified response.

質問: **313**
ネットワーク上の異なるデバイスに対して、異なるレベルのsyslogを設定する目的は何ですか？
A. 各デバイスからの異なる重要度レベルのメッセージのレート制限を行う
B. 各デバイスからのsyslogメッセージの重要度を設定します
C. 各syslogメッセージの発信元を識別する
D. ローカルに保存されるさまざまなデバイスからの syslog メッセージの数を制御する
正解: (正解を表示します)
to set the severity of syslog messages from each device. IP services questions require matching the service to its exact operational role, such as logging, address assignment, file transfer, monitoring, redundancy, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under IP Services, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The distractors are real technologies, but they solve different infrastructure problems. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **314**
展示資料を参照してください。

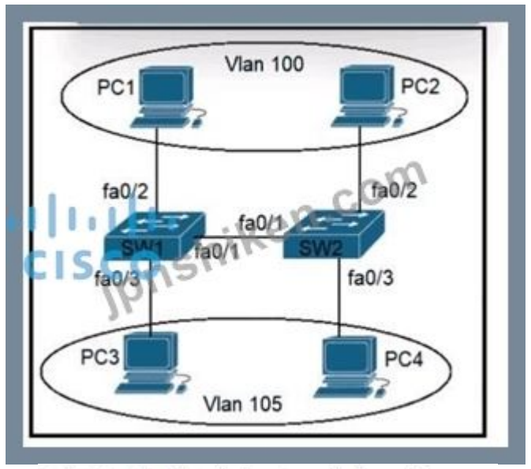
管理者は、暗号化ハッシュに格納されたパスワードを使用してローカル認証を行うように4台のスイッチを設定します。また、管理者がネットワークインフラストラクチャを管理できるように、4台のスイッチはSSHアクセスもサポートする必要があります。これらの要件を満たすように正しく設定されているスイッチはどれですか？

A. SW1
B. SW2
C. SW3
D. SW4

正解: C (コメントを発表する)

SW3. IP services questions test the exact function of infrastructure services such as addressing, name resolution, time synchronization, logging, monitoring, and secure management. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The distractors name valid services, but they provide a different service function from the one required in the prompt. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: 315



A.
```
Switch(config-if)#switchport mode dynamic
Switch(config-if)#switchport access vlan 100,105
Switch(config-if)#switchport trunk native vlan 1
```

B.
```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport access vlan 100,105
Switch(config-if)#switchport trunk native vlan 3
```

C.
```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation isl
Switch(config-if)#switchport trunk allowed vlan 100,105
Switch(config-if)#switchport trunk native vlan 1
```

D.
```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 100,105
Switch(config-if)#switchport trunk native vlan 3
```

正解: (正解を表示します)

Option B. The answer follows from standard Cisco behavior and the operational clue in the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. The other choices are adjacent technologies or commands, but they do not meet the stated requirement. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **316**

ネットワーク管理者は自動化の導入を決定する際に何を考慮する必要がありますか?

A. 自動化システムでは、ネットワークの変更を大規模に拡張することが難しい場合があります。

B. ネットワークの自動化は通常、ネットワーク内の仮想デバイスの構成と管理に限定されます。

C. ネットワークの自動化は通常、企業の管理運用コストを増加させます。

D. 手動による変更により、構成エラーや不整合が頻繁に発生します。

正解: (正解を表示します)

Manual changes frequently lead to configuration errors and inconsistencies.. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE.

JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact with a controller, while southbound APIs allow the controller to communicate with network devices. NETCONF and RESTCONF are configuration/management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to-device communication

with application-to-controller communication or confuse a data format with a protocol. Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers.
The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **317**
ワイヤレス環境におけるオーバーラップしないチャネルの役割は何ですか?
A. 干渉を減らす
B. チャネル ボンディングを許可する
C. RF 環境を安定させる
D. 帯域幅を増やす
正解: (正解を表示します)
to reduce interference. Wireless questions require separating client association, RF design, AP mode, WLAN security, and controller policy. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Incorrect answers usually confuse an encryption method with authentication, or a controller feature with a switchport feature. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **318**
展示資料を参照してください。

```
RIP    10.1.1.16/28[120/5]  via  F0/0
OSPF   10.1.1.0/24[110/30]  via  F0/1
OSPF   10.1.1.0/24[110/40]  via  F0/2
EIGRP  10.1.0.0/26[90/20]   via  F0/3
EIGRP  10.0.0.0/8 [90/133]  via  F0/4
```

ルーターが BGP から受信したパケットは、シリアルインターフェイス 209 165 201 1 を介して入力されます。各ルートはルーティング テーブル内に存在します。宛先 IP アドレスが 10.1.1.19 のトラフィックを転送するために使用されるインターフェイスはどれですか?
A. F0/4
B. F0/0
C. F0/1
D. F0/3
正解: (正解を表示します)

F0/0. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym.
The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **319**
スイッチがフレームをすべてのポートにフラッディングするのはなぜですか?
A. フレームの宛先 MAC アドレスが 0 です。
B. フレームの送信元MACアドレスが不明
C. フレームの送信元と宛先の MAC アドレスが同じ
D. フレームの宛先 MAC アドレスが不明です。
正解: **D (**コメントを発表する**)**
The destination MAC address of the frame is unknown.. A switch floods a frame when the destination MAC address is unknown in the MAC address table. The switch already learns the source MAC address from the ingress frame, but forwarding requires a destination lookup. If that lookup fails, the switch sends the frame out all ports in the same VLAN except the port on which it arrived. Cisco CCNA 200-301 v1.1 Network Fundamentals expects this exact distinction: unknown unicast flooding is triggered by an unknown destination MAC address, not by an unknown source. Zero destination MAC addresses and identical source/destination addresses are not normal reasons for Ethernet flooding. Once the destination device replies, the switch learns the MAC-to-port mapping and future frames can be forwarded directly. Therefore, the correct answer is that the destination MAC address of the frame is unknown.

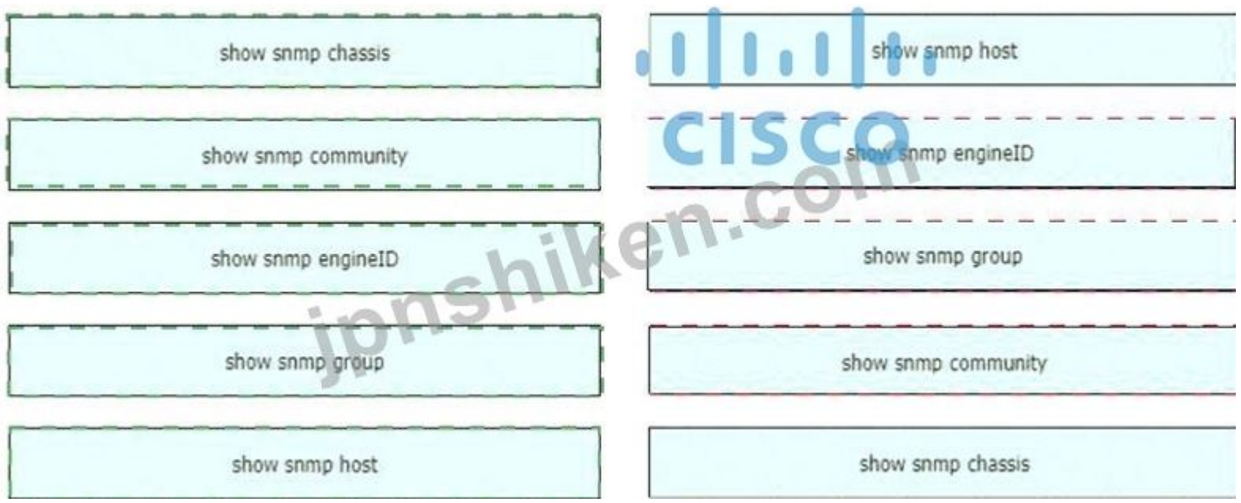
質問: **320**
認証と会計の違いを説明できる記述を2つ選びなさい。(2つ選択してください。)
A. 認証のみがユーザーの接続期間を記録します。
B. 認証のみがユーザーアクティビティ監査をサポートします。
C. 認証のみが課金ユーザーに関するサポート情報を提供します。
D. 認証のみがユーザーに資格情報の入力を求め、応答を返します。
E. 認証のみが あなたが誰であるか」を検証します。
正解: **(**正解を表示します**)**
Answer D,E is correct: D. Only authentication challenges users for their credentials and returns a response.; E.
Only authentication validates " who you are. " . Security questions in CCNA 200-301 v1.1 require matching the control to the threat or access requirement. Authentication proves identity, authorization controls what the user can do, and accounting records activity. Firewalls inspect and permit or deny traffic based on policy, while ACLs match packet fields in a defined order. VPN and IPsec questions require knowing whether the design protects unicast traffic, supports tunneling, or encrypts the original packet. Password and SSH questions depend on IOS behavior, including encrypted secrets, local users, domain names, and cryptographic images. The incorrect choices often use a valid technology in the wrong role or provide weaker protection.
The selected answer is the Cisco-consistent control because it directly satisfies the access, confidentiality, or threat-mitigation requirement stated in the question.

質問: **321**
ハブアンドスポーク型WANトポロジーの機能は何ですか？
A. 加入者サイト間でアクセス制限を実装できます。
B. 加入者間の直接接続を提供します
C. レイヤ2 VPNをサポート

D. アプリケーションの最適化をサポートします。
正解: **A** (コメントを発表する)
Use A for this item. In a hub-and-spoke WAN, spoke sites communicate through a central hub rather than direct spoke-to-spoke links. This structure lets the hub enforce routing, policy, inspection, and access restrictions between subscriber or branch sites. In Cisco CCNA 200-301 v1.1, Network Fundamentals questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. The topology does not inherently provide direct connections between every subscriber; that is closer to full mesh. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **322**
左側のSNMPマネージャとエージェント識別子コマンドを右側の機能にドラッグアンドドロップします。

正解:



Explanation:
Use the displayed drag-and-drop mapping for this item. SNMP uses manager and agent identifiers so a monitoring station can poll, receive traps, and identify managed devices. Commands for contact, location, chassis ID, and community or user parameters help the NMS organize and authenticate device management information. In Cisco CCNA 200-301 v1.1, IP Services questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve.
These identifiers are not forwarding commands; they support operational monitoring and inventory visibility.

A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **323**
インターフェイスで PortFast を設定する利点は何ですか?
A. ケーブルが接続されると、インターフェイスはそのケーブル タイプで使用可能な最速の速度設定を使用します。
B. ケーブルが接続された後、ユーザー データを送受信するためのインターフェイスがより高速に使用可能になります。
C. インターフェイスに入るフレームは、より高い優先順位でマークされ、スイッチによってより高速に処理されます。
D. インターフェイスに入るリアルタイムの音声およびビデオ フレームがより高速に処理されます。
正解: **(**正解を表示します**)**
After the cable is connected, the interface is available faster to send and receive user data. The answer follows directly from normal Cisco device behavior and the wording of the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **324**
SNMP操作におけるコミュニティ文字列の役割は何ですか？
A. SNMPトラフィックメッセージのシーケンスタグとして機能します。
B. MIBオブジェクトへのアクセスを保護するためのパスワードとして機能します。
C. デバイスへのアクセスに必要な Active Directory のユーザー名とパスワードを渡します
D. 英数字のMIB出力値を数値に変換します。
正解: **B (**コメントを発表する**)**
It serves as a password to protect access to MIB objects.. IP services questions require matching the service to its exact operational role, such as logging, address assignment, file transfer, monitoring, redundancy, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under IP Services, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The distractors are real technologies, but they solve different infrastructure problems. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **325**
アクセスポイントが固有のSSIDを1つ提供し、クライアントデータと管理トラフィックを転送し、自律モードで動作する場合、どのタイプの有線ポートが必要ですか？

A. ラグ
B. デフォルト
C. トランク
D. ボペス
正解: **(**正解を表示します**)**
default. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **326**
展示資料を参照してください。

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
      10.0.0.0/24 is subnetted, 5 subnets
D     10.1.2.0/24 [90/2170112] via 10.165.20.226, 00:01:30, Serial0/0
D     10.1.3.0/24 [90/2170112] via 10.165.20.226, 00:01:30, Serial0/0
D     10.1.2.0/25 [90/2170112] via 10.165.20.126, 00:01:30, Serial0/0
D     10.1.3.0/25 [90/2170112] via 10.165.20.146, 00:01:30, Serial0/0
D     10.1.4.0/25 [90/2170112] via 10.165.20.156, 00:01:30, Serial0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.18.10.0/24 is directly connected, GigabitEthernet0/0
      192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.11.0/24 is directly connected, GigabitEthernet0/1
     10.165.20.0/24 is variably subnetted, 2 subnets, 2 masks
C    10.165.20.224/24 is directly connected, Serial0/0
S     10.1.2.112/28 [1/0] via 10.165.20.166
```

宛先が10.1.2.126であるトラフィックがR1に入ってきた場合、次のホップは何ですか？
A. 10.165.20.126
B. 10.165.20.146
C. 10.165.20.166
D. 10.165.20.226
正解: **(**正解を表示します**)**
10.165.20.226. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under IP Services, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **327**
AAA 認証と承認の主な違いは何ですか?
A. 認証はユーザー名とパスワードを検証し、承認は認証エージェントとユーザー データベース間の通信を処理します。

B. 認証はシステムにアクセスしようとしているユーザーを識別し、承認はユーザーのパスワードを検証します。
C. 認証は、システムにアクセスしようとしているユーザーを識別して検証し、承認はユーザーが実行できるタスクを制御します。
D. 認証は、ユーザーがアクセスできるシステム プロセスを制御し、ユーザーが開始したアクティビティを承認ログに記録します。
正解: **C** (コメントを発表する)
Authentication identifies and verifies a user who is attempting to access a system, and authorization controls the tasks the user can perform.. Security fundamentals questions test the boundary between identity, authorization, accounting, encryption, inspection, and access-control functions. Cisco CCNA 200-301 v1.1 includes this topic under Security Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other answers confuse identity checking with traffic filtering, or they assign the correct security idea to the wrong device or protocol. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **328**
スパイン アンド リーフ トポロジのスイッチはどのように相互接続されていますか?
A. 各リーフ スイッチはいずれかのスパイン スイッチに接続されます。
B. 各リーフ スイッチは 2 つのスパイン スイッチに接続され、ループを形成します。
C. 各リーフ スイッチは各スパイン スイッチに接続されます。
D. 各リーフ スイッチは中央のリーフ スイッチに接続され、コア スパイン スイッチにアップリンクされます。
正解: (正解を表示します)
The correct response is C. In a spine-and-leaf topology, every leaf switch connects to every spine switch. This full bipartite design gives predictable latency and equal-cost paths for east-west traffic. For Cisco CCNA 200-
301 v1.1, the important point is the mechanism, not a generic description of the technology. Leaves do not connect only to one spine or through a central leaf, and spine switches normally do not connect to each other.
When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **329**
展示資料を参照してください。

エンジニアがCisco WLC GUIを使用して、AES暗号化方式のWPA2と事前共有キーCisc0123456を使用するWLANの設定を行っています。エンジニアがレイヤ2セキュリティのドロップダウンリストからWPA + WPA2オプションを選択した後、プロセスを完了するために実行する必要のある2つのタスクはどれですか？(2つ選択してください。)

A. WPA2ポリシー、AES、TKIPのチェックボックスを選択します。

B. PSK フォーマットのドロップダウン リストから ASCII を選択し、キーを入力して、認証キー管理の設定は空白のままにします。

C. [認証キー管理] ドロップダウンリストから [PSK] を選択し、[PSK フォーマット] を [ASCII] に設定して、キーを入力します。

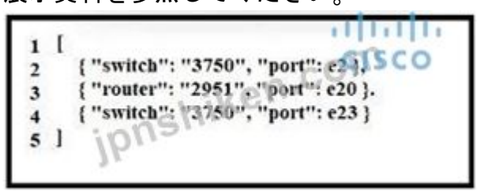
D. WPA2 ポリシーと AES のチェックボックスを選択します。

正解: **(**正解を表示します**)**

Answer C,D is correct: C. Select PSK froin the Auth Key Mgmt drop-down list, set the PSK Format to ASCII, and enter the key.; D. Select the WPA2 Policy and AES check boxes.. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **330**

展示資料を参照してください。



JSONスキーマの2行目にある「switch」という単語は何を表していますか？

A. 配列

B. キー

C. 値

D. オブジェクト

正解: **(**正解を表示します**)**

key. In JSON, a key is the name on the left side of a name/value pair. If the word switch appears as the field name in the JSON schema, it is a key, while the data associated with it is the value. Arrays are ordered lists enclosed in square brackets, and objects are collections of key/value pairs enclosed in braces. Cisco CCNA 200-301 v1.1 Automation and Programmability expects candidates to recognize basic JSON syntax because modern Cisco APIs commonly return JSON payloads. The corrected answer is key. Misreading a key as a value causes parsing mistakes when working with REST APIs, automation scripts, and controller responses.

質問: **331**

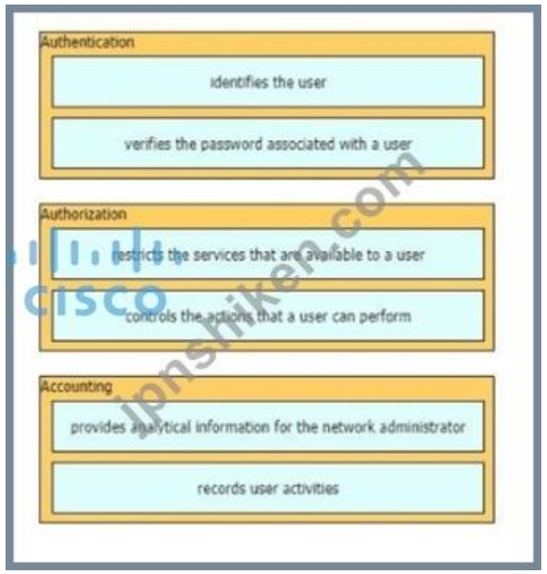
左側のAAA機能を右側の適切なAAAサービスにドラッグアンドドロップしてください。

正解:

Explanation:

AAA separates three related security functions. Authentication verifies identity: who the user or device is.

Authorization determines what that authenticated identity is allowed to do, such as which commands can be run or which services can be accessed. Accounting records what happened, including login times, commands, resource usage, or session start and stop information. The drag-and-drop answer should map identity checks to authentication, permission or privilege decisions to authorization, and tracking or logging of user activity to accounting. Cisco CCNA v1.1 Security Fundamentals includes AAA concepts and the practical differences between RADIUS and TACACS+. The best way to solve AAA questions is to translate the term into a plain operational question. Authentication asks, "Are you really this user?" Authorization asks, "What are you allowed to access?" Accounting asks, "What did you do?" Those three meanings remain the same whether the backend service is local, RADIUS, or TACACS+.



有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **332**
ネットワーク エンジニアは、ルーター ループバック インターフェイスを IPv6 アドレス空間に移行する必要があります。インターフェイスの現在の IPv4 アドレスが 10.54.73.1/32 で、エンジニアが IPv6 アドレス 0.0.0.0.0:ffff:a36:4901 を構成する場合、どのプレフィックス長を使用する必要がありますか?
A. /64
B. /96
C. /124
D. /128
正解: **(正解を表示します)**
/128. Routing and redundancy questions are solved by applying longest-prefix match, administrative distance, metrics, and gateway-redundancy behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Incorrect choices point to the wrong next hop, choose the wrong route source, or confuse routing with Layer 2 behavior. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **333**
PKI の一部を構成する 2 つのコンポーネントはどれですか？ 2つ選んでください。）
A. 接続を認証する事前共有キー
B. RSA トークン
C. 証明書を付与する CA

D. 接続を認証する平文のパスワード
E. 1 つ以上の CRL
正解: (正解を表示します)
Answer B,C is correct: B. RSA token; C. CA that grants certificates. Security fundamentals require distinguishing identity, authorization, accounting, encryption, inspection, and physical protection. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The incorrect choices apply a security term in the wrong control category or protect a different part of the system. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **334**
データプレーン上で発生するネットワーク機能はどれですか？
A. リモートクライアント/サーバートラフィックの転送
B. スパニングツリー選挙を容易にする
C. 受信SSH管理トラフィックを処理中
D. OSPF Heltoパケットの送受信
正解: (正解を表示します)
forwarding remote client/server traffic. OSPF decisions depend on router IDs, area membership, matching timers, network type, interface state, and cost calculation rather than arbitrary route preference. Cisco CCNA
200-301 v1.1 includes this topic under Automation and Programmability, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. Distractors that mention process IDs, unrelated metrics, or the wrong interface parameter do not satisfy OSPF neighbor or route-selection requirements. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **335**
管理者が軽量APでWebベースの管理セッションを開く必要がある場合、どのIPアドレスが使用されますか？
A. WLCIP
B. ゲートウェイIP
C. 自律型 AP IP
D. ACS IP
正解: (正解を表示します)
WLCIP. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **336**
展示資料を参照してください。

どのような種類のJSDNデータが表示されますか？

A. オブジェクト

B. シーケンス

C. 文字列

D. ブール値

正解: **(**正解を表示します**)**

String. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE. JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact with a controller, while southbound APIs allow the controller to communicate with network devices. NETCONF and RESTCONF are configuration /management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to- device communication with application-to-controller communication or confuse a data format with a protocol.

Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers. The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

質問: **337**

ルーターはネットワークを通してパケットを転送する際に、どのような動作を行いますか？

A. ルーターは、送信元ルーターのインターフェースラベルを送信元として、次のホップルーターのラベルを宛先として、送信元と宛先のラベルを置き換えます。

B. ルーターは送信元ルーターのIPアドレスを送信元、隣接ルーターのIPアドレスを宛先として、送信元および宛先IPアドレスをカプセル化します。

C. ルーターは、元の送信元MACアドレスと宛先MACアドレスを、送信元として送信ルーターのMACアドレス、宛先としてネイバーMACアドレスに置き換えます。

D. ルーターは元のパケットをカプセル化し、送信元ルーターのMACアドレスを識別するタグを追加して、宛先に透過的に送信します。

正解: **(**正解を表示します**)**

The router replaces the original source and destination MAC addresses with the sending router MAC address as the source and neighbor MAC address as the destination. Cisco routers select forwarding paths by longest- prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **338**

展示資料を参照してください。

```
R1#show ip ospf interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.2/24, Area 0
  Process ID 1, Router ID 192.168.1.2, Network Type POINT-TO-POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 15, Dead 20, Wait 20, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)

R2#show ip ospf interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:11
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
```

ネットワークエンジニアは、ルーターR2をネットワーク上の代替ルーターとして設定しています。初期設定を適用した後、R2がR1をネイバーとして認識しなかったことが判明しました。OSPF設定を完了し、R1とのネイバー関係を確立できるようにするには、R2にどの設定を適用する必要がありますか？

A.
```
R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 255.255.255.0 area 2
R2(config-router)#network 10.1.1.0 255.255.255.255 area 2
```

B.
```
R2(config)#router ospf 1
R2(config-router)#router-id 192.168.1.2
```

C.
```
R2(config)#interface g0/0/0
R2(config-if)#ip ospf dead-interval 20
```

D.
```
R2(config)#interface g0/0/0
R2(config-if)#ip ospf hello-interval 15
R2(config-if)#ip ospf dead-interval 20
```

正解: **(**正解を表示します**)**

Option. Routing questions are solved by applying longest-prefix match, administrative distance, metric, and protocol-specific behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Wrong answers either use the wrong prefix, the wrong next hop, or a route source that would not be preferred. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問**: 339**

REST API は通信にどのプロトコルを使用しますか?

A. SSH

B. SNMP
C. HTTP
D. STP
正解: **C (**コメントを発表する**)**
HTTP. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology.
The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **340**
組織は、クラウド提供サービスの使用を開始することを決定しました。組織が独自のオペレーティング システムを仮想マシンにインストールできるようにするクラウド サービスはどれですか?
A. サービスとしてのプラットフォーム
B. サービスとしてのソフトウェア
C. サービスとしてのネットワーク
D. サービスとしてのインフラストラクチャ
正解: **(**正解を表示します**)**
The correct cloud service model is infrastructure as a service, so the answer is D. IaaS gives the customer virtualized infrastructure such as compute, storage, and networking while leaving operating system installation and management under the customer's control. That is the model used when an organization wants to deploy its own OS on a cloud virtual machine. SaaS is the opposite end of the stack: the provider delivers a finished application, and the customer normally does not manage the operating system or runtime. PaaS gives developers a platform for application deployment but still abstracts the underlying OS more than IaaS.
Network as a service is not the best match to "install its own operating system on a virtual machine." CCNA
200-301 v1.1 Network Fundamentals includes cloud service models, and this question tests the boundary between SaaS, PaaS, and IaaS. Reference: Cisco CCNA cloud fundamentals and Cisco 200-301 v1.1 exam topics.

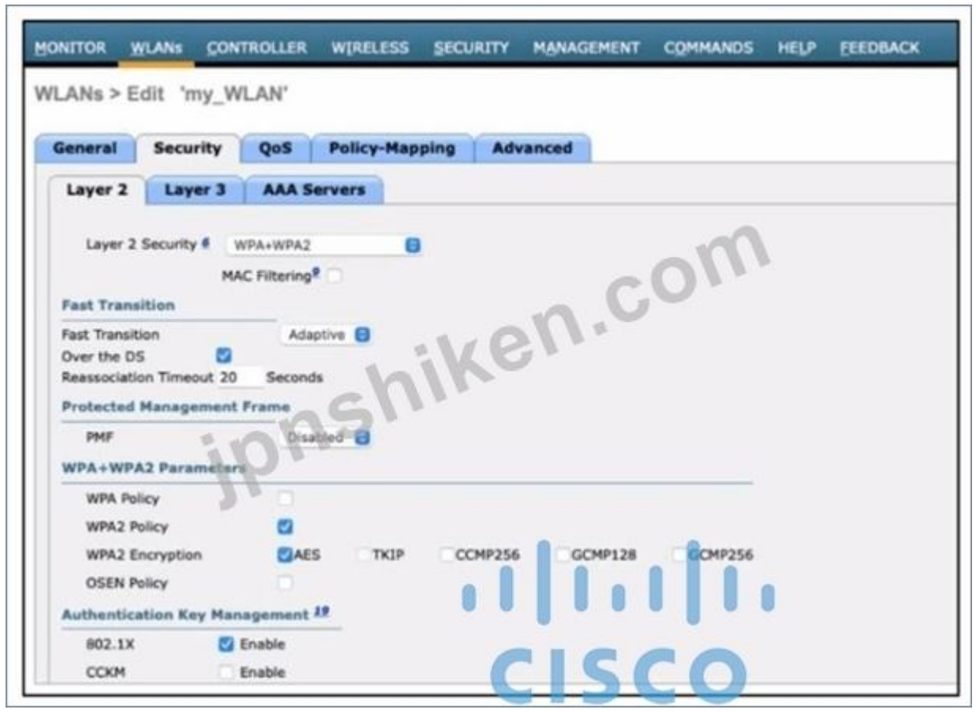
質問: **341**
VRRPはどのタイプのプロトコルですか？
A. 動的IPアドレス割り当てを使用します
B. 2 つ以上のルーターをデフォルトゲートウェイとして機能させる
C. ルーター間通信に宛先IPアドレス224.0.0.102を使用します
D. シスコ独自のファーストホップ冗長プロトコルを使用します
正解: **D (**コメントを発表する**)**
uses Cisco-proprietary First Hop Redundancy Protocol. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **342**
組織のセキュリティプログラムの一環として、物理的なアクセス制御を実施するアクションはどれですか？

A. リモートロケーションでのシステムログのバックアップ
B. コンソールポートのパスワードを設定する
C. ネットワークデバイスで有効化パスワードを設定する
D. 主要インフラを監視するためのIPカメラの設置
正解: (正解を表示します)
setting up IP cameras to monitor key infrastructure. Physical access control protects buildings, rooms, closets, racks, and infrastructure from unauthorized physical interaction. IP cameras monitoring key infrastructure are a physical security control because they deter, detect, and document access to protected spaces. Console passwords and enable passwords are logical access controls on devices, not physical controls. Backing up syslogs is an operational logging and recovery practice. Cisco CCNA 200-301 v1.1 Security Fundamentals separates physical controls from administrative and technical controls because all three are needed in a secure network. A router with strong passwords is still exposed if an attacker can physically reach the console cable or remove hardware. The corrected answer is setting up IP cameras to monitor key infrastructure.

質問: **343**
HSRPにおいて予測可能な結果は次のうちどれですか？(2つ選択してください)
A. 2 つのルーターは、LAN 上のデバイスのデフォルト ゲートウェイとして使用される仮想 IP アドレスを共有します。
B. 2台のルーターは、一方のルーターをアクティブルーター、もう一方をスタンバイルーターとしてネゴシエートする。
C. 各ルーターは異なるIPアドレスを持ち、両方のルーターがLAN上のデフォルトゲートウェイとして機能し、トラフィックはルーター間で負荷分散されます。D 2つのルーターは設定を同期して、一貫したパケット転送を提供します。
D. 2 つのルーティングは同じ IP アドレスを共有し、デフォルト ゲートウェイのトラフィックはそれらの間で負荷分散されます
正解: (正解を表示します)
Answer A,B is correct: A. The two routers share a virtual IP address that is used as the default gateway for devices on the LAN.; B. The two routers negotiate one router as the active router and the other as the standby router. Cloud and virtualization questions require separating physical resources, hypervisor control, virtual switching, server functions, and the service model being consumed. Cisco CCNA 200-301 v1.1 includes this topic under IP Connectivity, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The wrong choices confuse SaaS, PaaS, IaaS, the hypervisor role, or the way virtual machines reach the physical network. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **344**



jpnshiken.com

図を参照してください。ネットワークエンジニアが、Webパススルーレイヤ3 Webポリシーを使用して無線LANを構成しています。構成を完了するために、エンジニアはどのような操作を行う必要がありますか？

A. レイヤ2セキュリティを802.1Xに設定します。
B. TKIPとCCMP256 WPA2暗号化を有効にします。
C. レイヤ2セキュリティを "なし"に設定します。
D. WPAポリシーを有効にします。
正解: **(**正解を表示します**)**
Set the Layer 2 Security to None.. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band.
The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities.
Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right- looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

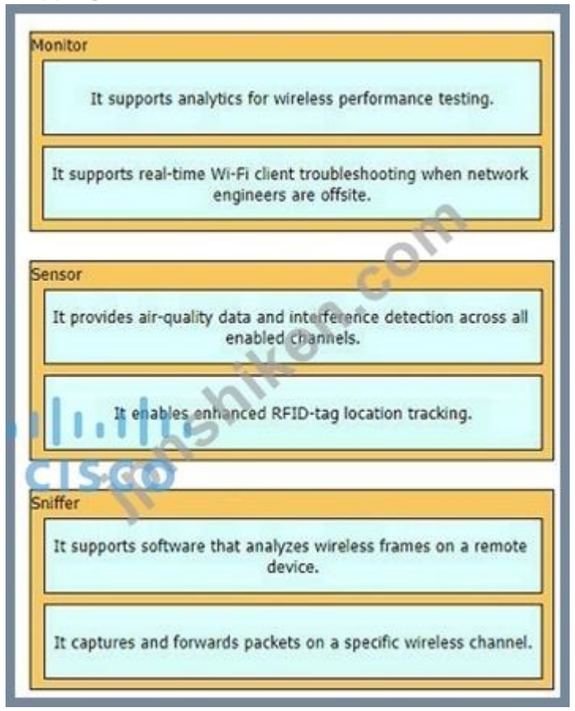
質問: **345**
左側のアクセスポイントモードに関する記述を、右側の対応するモードにドラッグアンドドロップしてください。

正解:

Explanation:

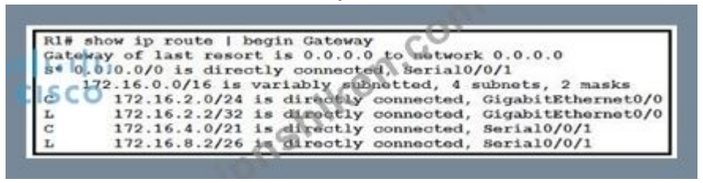
Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this form test whether each protocol, command, service, or architecture term is placed with the function it actually performs. The safest approach is to classify each item by operating layer and purpose before matching it: routing behavior belongs to IP connectivity, wireless modes belong to access, REST methods belong to automation, and AAA functions

belong to security services. Several distractors are valid networking terms, but they become wrong when mapped to the wrong plane or protocol. The retained mapping follows Cisco terminology and reflects how the features are used in implementation and troubleshooting. In practice, this prevents mixing up forwarding behavior with management behavior or authentication with authorization/accounting. The mapping shown in the file is therefore retained as the verified response.



質問: **346**

展示資料を参照してください。



ルート172.16.4.0のサブネットマスクは何ですか？

A. 255.255.255.192

B. 255.255.254.0

C. 255.255.240.0

D. 255.255.248.0

正解: **(正解を表示します)**

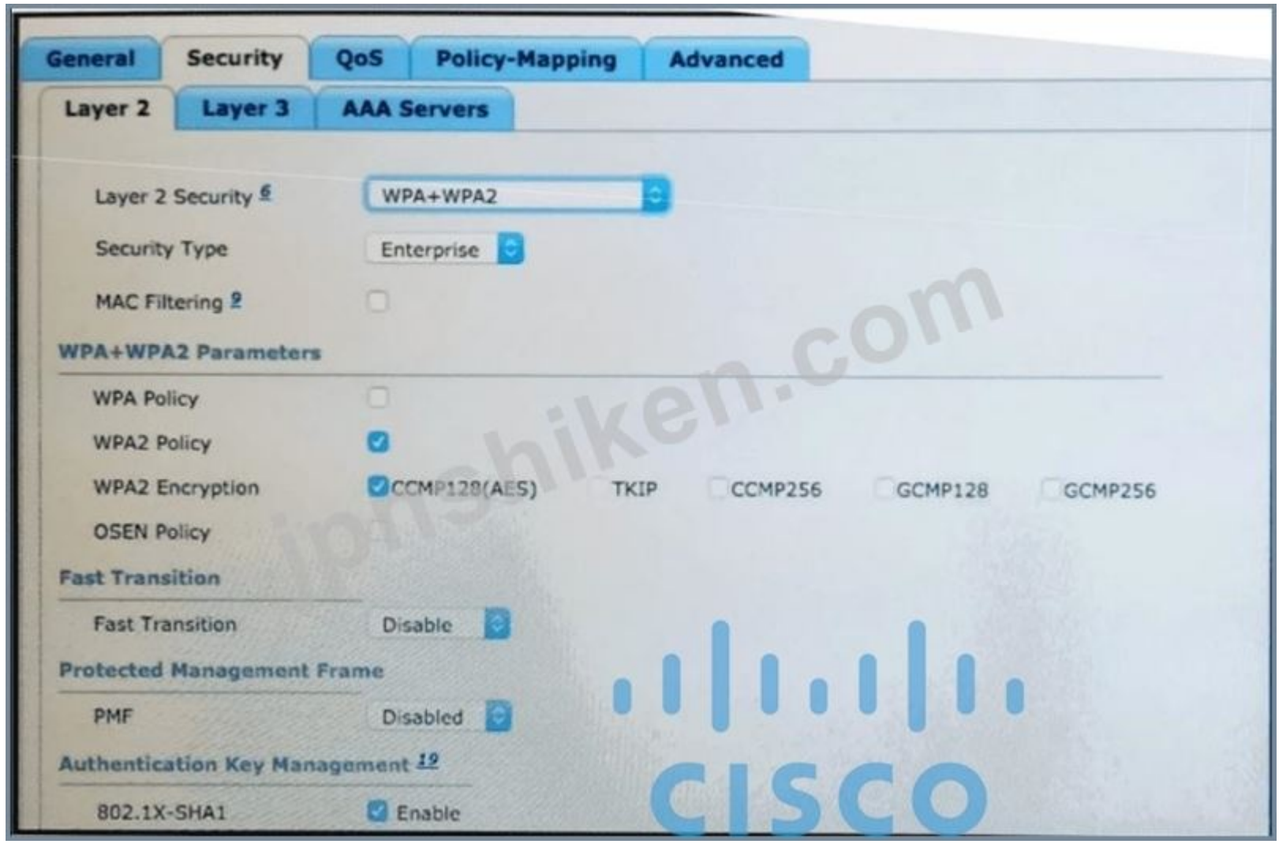
255.255.248.0. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.

Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.

The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **347**
展示資料を参照してください。



WLANで802.11wを有効にするには、どのような設定が必要ですか？
A. PMFを必須に設定します。
B. MACフィルタリングを有効にする。
C. WPAポリシーを有効にする。
D. 高速トランジションを有効に設定する
正解: **(**正解を表示します**)**
Set PMF to Required.. Wireless design and security require separating AP mode, WLAN identity, RF behavior, authentication, and encryption. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The distractors confuse wireless standards, security mechanisms, controller settings, or RF design practices. In a real network, selecting the wrong option would usually

produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **348**
DHCPクライアントとは何ですか？
A. ホストにIPアドレスを動的に割り当てるサーバー
B. ホストに静的にIPアドレスを割り当てるルーター
C. IPアドレスを自動的に要求するように設定されたホスト
D. IPアドレスに関連付けられたドメイン名を要求するワークステーション
正解: **(正解を表示します)**
a host that is configured to request an IP addressss automatically. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **349**
管理者がアクセスポイントの認証と設定に使用するプロトコルはどれですか？(2つ選択)
A. Kerberos
B. 802.1Q
C. 802.1x
D. TACACS+
E. RADIUS
正解: **(正解を表示します)**
Answer D,E is correct: D. TACACS+; E. RADIUS. Wireless questions require separating client association, RF design, AP mode, WLAN security, and controller policy. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Incorrect answers usually confuse an encryption method with authentication, or a controller feature with a switchport feature. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **350**
パスワードがルーターまたはスイッチの構成にプレーンテキストとして保存されるのを防ぐコマンドはどれですか?
A. シークレットを有効にする
B. サービス パスワード暗号化
C. ユーザー名 Cisco パスワード 暗号化
D. パスワードを有効にする
正解: **B (コメントを発表する)**
The global command service password-encryption prevents supported plain-text passwords from being displayed in clear text in the running configuration. After the command is enabled, passwords configured under lines, usernames using the password keyword, and similar legacy password fields are obfuscated with Cisco Type 7 encoding. This is not strong cryptographic protection, but it does stop casual viewing of plain text during show running-config. The enable secret command protects the privileged EXEC password with a stronger hash, but it does not encrypt all plain-text passwords in the configuration. The enable password command creates a less secure privileged password, and the username Cisco password encrypt syntax is not the correct IOS command. CCNA 200-301 v1.1 Security Fundamentals expects

candidates to know basic device hardening commands and the difference between enable secret and service password-encryption. The verified answer is B. Reference: Cisco IOS password encryption and secure device-management guidance.

質問: **351**
新しいCisco ISEサーバーをインストールした後、エンジニアはCisco WLC上で、認証情報に基づいて特定のVLAN上のワイヤレスクライアントを接続するために、どのようなタスクを実行する必要がありますか？
A. AAAオーバーライドを有効にする
B. イベント駆動型RRMを有効にします。
C. LAG モードまたは次回の再起動を無効にします。
D. 認証リストまたはAAAに対して、承認済みMIC APを有効にします。
正解: **(正解を表示します)**
Use A for this item. AAA Override on the Cisco WLC allows returned AAA attributes to override WLAN defaults, including VLAN assignment. When Cisco ISE authenticates a user, it can return authorization attributes that place the client into a specific VLAN. In Cisco CCNA 200-301 v1.1, Network Access questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. RRM, LAG reboot settings, and MIC authorization do not provide credential-based VLAN assignment. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **352**
ネットワーク管理者が、プリンタに接続されたスイッチ インターフェイスでポート セキュリティを有効にしました。ポートがプリンターの MAC アドレスを学習し、それをテーブルに自動的に挿入できるようにするための次の構成アクションは何ですか?
A. 動的 MAC アドレス学習を有効にする
B. 静的 MAC アドレス指定を実装します。
C. スティッキー MAC アドレッシングを有効にする
D. 自動 MAC アドレス学習を実装する
正解: **(正解を表示します)**
enable sticky MAC addressing. The answer follows directly from normal Cisco device behavior and the wording of the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control- plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **353**

図を参照してください。設定を適用した後、2台のルーターがOSPFネイバー関係を確立できません。この問題の原因は何ですか？

A. OSPFルーターIDが一致していません。

B. Router2 はデフォルトの helto タイマーを使用しています。

C. Router1 のネットワークステートメントの設定が間違っています。

D. OSPFプロセスIDが一致していません。

正解**: B (**コメントを発表する**)**

Router2 is using the default helto timer.. OSPF decisions depend on router IDs, area membership, matching timers, network type, interface state, and cost calculation rather than arbitrary route preference.

Cisco CCNA

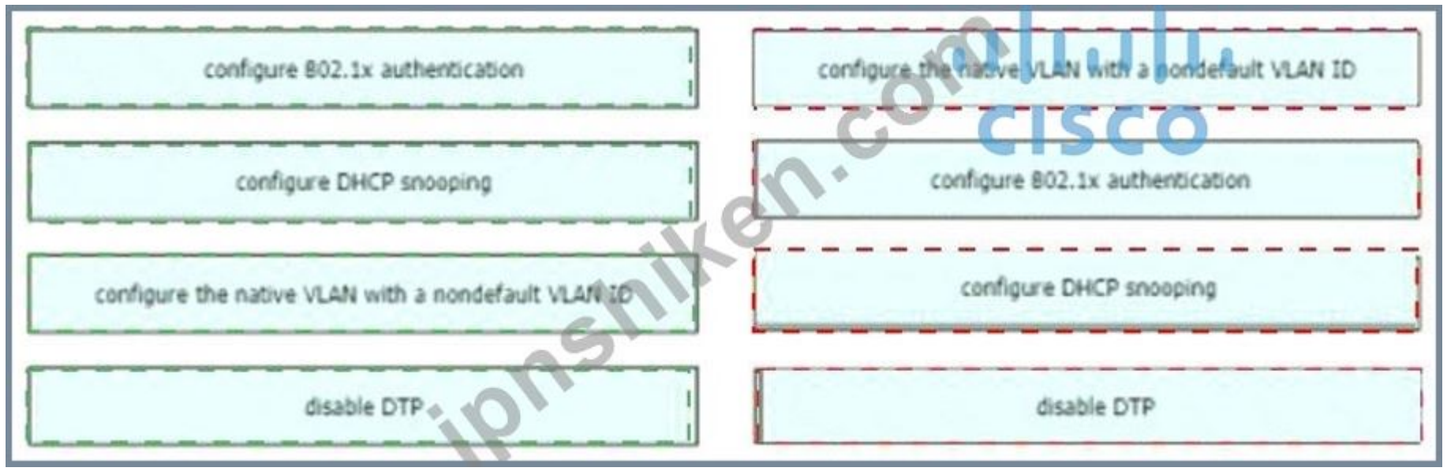
200-301 v1.1 includes this topic under IP Connectivity, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces.

Distractors that mention process IDs, unrelated metrics, or the wrong interface parameter do not satisfy OSPF neighbor or route-selection requirements. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問**: 354**

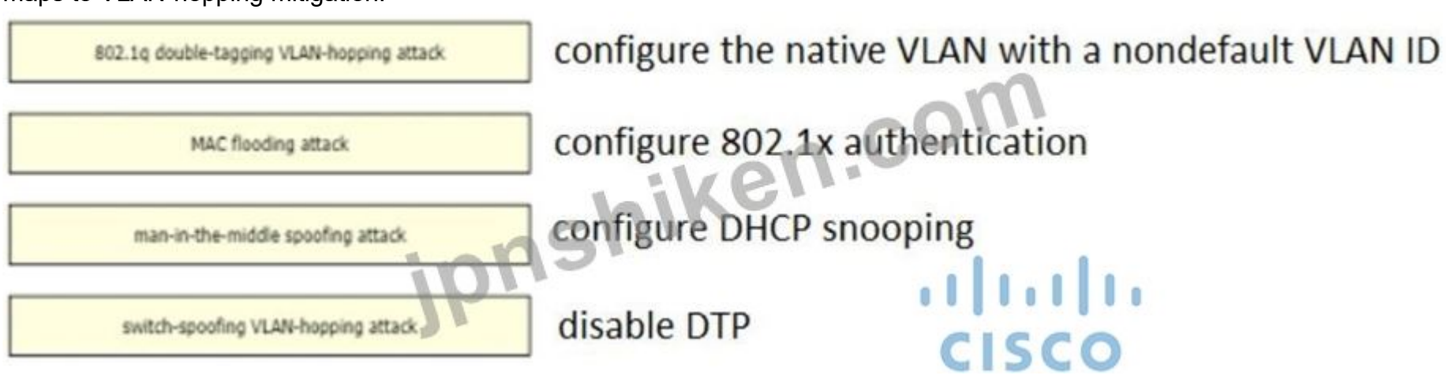
左側の攻撃軽減策を、右側の軽減対象となる攻撃の種類にドラッグ＆ドロップしてください。

正解:



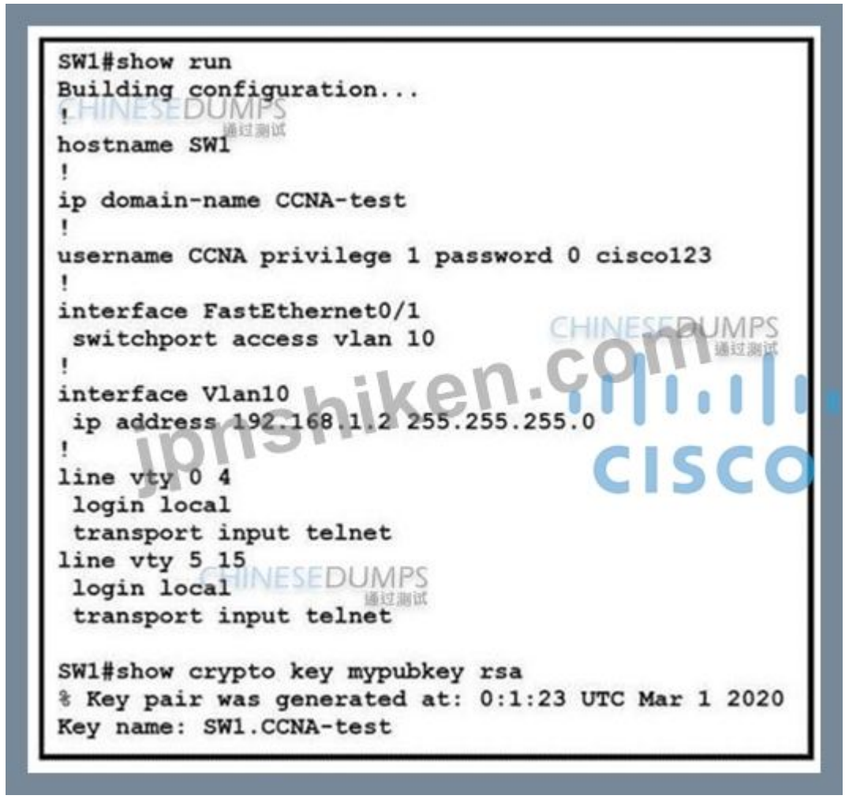
Explanation:

This drag-and-drop item maps common Layer 2 and access-layer threats to their mitigation controls. Dynamic ARP Inspection protects against ARP spoofing or poisoning by validating ARP packets against trusted binding information. DHCP snooping blocks rogue DHCP behavior and builds the binding table used by other protections. BPDU Guard protects PortFast edge ports by err-disabling a port that receives an unexpected spanning-tree BPDU, which helps prevent rogue switch insertion. A nondefault or unused native VLAN, combined with disabling DTP and manually configuring trunks, reduces VLAN hopping exposure. Cisco CCNA 200-301 v1.1 Security Fundamentals and Network Access both touch these controls because many campus attacks happen before traffic ever reaches a firewall. The dependable way to solve the matching is to identify the abused protocol: ARP attacks map to DAI, DHCP attacks map to DHCP snooping, unexpected switch/STP participation maps to BPDU Guard, and trunk/native-VLAN abuse maps to VLAN-hopping mitigation.



質問: **355**

展示資料を参照してください。



エンジニアが、スイッチSW1の管理アクセス設定を更新して、安全で暗号化されたリモート設定を可能にしようとしています。エンジニアは、スイッチに対してどの2つのコマンドまたはコマンドシーケンスを適用する必要がありますか？

(2つ選択してください。)

A. SW1(config)#enable secret ccnaTest123

B. SW1(config)#username NEW secret R3mote123

C. SW1(config)#line vty 0 15 SW1(config-line)#transport input ssh

D. SW1(config)# crypto key generate rsa

E. SW1(config)# interface f0/1 SW1(config-if)# switchport mode trunk

正解: **(正解を表示します)**

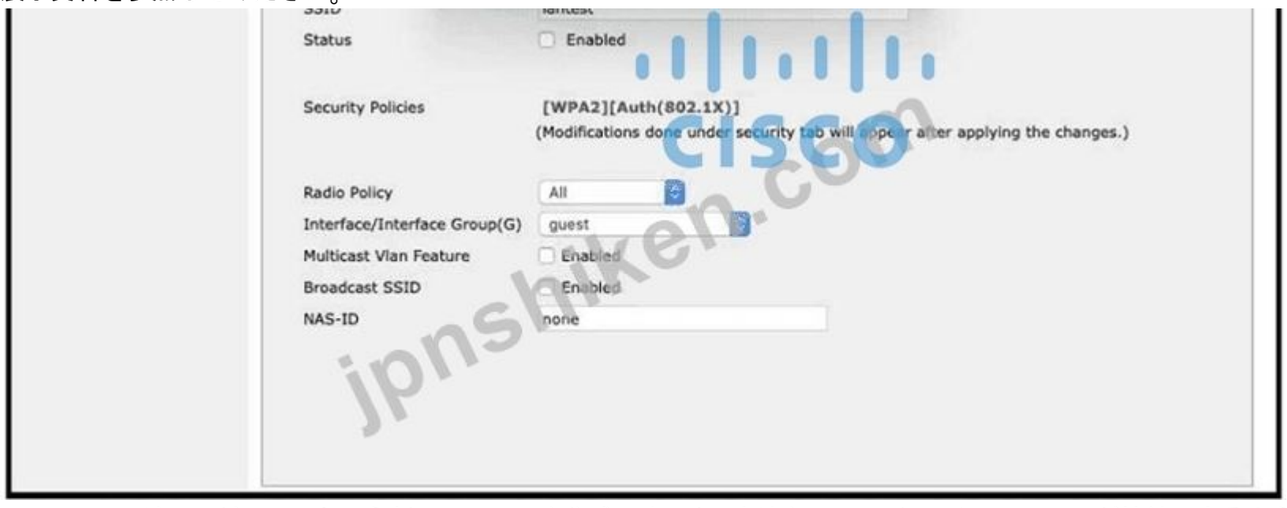
Answer C,D is correct: C. SW1(config)#line vty 0 15 SW1(config-line)#transport input ssh; D. SW1(config)# crypto key generate rsa. Secure encrypted remote management requires the VTY lines to accept SSH and the switch to have RSA keys available for SSH operation. The enable secret protects privileged EXEC mode, but it does not by itself enable encrypted remote access. A trunk command is unrelated to management-plane security. A local username may also be required depending on the existing configuration, but the two choices that directly enable encrypted remote management from the listed commands are transport input ssh and crypto key generate rsa. Cisco CCNA 200-301 v1.1 Security Fundamentals expects engineers to know the SSH prerequisites: hostname/domain context, RSA keys, appropriate line transport, and authentication. The corrected answer pair is the VTY SSH transport command and RSA key generation.

質問: **356**

従来のキャンパスデバイス管理とCisco DNA Centerデバイス管理は、導入に関してどのような違いがありますか？

A. Cisco DNA Centerのデバイス管理は、従来のキャンパスデバイス管理よりも迅速にネットワークを展開できます。
B. 従来のキャンパスデバイス管理では、Cisco DNA Centerデバイス管理よりもネットワークの拡張が迅速に行えます。
C. Cisco DNA Centerのデバイス管理は、従来のキャンパスデバイス管理オプションのほとんどよりも低コストで実装できます。
D. 従来のキャンパスデバイス管理スキームは、通常、Cisco DNA Center デバイス管理よりもパッチやアップデートを迅速に展開できます。
正解: (正解を表示します)
Cisco DNA Center device management can deploy a network more quickly than traditional campus device management. Automation questions require separating controller roles, API direction, data formats, HTTP behavior, and configuration-management tooling. Cisco CCNA 200-301 v1.1 includes this topic under Automation and Programmability, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The incorrect options mix northbound and southbound communication, confuse data serialization with transport, or describe traditional device-by-device management. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **357**
展示資料を参照してください。



Ciscoのエンジニアがlantestという新しいWLANを作成しました。高速な2.4GHzクライアントのみが接続できるようにするには、どの2つの操作を実行する必要がありますか？(2つ選択してください。)
A. ブロードキャストSSIDオプションを有効にする
B. ステータスオプションを有効にします。
C. 無線ポリシーオプションを802.11gのみに設定します。
D. 無線ポリシーオプションを802.11aのみに設定します。
E. インターフェイス/インターフェイス グループ(G)をゲスト以外のインターフェイスに設定します
正解: (正解を表示します)
Answer B,C is correct: B. Enable the Status option.; C. Set the Radio Policy option to 802.11g Only.. To allow only high-speed 2.4-GHz clients on the WLAN, the WLAN must be enabled and its radio policy must be limited to 802.11g only. 802.11g operates in the 2.4-GHz band and supports higher data rates than 802.11 b. Broadcasting the SSID is not required to restrict client data rates or band capability, and 802.11a is a 5- GHz standard rather than 2.4 GHz. Cisco CCNA 200-301 v1.1 Network Access expects engineers to distinguish wireless bands and PHY standards when configuring WLAN policy. The corrected answer pair is enabling the WLAN status and setting the radio policy to 802.11g Only. That combination activates the WLAN and restricts association to the intended high-speed 2.4-GHz client type.

質問: **358**

展示資料を参照してください。

この設定による影響は何ですか？

A. スイッチはすべてのARIPパケットを破棄します

B. 送信トラフィックは、宛先がDHCPサーバーである場合にのみ通過します。

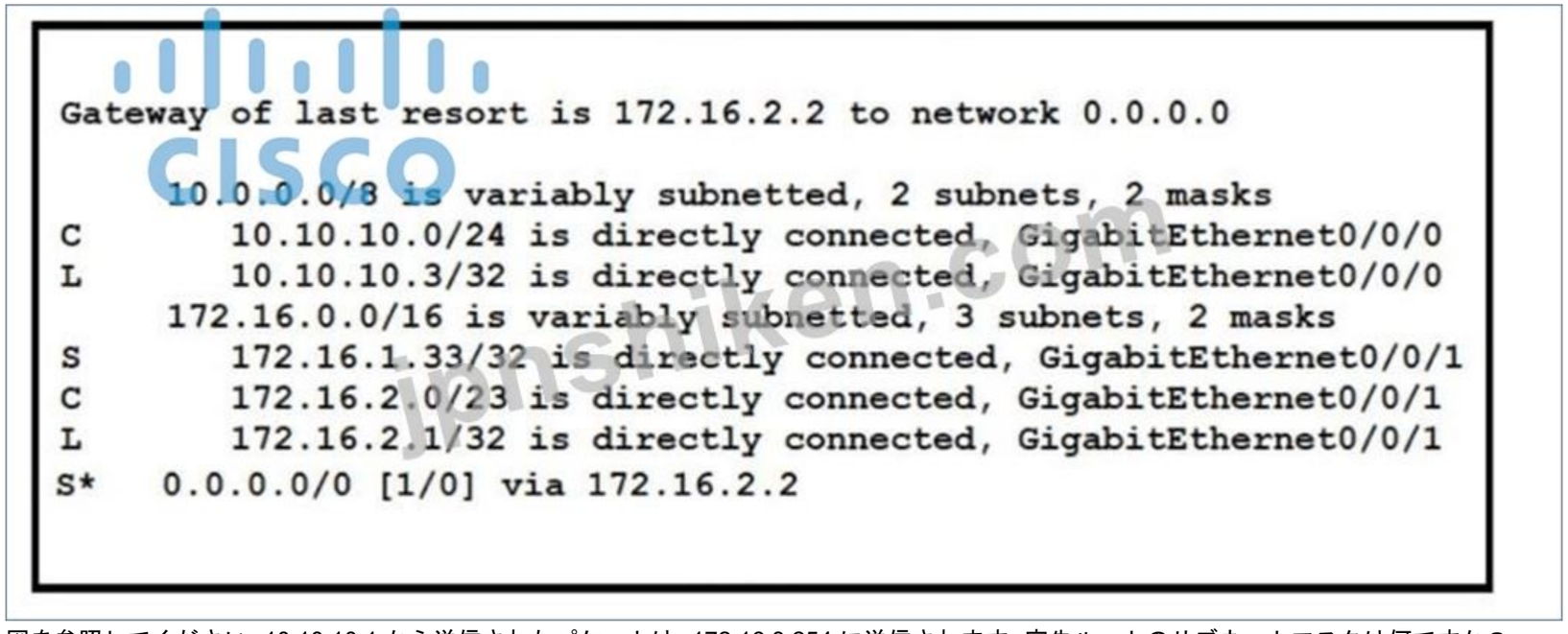
C. インターフェースが信頼できないため、すべての受信および送信トラフィックが破棄されます

D. スイッチは、無効な MAC アドレスと IP アドレスのバインディングを持つすべての受信 ARP トラフィックを破棄します。

正解: **(**正解を表示します**)**

The switch discard all ingress ARP traffic with invalid MAC-to-IP address bindings.. IP services questions test the exact function of infrastructure services such as addressing, name resolution, time synchronization, logging, monitoring, and secure management. Cisco CCNA 200-301 v1.1 includes this topic under Security Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The distractors name valid services, but they provide a different service function from the one required in the prompt. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **359**



図を参照してください。10.10.10.1 から送信されたパケットは、172.16.3.254 に送信されます。宛先ルートのサブネットマスクは何ですか？

A. 0.0.0.0

B. 255.255.254.0

C. 255.255.255.0

D. 255.255.255.255

正解: **A** (コメントを発表する)
0.0.0.0. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **360**
事前共有キー モードで WPA2 に使用されるワイヤレス暗号化のタイプはどれですか?
A. RC4 による TKIP
B. RC4
C. AES-128
D. AES-256
正解: (正解を表示します)
The correct answer is C: AES-128. Cisco's WPA2 documentation describes WPA2 as using AES with CCMP; AES Counter Mode encrypts 128-bit blocks with a 128-bit encryption key. The existing answer of AES-256 confuses PSK material or hexadecimal key-entry length with the actual WPA2 CCMP encryption cipher. WPA2-Personal uses a pre-shared key for authentication/key derivation, but the data-protection mechanism is AES-CCMP, not RC4, TKIP with RC4, or plain RC4. TKIP was associated with WPA and is considered legacy; WEP and RC4-based approaches are not acceptable modern wireless protection. CCNA
200-301 v1.1 Network Access expects the basic security pairing: WPA2 uses AES/CCMP, and WPA3 improves authentication with SAE. Because the option set forces a key-size distinction, Cisco's WPA2 configuration reference supports AES-128. Reference: Cisco WPA2 configuration example describing AES Counter Mode and a 128-bit encryption key.

質問: **361**
パケットが同じポートを通過し、VLAN 間のトラフィックの分離を維持するように、異なる VLAN のパケットをカプセル化するレイヤー 2 スイッチ機能はどれですか?
A. VLAN の番号付け
B. VLAN DSCP
C. VLAN タギング
D. VLAN マーキング
正解: **C** (コメントを発表する)

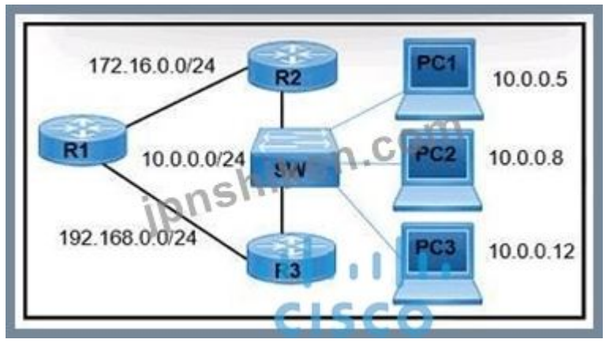
VLAN tagging. Switching behavior depends on VLAN tagging, trunk negotiation, STP role selection, EtherChannel mode, and whether a protocol is standards-based or Cisco-specific. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. Incorrect options change existing VLAN reachability, use the wrong negotiation behavior, or apply a feature to the wrong switch function. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **362**

図を参照してください。HQCは以下の構成を使用する必要があります。
最大15万の同時接続を処理
パブリックIPアドレスの消費を最小限に抑えます
どの構成が要件を満たしていますか？
A. ip nat pool NATPOOL 209.165.201.1 209.165.201.5 netmask 255.255.255.248ip nat inside source list HQC interface gigabitEthernet0/0 overload
B. ip nat pool NATPOOL 209.165.200.225 209.165.200.226 netmask 255.255.255.252ip nat outside source list HQC pool NATPOOL overload
C. ip nat pool NATPOOL 209.165.201.1 209.165.201.3 netmask 255.255.255.248ip nat inside source list HQC pool NATPOOL overload
D. ip nat pool NATPOOL 209.165.201.1 209.165.201.248 netmask 255.255.255.248ip nat outside source list HQC pool NATPOOL overload
正解: **(正解を表示します)**
ip nat pool NATPOOL 209.165.201.1 209.165.201.5 netmask 255.255.255.248ip nat inside source list HQC interface gigabitEthernet0/0 overload. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band.
The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities.
Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right- looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **363**
展示資料を参照してください。



ネットワークエンジニアは、R1 が 10.0.0.0/24 ネットワーク宛てのすべてのパケットを R3 に送信し、PCI 宛てのすべてのパケットを R2 に送信するように構成する必要があります。エンジニアはどのような構成を実装する必要がありますか？

A.
```
R1(config)#ip route 10.0.0.0 255.255.255.0 172.16.0.2
R1(config)#ip route 10.0.0.5 255.255.255.255 192.168.0.2
```

B.
```
R1(config)#ip route 10.0.0.0 255.255.0.0 172.16.0.2
R1(config)#ip route 10.0.0.5 255.255.255.255 192.168.0.2
```

C.
```
R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.0.2
R1(config)#ip route 10.0.0.5 255.255.255.255 172.16.0.2
```

D.
```
R1(config)#ip route 10.0.0.0 255.255.0.0 192.168.0.2
R1(config)#ip route 10.0.0.0 255.255.255.0 172.16.0.2
```

正解: **C** (コメントを発表する)

Option C. The answer follows from normal Cisco device behavior and the operating clue in the scenario.
Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The other options use adjacent terms, wrong-layer behavior, or configuration that would not produce the requested result. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **364**

エンジニアが、Wi-Fi ネットワーク上に静的 IP アドレスを持つ新しいワイヤレス プリンターをインストールしています。
プリンターとの接続の問題を防ぐために、どの機能を有効にして構成する必要がありますか?

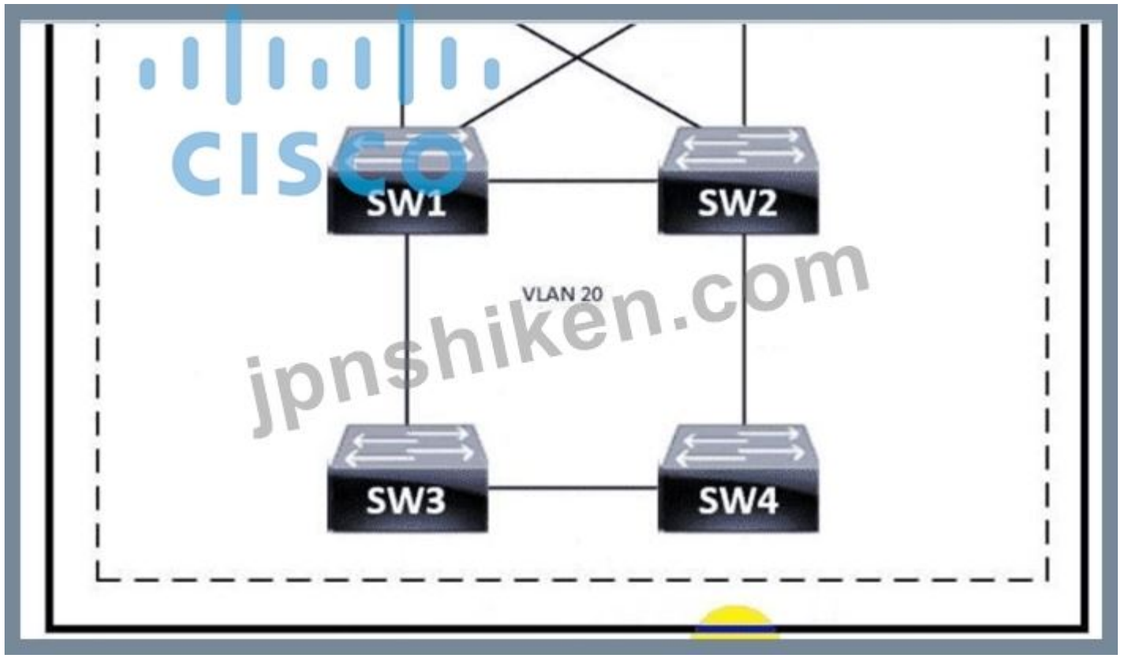
A. クライアント除外
B. パッシブ クライアント
C. DHCP アドレスの割り当て
D. 静的 IP トンネリング

正解: **B** (コメントを発表する)

passive client. Wireless clients with static IP addresses can be affected by controller behavior that expects DHCP learning for client state. On Cisco WLCs, the passive client feature is used for devices such as wireless printers that do not behave like typical DHCP clients or that use static addressing. DHCP address assignment is not the right answer because the prompt explicitly says the printer uses a static IP address. Client exclusion blocks or delays client access after failures; it does not solve static-client reachability. Static IP tunneling is not the standard WLC feature required here. Cisco CCNA 200-301 v1.1 Network Access expects candidates to recognize this common wireless operations issue. The corrected answer is passive client. Enabling that feature helps the WLC support static-IP wireless devices without unnecessary connectivity problems.

質問: **365**

展示資料を参照してください。



すべてのリンクの速度が同じ場合、VLAN 20のスパニングツリーのルートとなるスイッチはどれですか？

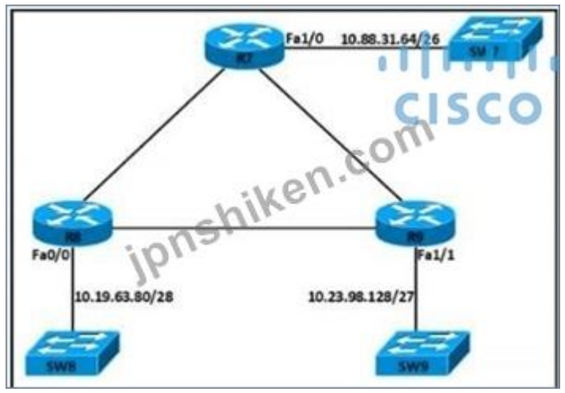
SW1 = 24596 0018.184e.3c00
SW2 = 28692 004a.14e5.4077
SW3 = 32788 0022.55cf.dd00
SW4 = 64000 0041.454d.407f

A. SW1
B. SW2
C. SW3
D. SW4

正解: **(正解を表示します)**

SW3. Switching behavior depends on VLAN tagging, trunk negotiation, STP role selection, EtherChannel mode, and whether a protocol is standards-based or Cisco-specific. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. Incorrect options change existing VLAN reachability, use the wrong negotiation behavior, or apply a feature to the wrong switch function. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **366**



図を参照してください。各ルータには、サブネット内で最後に使用可能なIPアドレスを設定する必要があります。この要件を満たす設定はどれですか？

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

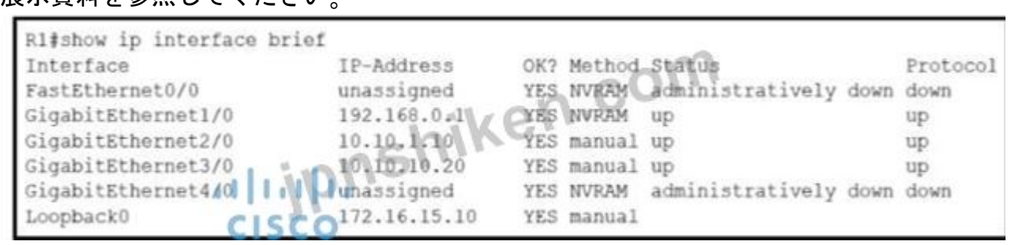
正解: **(**正解を表示します**)**

Option C. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **367**

図を参照してください。ネットワークエンジニアがリモートアクセスを可能にするためにSW1のデフォルト設定を変更し始め、設定モードで以下の内容を入力しました。
SW1(config)#line vty 0 15
SW1(config-line)#password Labtest32!
SSHアクセスのみを許可し、実行中の設定ファイルでパスワードを隠すには、どのコマンドセットが必要ですか？
A. SW1(config-line)#exitSW1(config)#aaa new-model
B. SW1(config-line)#login localSW1(config-line)#exitSW1(config)#enable secret test!2E
C. SW1(config-line)#transport input sshSW1(config-line)#exitSW1(config)#service password-encryption
D. SW1(config-line)#login localSW1(config-line)#exitSW1(config)#crypto key generate rsa
正解: **(**正解を表示します**)**
SW1(config-line)#transport input sshSW1(config-line)#exitSW1(config)#service password-encryption. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **368**
展示資料を参照してください。

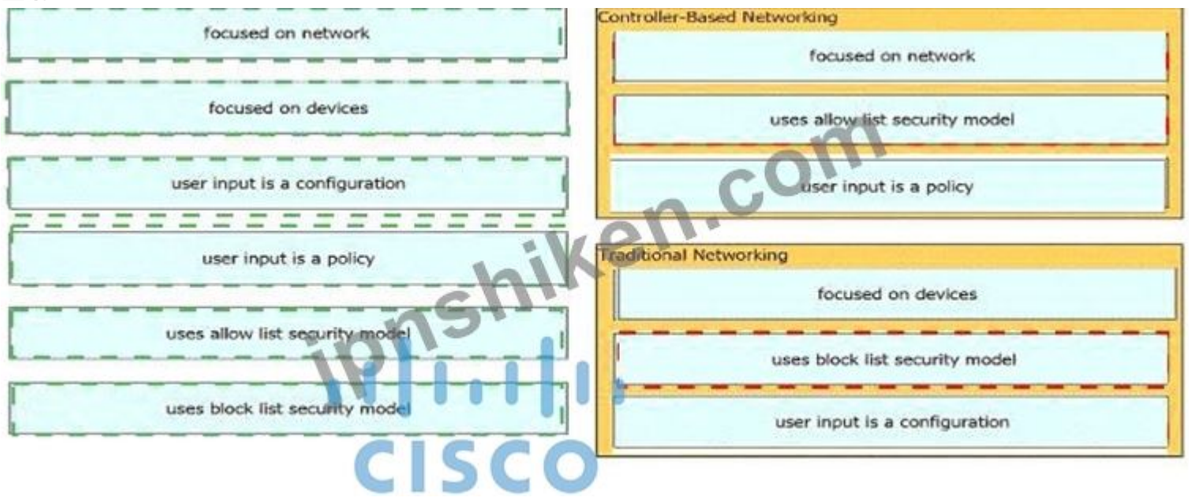


ルーターR1はOSPFルーターIDとして何を使用しますか？
A. 10.10.1.10
B. 2020年10月10日
C. 172.16.15.10
D. 192.168.0.1
正解: **C (**コメントを発表する**)**
172.16.15.10. OSPF decisions depend on router IDs, area membership, matching timers, network type, interface state, and cost calculation rather than arbitrary route preference. Cisco CCNA 200-301 v1.1 includes this topic under IP Connectivity, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. Distractors that mention process IDs, unrelated metrics, or the wrong interface parameter do not satisfy OSPF

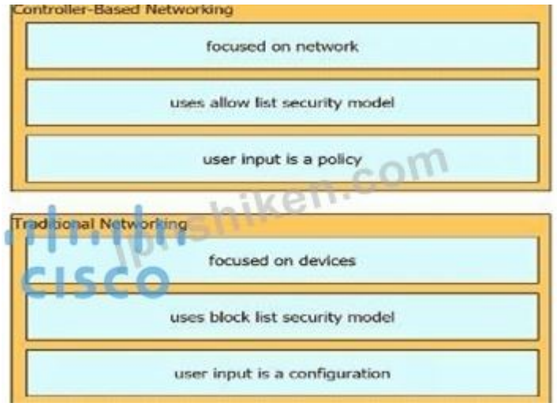
neighbor or route- selection requirements. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **369**
左側のネットワークの特徴を、右側のネットワークの種類にドラッグ＆ドロップしてください。

正解:



Explanation:
Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.



質問: **370**

展示資料を参照してください。

```
R1#

Gateway of last resort is 10.56.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.56.0.1
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.56.0.0/16 is directly connected, Null0
C        10.56.0.0/26 is directly connected, Vlan58
C        10.56.0.0/17 is directly connected, Vlan59
C        10.56.0.0/24 is directly connected, Vlan60
```

ルーターR1が宛先IPアドレス10.56.062のパケットを受信した場合、どのインターフェースを経由してパケットをルーティングしますか？

A. Null0

B. VLAN58

C. VLAN60

D. VLAN59

正解: **(正解を表示します)**

Vlan58. IP services questions require matching the service to its exact operational role, such as logging, address assignment, file transfer, monitoring, redundancy, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The distractors are real technologies, but they solve different infrastructure problems. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **371**

サービスポートインターフェースでサポートされているプロトコルはどれですか？(2つ選択してください。)

A. RADIUS

B. TACACS+

C. SCP

D. Telnet

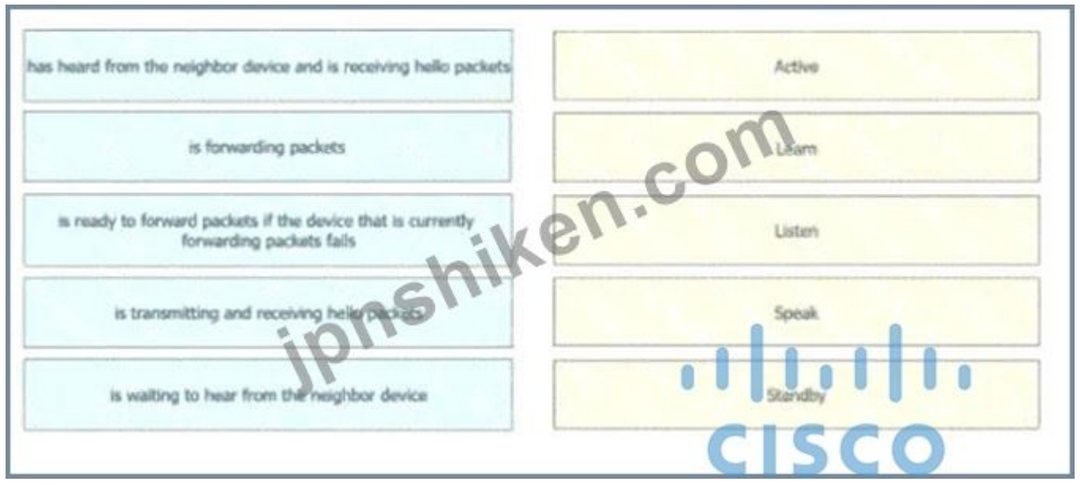
E. SSH

正解: **(正解を表示します)**

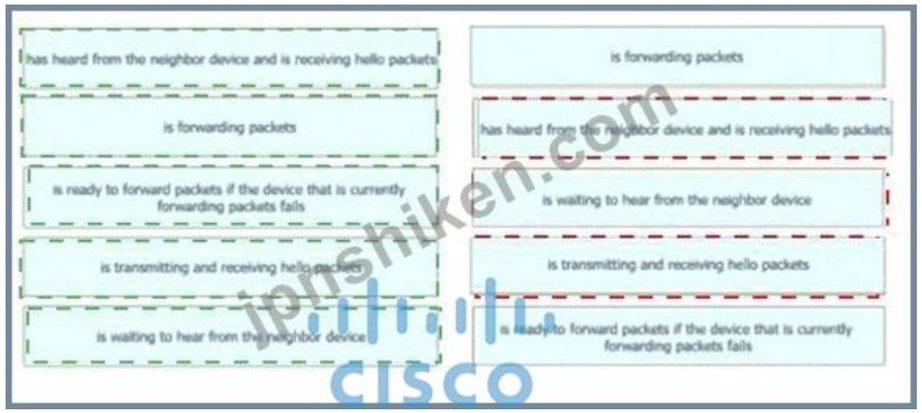
Answer D and E is the technically correct selection. Cisco WLC service-port management supports Telnet and SSH access. The service port is an out-of-band management interface and can be used for direct management connectivity depending on platform configuration. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. RADIUS and TACACS+ are AAA protocols, and SCP is file transfer, not the pair of management access protocols asked here. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

質問: **372**
Cisco DNA Center Intent API でオブジェクトを更新する REST メソッドはどれですか?
A. 変更
B. 更新
C. ポスト
D. 置く
正解: **(**正解を表示します**)**
PUT. Automation questions depend on recognizing controllers, APIs, data formats, HTTP methods, and cloud- service characteristics. Cisco CCNA 200-301 v1.1 includes this under Automation and Programmability, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The wrong options mix controller functions with data-plane forwarding or confuse API operations with unrelated management terms. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **373**
左側のデバイス動作を、右側の対応するHSRP状態にドラッグアンドドロップしてください。



jpnshiken.com
CISCO
正解:



Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals drag-and-drop items test whether each protocol, address type, API action, or infrastructure component is matched to its real function. The correct way to solve these is to classify every item by layer, scope, and operational behavior before matching it. Several distractors are legitimate networking terms, but they are wrong when placed under the wrong protocol family or management model. The retained mapping preserves the Cisco distinctions between TCP and UDP behavior, AAA functions, IPv6 address scopes, device-management approaches, and REST operations. In implementation work, these distinctions matter because applying a feature at the wrong layer or associating a control with the wrong service creates broken configurations and wasted troubleshooting effort. The shown mapping is therefore retained as the verified response.

質問: **374**

ソフトウェア定義ネットワークには、次のうちどの2つの北向きAPIがありますか？(2つ選択してください。)

A. OpenFlow

B. REST

C. OpFlex

D. SOAP

E. NETCONF

正解: **(**正解を表示します**)**

Answer B,D is correct: B. REST; D. SOAP. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE. JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact

with a controller, while southbound APIs allow the controller to communicate with network devices. NETCONF and RESTCONF are configuration/management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to-device communication with application-to-controller communication or confuse a data format with a protocol. Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers. The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

質問: **375**
スイッチ ポートが前のフレームをアクティブに送信しているときに新しいフレームを受信した場合、フレームはどのように処理されますか?
A. 新しいフレームが最初に配信され、前のフレームが破棄され、再送要求が送信されます。
B. 前のフレームが配信され、新しいフレームがドロップされ、再送要求が送信されます。
C. 新しいフレームは、前のフレームの後に送信するためにキューに入れられます。
D. 2 つのフレームが同時に処理され、配信されます。
正解: **(**正解を表示します**)**
Answer C is the technically correct selection. A switch queues a new frame if the egress port is already transmitting another frame. Ethernet interfaces transmit one frame at a time on the link, so buffering handles temporary contention. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. The switch does not drop a valid new frame just because another frame is currently being transmitted unless buffers are exhausted. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

質問: **376**
VoIPなど、低遅延が求められるアプリケーションにおいて、UDPがTCPよりも適しているのはなぜですか？
A. TCPは効率的なパケット配信のために輻輳制御を使用し、UDPはパケット配信のためにフロー制御メカニズムを使用します。
B. TCPは受信したパケットごとに確認応答を送信し、UDPは確認応答なしで動作します。
C. UDPはすべてのパケットの確実な配信を保証しますが、TCPは負荷が高い場合にパケットを破棄します。
D. UDPはパケットが順番に到着するようにシーケンスデータを使用し、TCPはパケットをランダムな順序で受信する機能を提供します。
正解: **(**正解を表示します**)**
TCP sends an acknowledgment for every packet that is received, and UDP operates without acknowledgments.. Network fundamentals questions require careful attention to address scope, media type, cabling limits, topology design, virtualization, cloud service models, and the difference between TCP and UDP. The CCNA 200-301 v1.1 blueprint expects candidates to identify not only definitions but also the operational consequence of each choice. For example, public and private addressing have different routing behavior; fiber and copper use different physical media; TCP and UDP make different reliability tradeoffs; and virtualization abstracts physical resources through a hypervisor. The wrong answers are usually plausible terms from the same area, but they do not match the exact condition described in the question. The selected answer is correct because it is the only option that fits the stated network behavior, design requirement, or physical/logical property. That is the level of precision needed for Cisco troubleshooting and implementation work.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **377**
スイッチは Fa0/1 で受信した宛先 MAC アドレスのフレームをどのように処理しますか?
テーブルにアドレスがない場合は 0e38.7363.657b ですか?
A. フレームをすぐにドロップします。

B. フレームをインターフェイス Fa0/1 から転送します。
C. Fa0/1 以外のすべてのインターフェースにフレームをフラッディングします。
D. MAC アドレス タイマーが満了するまでフレームを保持し、その後フレームをドロップします。
正解: (正解を表示します)
The verified answer is C. A Layer 2 switch floods an unknown unicast frame when the destination MAC address is missing from its MAC address table. The flood is limited to ports in the same VLAN and excludes the ingress port where the frame arrived. Cisco CCNA 200-301 v1.1 places this skill in Network Access, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. The switch does not drop the frame immediately, send it back out the receiving port, or wait for the aging timer to expire. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **378**
T1 ポイントツーポイント接続の最大帯域幅は?
A. 1.544Mbps
B. 2.048Mbps
C. 34.368Mbps
D. 43.7Mbps
正解: (正解を表示します)
Use A for this item. A T1 point-to-point circuit provides 1.544 Mbps of bandwidth. T1 service is a legacy digital carrier technology built from twenty-four 64-kbps DS0 channels plus framing overhead. In Cisco CCNA 200-301 v1.1, Network Fundamentals questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. 2.048 Mbps is associated with E1 service, while the larger values describe higher-capacity carrier circuits. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **379**
アクセス ポイントがワイヤレス LAN コントローラに参加しようとしているときに、AP マネージャ インターフェイスに送信されるメッセージはどれですか?
A. ディスカバリ応答
B. DHCP リクエスト
C. DHCP 検出
D. ディスカバリ リクエスト
正解: (正解を表示します)
Discovery request. Wireless questions depend on AP mode, WLAN security, RF band selection, controller interfaces, and client roaming or authentication behavior. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong options confuse encryption with authentication, local switching with tunneling, or controller management with client data handling. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

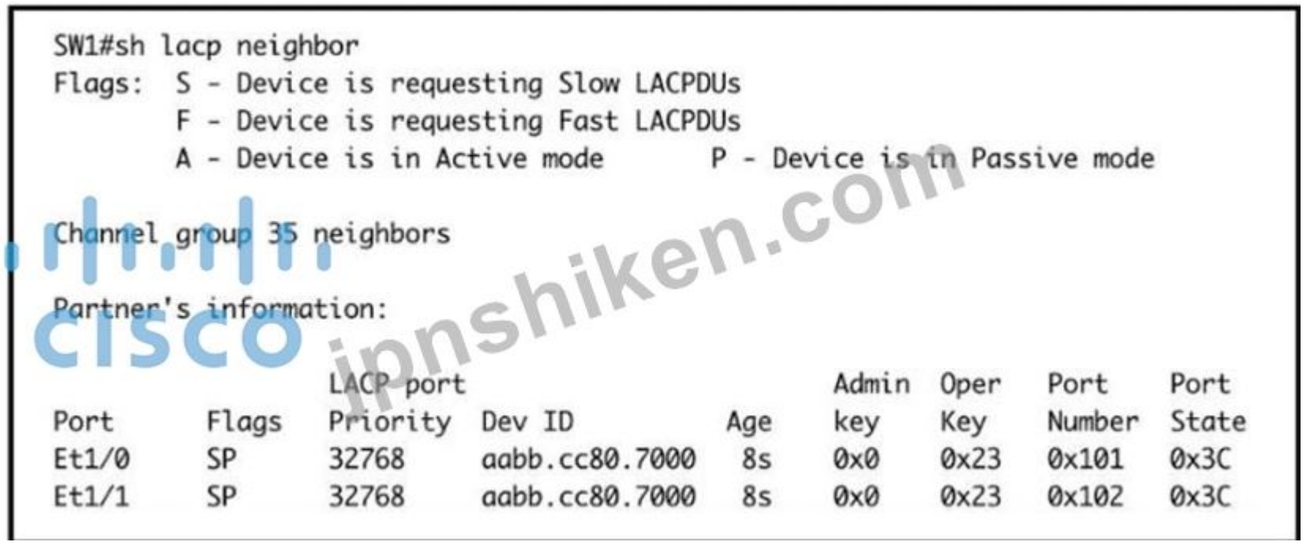
質問: **380**
中間者攻撃を防ぐために使用されるセキュリティ方法はどれですか?
A. 認可
B. 認証
C. アンチリプレイ

D. 会計
正解: **B** (コメントを発表する)
authentication. Security questions require distinguishing authentication, authorization, encryption, secure management, malware protection, and physical controls. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The wrong options apply the right security vocabulary to the wrong control or use weaker/deprecated protection. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **381**
企業のネットワークの拡張性と信頼性を向上させるのに役立つWANアーキテクチャのオプションはどれですか？(2つ選択してください)
A. 非同期ルーティング
B. シングルホームブランチ
C. デュアルホームブランチ
D. 静的ルーティング
E. 動的ルーティング
正解: (正解を表示します)
The two options that improve WAN scalability and reliability are dual-homed branches and dynamic routing.
A dual-homed branch has more than one upstream connection, which reduces the chance that a single circuit, provider, or edge device failure disconnects the site. Dynamic routing improves scalability because routes can be learned, withdrawn, and recalculated automatically as the WAN changes. Static routing can work in small topologies, but it becomes operationally fragile at scale. Single-homed branches are simpler but less resilient.
The listed ' asynchronous routing ' choice is not the correct CCNA design answer for business scalability and reliability. Cisco CCNA 200-301 v1.1 IP Connectivity expects engineers to understand that redundancy and automatic route convergence are core design tools. A WAN with dual connectivity and dynamic routing can survive failures and grow with less manual intervention. Therefore, the corrected answer is C and E.

質問: **382**
IPv6のリンクローカルアドレスとユニークローカルアドレスの違いは何ですか？
A. IPv6リンクローカルアドレスのスコープはループバックアドレスに限定され、IPv6ユニークローカルアドレスは直接接続されたインターフェースに限定されます。
B. IPv6リンクローカルアドレスのスコープは、企業サイトまたはネットワーク全体で使用できますが、IPv6ユニークローカルアドレスはループバックアドレスに限定されます。
C. IPv6リンクローカルアドレスのスコープはグローバルですが、IPv6ユニークローカルアドレスのスコープはループバックアドレスに限定されます。
D. IPv6リンクローカルアドレスの適用範囲は直接接続されたインターフェースに限定されますが、IPv6ユニークローカルアドレスは企業サイトまたはネットワーク全体で使用されます。
正解: (正解を表示します)
The scope of an IPv6 link-local addresss can be used throughout a company site or network, but an IPv6 unique local addresss is limited to a loopback addresss.. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco- consistent configuration or behavior for this wireless scenario.

質問: **383**
展示資料を参照してください。



LACPネイバーの状態に基づいて、SW1ポートチャネルはどのモードで構成されていますか？

A. 受動態

B. モードオン

C. 自動

D. アクティブ

正解: (正解を表示します)

active. Switching features such as trunks and EtherChannels are controlled by negotiation mode, encapsulation, VLAN membership, and whether the selected protocol is Cisco proprietary or standards based. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces.

The incorrect options either disable negotiation, select the wrong negotiation protocol, or configure a mode that cannot form the requested link under the stated conditions. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **384**

デバイスが Cisco DNA Center に追加されたときに自動的に発生する 2 つのイベントはどれですか？ 2つお選びください。）

A. デバイスはグローバル サイトに割り当てられます。

B. デバイスは非管理状態になります。

C. デバイスはプロビジョニング済み状態になります。

D. デバイスは管理状態になります。

E. デバイスはローカル サイトに割り当てられます。

正解: (正解を表示します)

The correct response is A and B. When a device is added to Cisco DNA Center, it is initially associated with the Global site and placed in an unmanaged state until claimed or provisioned. Provisioning is a later workflow that applies site-specific intent and configuration. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. Local site assignment and managed /provisioned status require additional administrative action. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **385**
2 台のルータ間の単一エリアでユーザが設定した OSPF R1 と R2 を接続するシリアル インターフェイスは、カプセル化 PPP を実行しています。
デフォルトでは、R1 または R2 でユーザー タイプが ip ospf インターフェイスを表示するときに、このインターフェイスでどの OSPF ネットワーク タイプが表示されますか?
A. ポートからマルチポイントへ
B. ブロードキャスト
C. ポイントツーポイント
D. 非放送
正解: **(**正解を表示します**)**
point-to-point. OSPF decisions depend on router IDs, area membership, matching timers, network type, interface state, and cost calculation rather than arbitrary route preference. Cisco CCNA 200-301 v1.1 includes this topic under IP Connectivity, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. Distractors that mention process IDs, unrelated metrics, or the wrong interface parameter do not satisfy OSPF neighbor or route- selection requirements. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

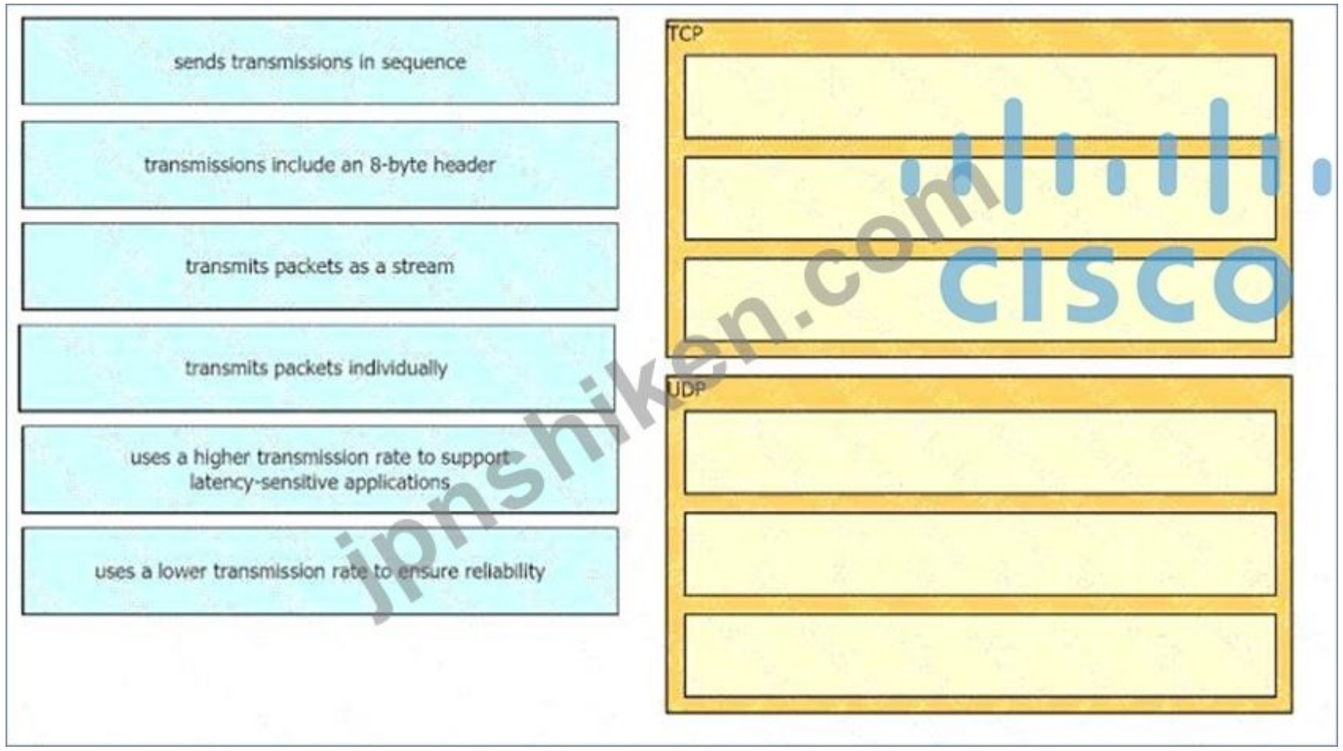
質問: **386**
Cisco DNA Centerの機能は何ですか？
A. データセンターネットワークポリシー制御
B. すべてのネットワークデバイスへの安全なアクセスを許可するコンソールサーバー
C. IPアドレスプール配布スケジューラ
D. デバイスとサービスの自動化のためのソフトウェア定義コントローラ
正解: **D (**コメントを発表する**)**
software-defined controller for automation of devices and services. Automation questions require recognizing data structures, HTTP methods, APIs, controllers, and the separation of northbound and southbound communication. Cisco CCNA 200-301 v1.1 includes this under Automation and Programmability, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Distractors mix application-facing and device- facing roles or confuse values, keys, arrays, and objects. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **387**
ルーターを DHCP クライアントにできるようにするコマンドはどれですか?
A. IP アドレス dhcp
B. IP ヘルパー アドレス
C. ip dhcp プール
D. ip dhcp クライアント
正解: **(**正解を表示します**)**
The command ip address dhcp makes a Cisco router interface act as a DHCP client. Instead of manually assigning an IPv4 address and mask to the interface, the router sends DHCP client messages and accepts an address, default gateway information, and other options from a DHCP server when available. The ip helper- address command is different: it configures DHCP relay on an interface so client broadcasts can be forwarded to a DHCP server on another subnet. The ip dhcp pool command builds a DHCP server pool on the router, and ip dhcp client is not the interface command used for this purpose. This is a typical CCNA 200-301 v1.1 IP Services distinction: client, server, and relay roles are separate. When a router must obtain its own interface address dynamically, configure ip address dhcp under the interface and ensure the interface is no shutdown.

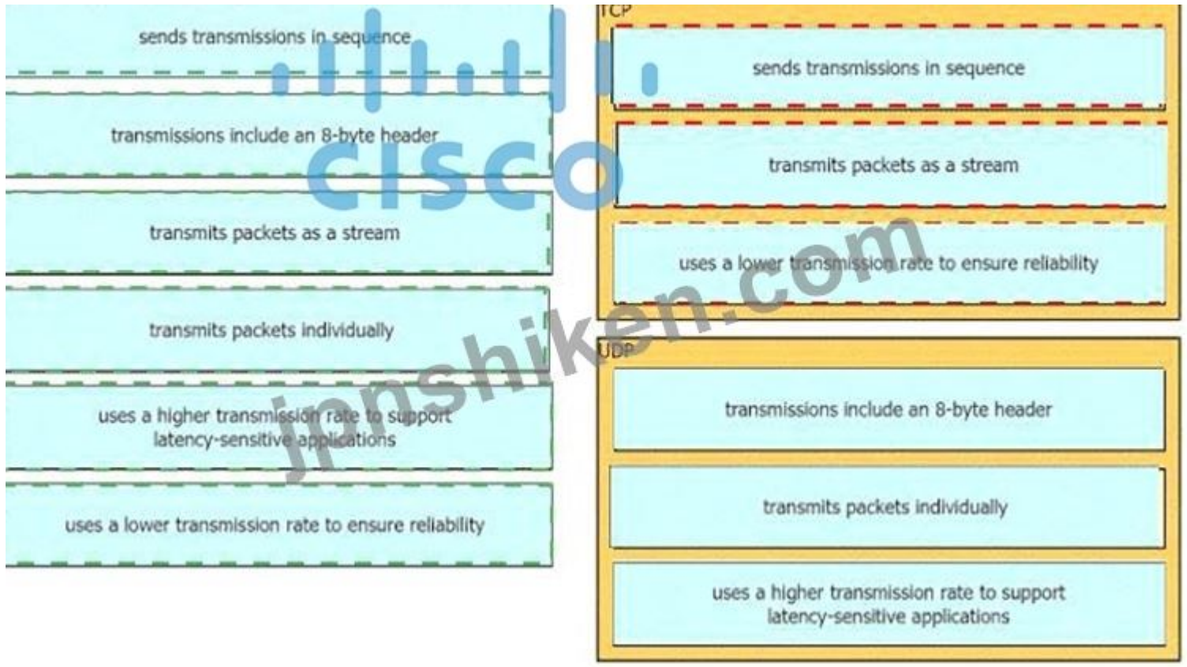
Therefore the verified answer is A. Reference: Cisco IOS DHCP client configuration guidance.

質問: 388

左側のIPプロトコル伝送の説明を、右側のIPトラフィックの種類にドラッグしてください。



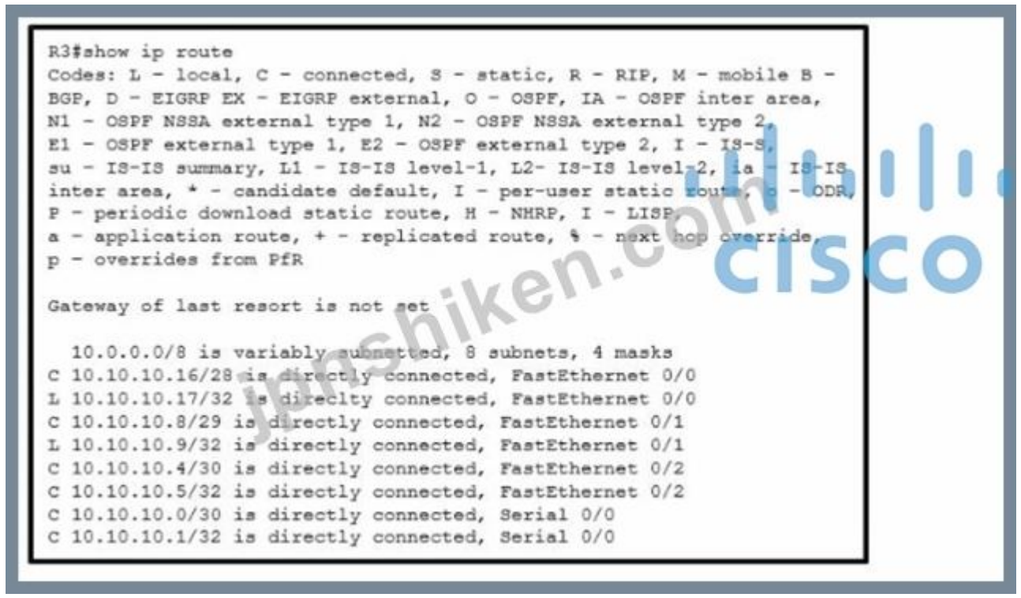
正解:



Explanation:

This item belongs to Cisco CCNA 200-301 v1.1 Network Fundamentals, where the exam measures whether the candidate can match a technology, field, protocol, or network behavior to its correct operational role. The important step is to classify each left-side item by what it actually does, not by a similar-sounding term. For example, management protocols, address types, QoS mechanisms, wireless settings, and topology terms all have strict meanings in Cisco documentation and IOS behavior. A wrong match usually places a function at the wrong layer or assigns a feature to the wrong control point. The shown mapping keeps those boundaries intact: the component that performs the function is paired with the matching description, while unrelated distractors are left unused or mapped elsewhere. In real troubleshooting, this same skill prevents engineers from applying a security, routing, switching, or automation feature in the wrong part of the design.

質問: 389



図を参照してください。パケットが宛先アドレス10.10.10.147に到達するには、どのインターフェースを経由しますか？

A. FastEthemet 0/0

B. セナル0/0

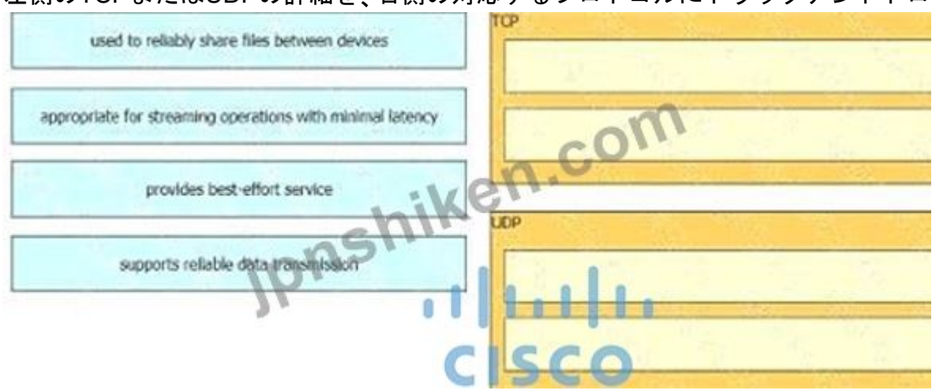
C. 高速イーサネット 0/1

正解: (正解を表示します)

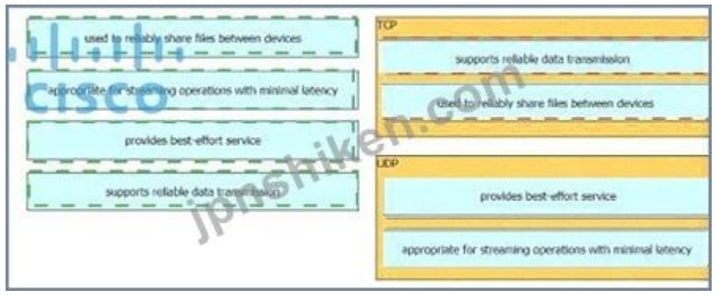
Senal0/0. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **390**

左側のTCPまたはUDPの詳細を、右側の対応するプロトコルにドラッグアンドドロップしてください。

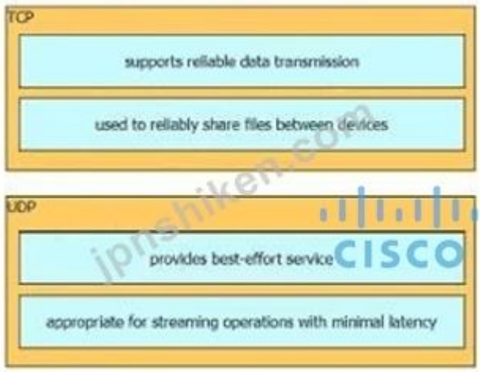


正解:



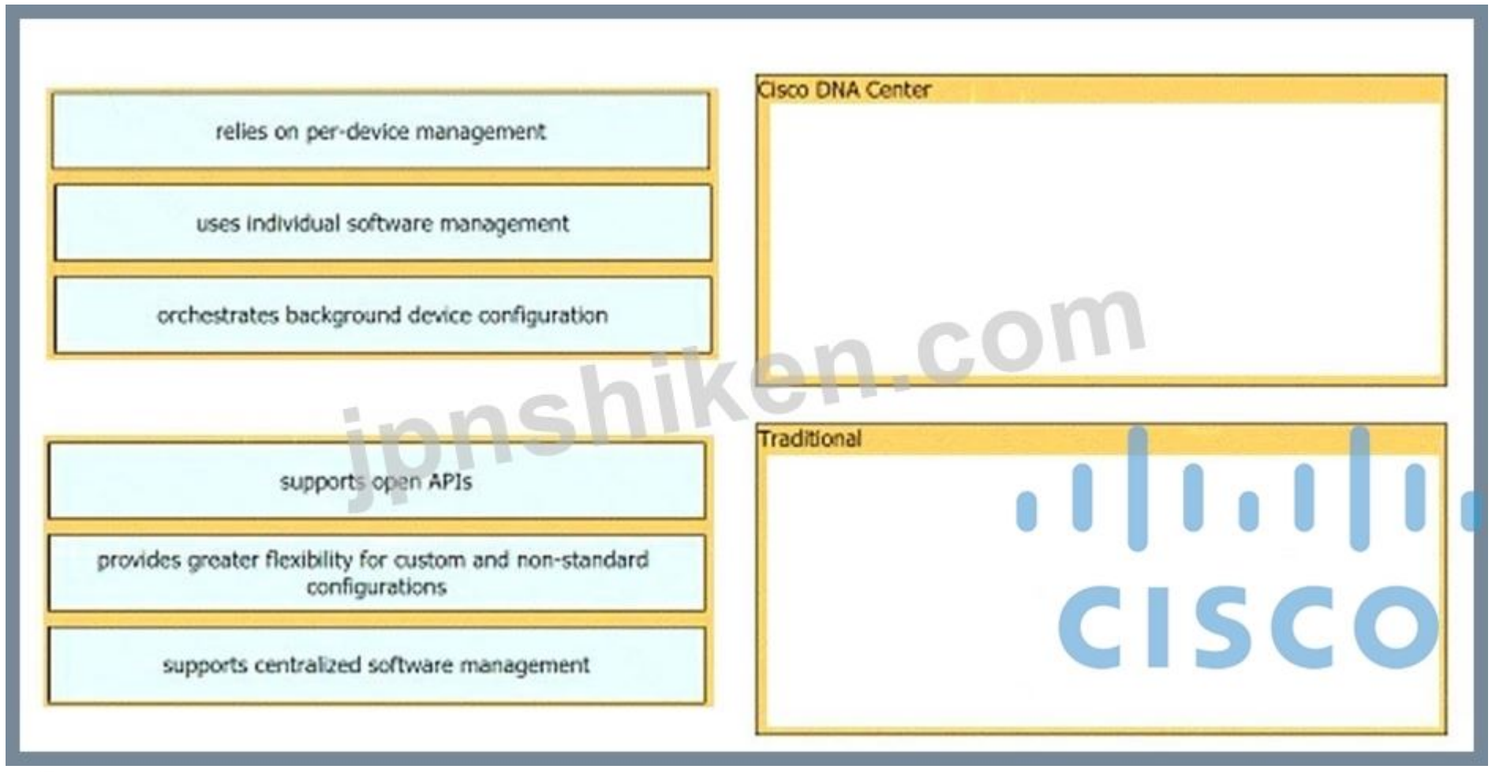
Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.

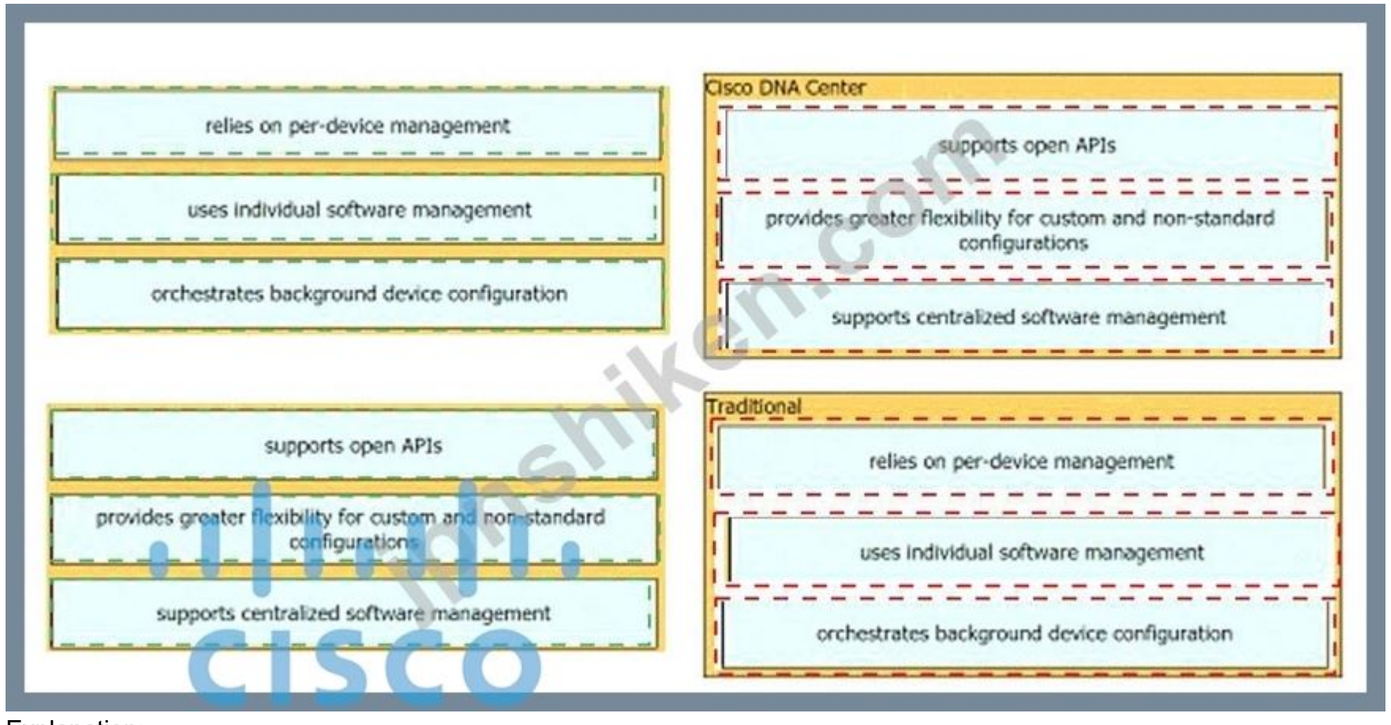


質問: 391

左側のデバイス管理技術の各特性を、右側の展開タイプにドラッグ＆ドロップしてください。

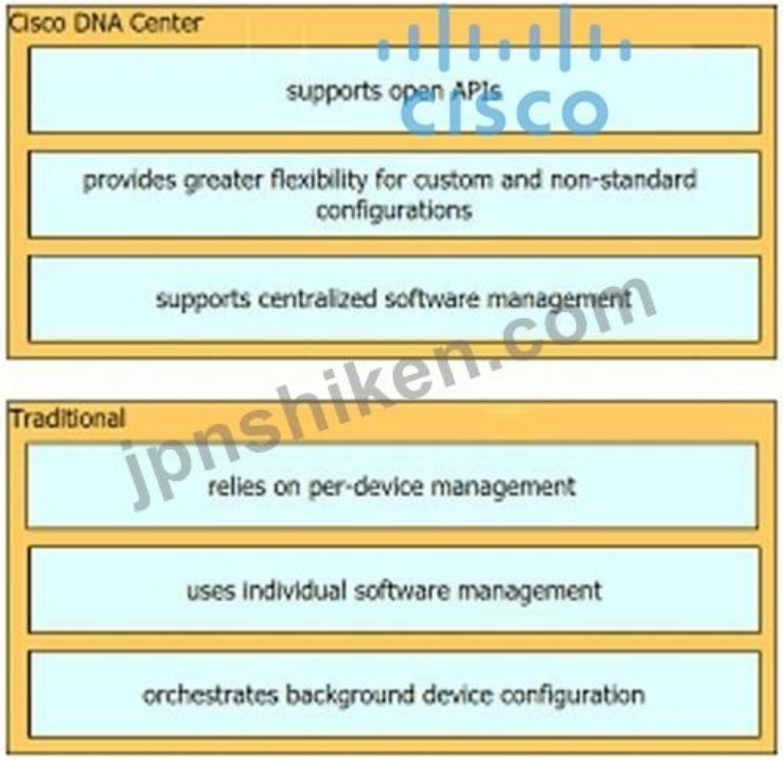


正解:



Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.



有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

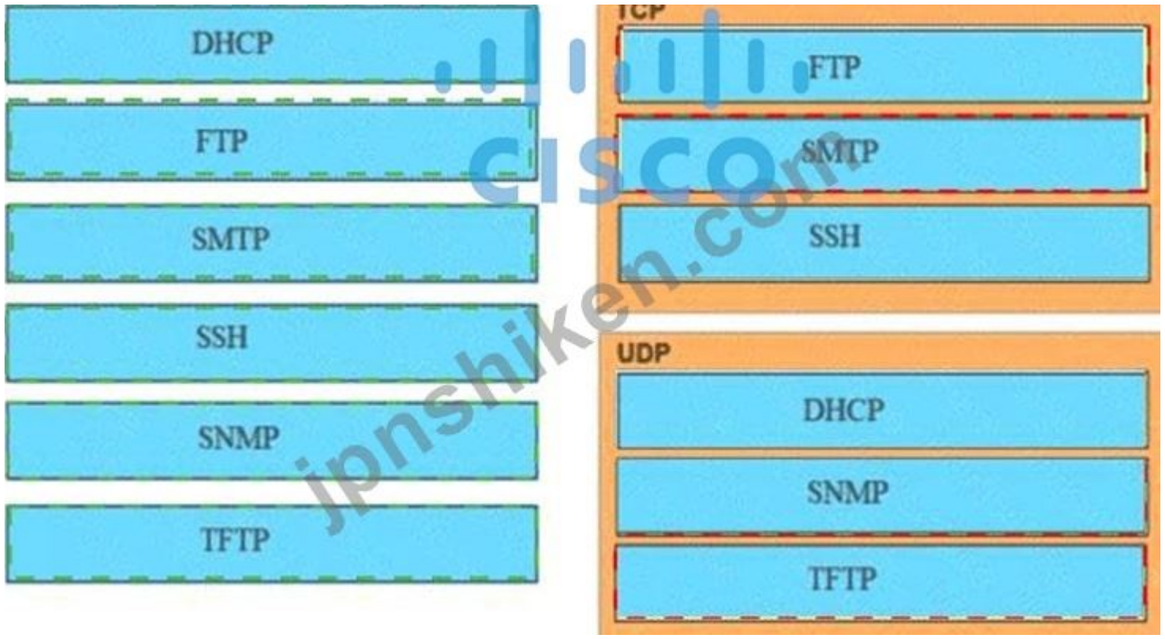
質問: **392**
展示資料を参照してください。

R1は、192 168.16.2宛てのトラフィックに対してどの経路を選択しますか？

A. 192.168.16.0/21
B. 192.168.16.0/24
C. 192.168 26.0/26
D. 192.168.16.0/27
正解: **D** (コメントを発表する)
192.168.16.0/27. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under IP Services, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **393**
左側のアプリケーションプロトコルを、右側のアプリケーションプロトコルが使用するトランスポートプロトコルにドラッグアンドドロップしてください。

正解:



Explanation:

This item belongs to Cisco CCNA 200-301 v1.1 Network Fundamentals, where the exam measures whether the candidate can match a technology, field, protocol, or network behavior to its correct operational role. The important step is to classify each left-side item by what it actually does, not by a similar-sounding term. For example, management protocols, address types, QoS mechanisms, wireless settings, and topology terms all have strict meanings in Cisco documentation and IOS behavior. A wrong match usually places a function at the wrong layer or assigns a feature to the wrong control point. The shown mapping keeps those boundaries intact: the component that performs the function is paired with the matching description, while unrelated distractors are left unused or mapped elsewhere. In real troubleshooting, this same skill prevents engineers from applying a security, routing, switching, or automation feature in the wrong part of the design.

質問: **394**

展示資料を参照してください。

ネットワーク環境が正常に動作している場合、FastEthernet 0/1インターフェースにはどのタイプのデバイスを接続する必要がありますか？

A. DHCPクライアント

B. アクセスポイント

C. ルーター

D. PC

正解: **C (**コメントを発表する**)**

The exhibit shows an interface configured as trusted for Dynamic ARP Inspection. In a normal access-layer design, trusted DAI ports are not user-facing ports. They are uplinks or infrastructure-facing links where valid ARP replies may arrive, typically toward a router, distribution switch, or another trusted network device. End- user devices such as PCs and ordinary DHCP clients should stay untrusted so the switch can validate their ARP traffic against the DHCP snooping binding database. If an untrusted host sends forged ARP information, DAI can drop it before it poisons neighboring hosts. That is why the device connected to FastEthernet0/1 is expected to be a router in this scenario. Cisco CCNA 200-301 v1.1 places this under IP Services and access- layer security behavior because DHCP snooping and DAI work together to protect Layer 2 addressing. The clue is the ip arp inspection trust interface setting. A trusted port should face infrastructure, not an endpoint, so C is correct.

質問: **395**

崩壊型コアネットワークトポロジーの特徴は何ですか？

A. コア層とディストリビューション層を単一の結合層として実行できるようにします。

B. コア層とアクセス層が、EtherChannel を介して 1 つの論理ディストリビューション デバイスに接続できるようにします。

C. SOHO環境内のすべてのワークステーションを単一のスイッチに接続し、インターネットアクセスを可能にします。

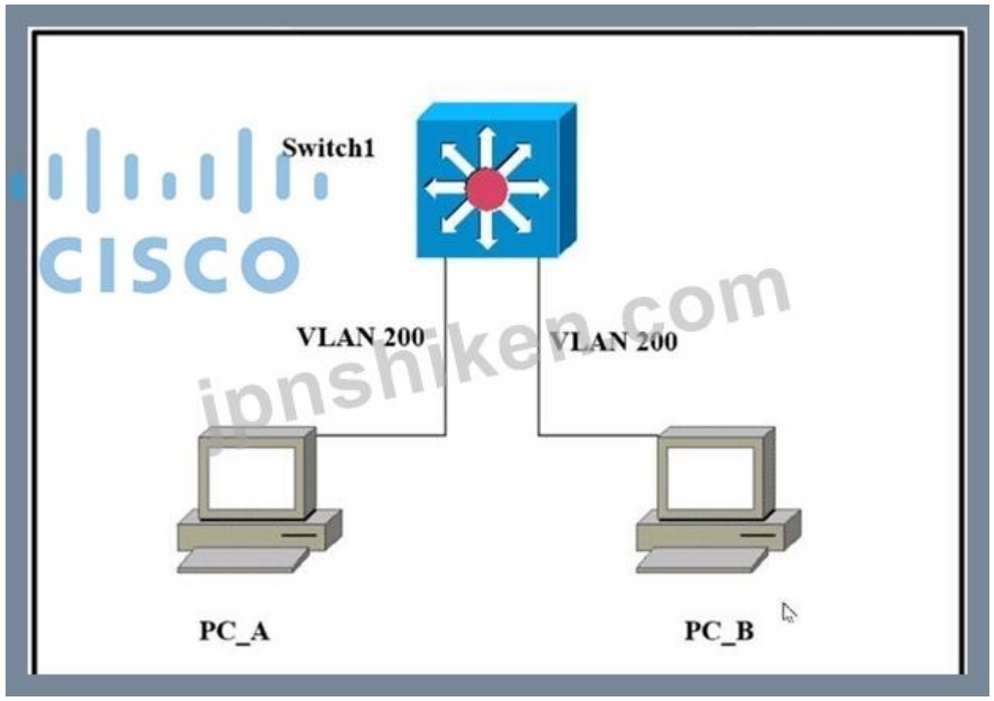
D. ワイヤレスデバイスがコア層に直接接続できるようになり、より高速なデータ伝送が可能になります。

正解: **(**正解を表示します**)**

It allows the core and distribution layers to run as a single combined layer.. A collapsed-core design combines the core and distribution layers into a single functional layer. It is used when a separate core is unnecessary for the size or scale of the network. It does not mean the access and core layers connect through EtherChannel to one logical distribution device, and it is not a SOHO single-switch design. Cisco CCNA 200-301 v1.1 Network Fundamentals expects candidates to distinguish two-tier and three-tier campus models. In a two-tier collapsed-core design, access switches connect to devices that provide both distribution-layer policy/routing and core-like aggregation. The corrected answer is that the core and distribution layers run as one combined layer. This keeps the design simpler while retaining separation between the access layer and the combined aggregation layer.

質問: **396**

展示資料を参照してください。



PC_AがPC_Bにデータを送信した場合、どのような結果が予想されますか？
A. スイッチは送信元および宛先の MAC アドレスを自身のアドレスで書き換えます。
B. 送信元MACアドレスが変更されました。
C. 送信元および宛先のMACアドレスは変更されません。
D. 宛先MACアドレスはffff.ffff.ffffに置き換えられます。
正解: (正解を表示します)
A Layer 2 switch does not rewrite source and destination MAC addresses when forwarding a normal Ethernet frame within the same VLAN. It learns the source MAC address from the incoming frame, looks up the destination MAC address in its MAC table, and forwards the frame out the appropriate port. The frame ' s Layer 2 addresses remain the original source host MAC and destination host MAC. A router behaves differently: when routing between networks, it removes the old Layer 2 header and builds a new one for the next hop. This question is testing that boundary. Cisco CCNA 200-301 v1.1 Network Access requires candidates to understand switching behavior at Layer 2 versus routing behavior at Layer 3. The switch may flood if the destination is unknown, but it still does not replace addresses with its own. It also does not change the destination to ffff.ffff.ffff unless the original frame is a broadcast. The expected outcome is that source and destination MAC addresses remain the same.

質問: **397**
ワイヤレス LAN コントローラ GUI で WPA2 PSK を使用する WLAN が設定されている場合、どのフォーマットがサポートされますか?
A. ユニコード
B. base64
C. 10 進数
D. アスキー
正解: (正解を表示します)
ASCII. Wireless designs depend on the correct access point mode, WLAN security method, controller function, RF band behavior, and client authentication process. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The wrong options confuse authentication with encryption, autonomous behavior with controller-based operation, or management

functions with client data forwarding. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **398**
マネージャはネットワーク エンジニアに、従業員がたまにしか使用しないソフトウェアのインストール、管理、および更新に時間を浪費する必要がないように、どのクラウド サービス モデルが使用されているかをアドバイスするように依頼します。エンジニアはどのクラウド サービス モデルを推奨しますか?
A. サービスとしてのインフラストラクチャ
B. サービスとしてのプラットフォーム
C. さまざまなタイプのサービスをサポートするサービスとしてのビジネス プロセス
D. サービスとしてのソフトウェア
正解: **(**正解を表示します**)**
Software as a Service is the cloud model used when employees need to consume an application without installing, managing, patching, or updating the software themselves. The provider operates the application and supporting infrastructure, and users access the service through a browser or client. That is exactly the scenario described: occasional software use without local installation and administrative overhead. Infrastructure as a Service would still require the organization to manage operating systems and applications on virtual machines. Platform as a Service is aimed more at application development and runtime environments. The business-process option is not the standard CCNA cloud service model answer here. Cisco CCNA 200-301 v1.
1 Network Fundamentals expects candidates to distinguish SaaS, PaaS, and IaaS by responsibility boundary.
If the customer simply uses the finished application, the model is SaaS. The correct recommendation is software-as-a-service.

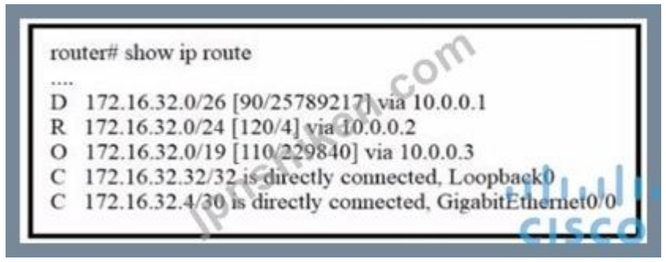
質問: **399**
企業環境に新しいDHCPサーバーが導入され、リース期間が8時間に設定されています。Windowsベースのデバイスでエンジニアが DHCPリースの有効期限を確認できるコマンドはどれですか？
A. ipconfig /renew
B. ipconfig
C. ipconfig /all
D. ipconfig /displaydns
正解: **C (**コメントを発表する**)**
ipconfig /all. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic.
Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **400**
指定した IPv6 プレフィックスとインターフェイスの MAC アドレスから IPv6 アドレスを自動的に生成するコマンドはどれですか?
A. ipv6 アドレス dhcp
B. ipv6 アドレス 2001:DB8:5:112::/64 eui-64
C. ipv6 アドレスの自動構成
D. ipv6 アドレス 2001:DB8:5:112::2/64 リンクローカル
正解: **(**正解を表示します**)**

The correct command is ipv6 address 2001:DB8:5:112::/64 eui-64. The wording says the address is generated from a specified IPv6 prefix and the interface MAC address. That is exactly what the eui-64 keyword does: it derives the 64-bit interface identifier from the MAC address and combines it with the configured /64 prefix.
The ipv6 address autoconfig command also can create an address, but it learns the prefix from Router Advertisement messages through SLAAC; the prefix is not explicitly specified in the command. DHCPv6 would request addressing information from a DHCPv6 server, and the link-local option shown is not a global unicast address built from the stated prefix. Cisco CCNA v1.1 Network Fundamentals includes IPv6 address types and address configuration methods, and this question tests precise IOS syntax. When the prefix is typed in the command and the MAC-derived interface ID is required, choose the static EUI-64 form, not autoconfig.

質問: **401**
従来型のネットワーク機器が担っていた機能のうち、ソフトウェア定義コントローラによって置き換えられるのはどれか？
A. VPNリンク処理のための暗号化と復号化
B. ルートテーブルの構築と転送テーブルの更新
C. NAT操作中に送信元アドレスまたは宛先アドレスを変更する
D. データリンクフレーム内のパケットのカプセル化とデカプセル化
正解: **(**正解を表示します**)**
building route tables and updating the forwarding table. Routing and redundancy questions are solved by applying longest-prefix match, administrative distance, metrics, and gateway-redundancy behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under Automation and Programmability, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Incorrect choices point to the wrong next hop, choose the wrong route source, or confuse routing with Layer 2 behavior. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

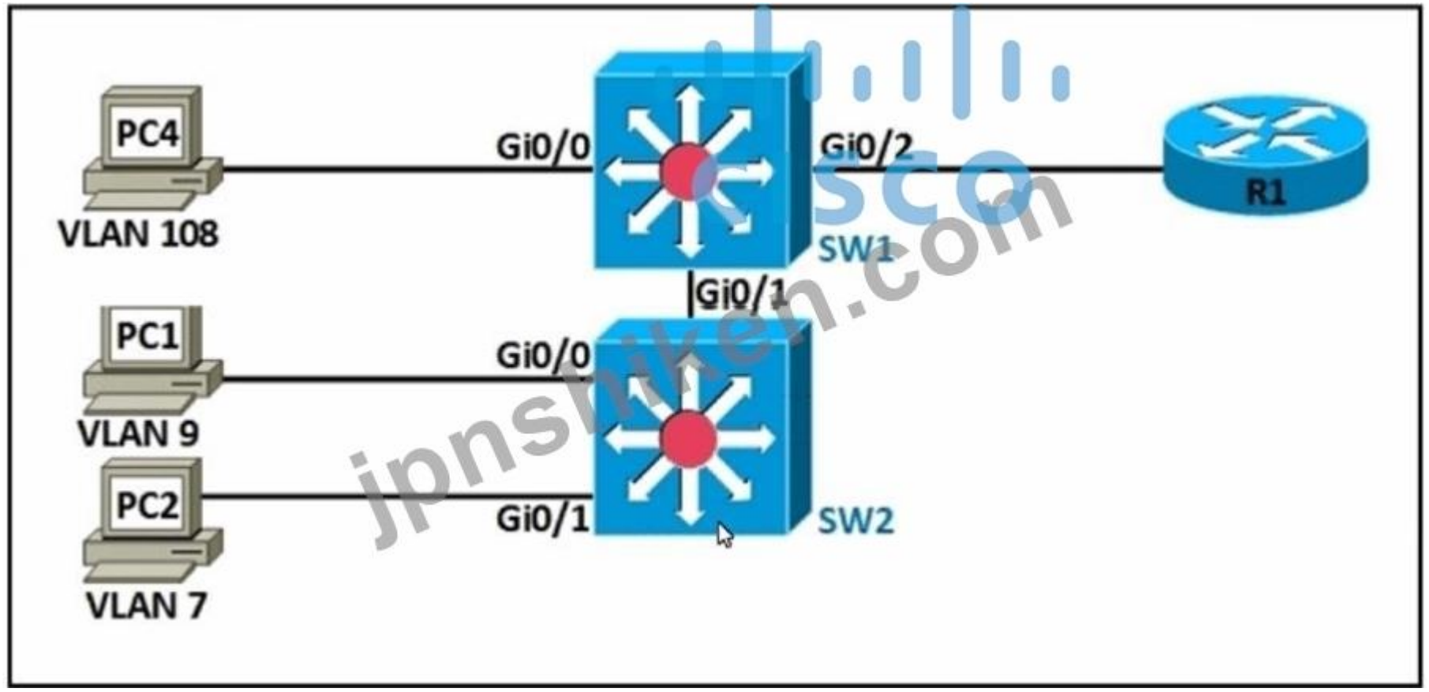
質問: **402**
展示資料を参照してください。



172.16.32 254 から送信されたパケットは、172.16.32.8 に送信されます。優先宛先ルートのサブネットマスクは何ですか？
A. 255.255.224.0
B. 255.255.255.0
C. 255.255.255.192
D. 255.255.255.252
正解: **C (**コメントを発表する**)**
255.255.255.192. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **403**
ソフトウェア定義ネットワークにおけるコントローラーの機能は何ですか?
A. ハードウェア レベルでのマルチキャスト レプリケーション
B. パケットの断片化と再組み立て
C. ルーティングの決定
D. 転送パケット
正解: (正解を表示します)
making routing decisions. Automation questions depend on recognizing controllers, APIs, data formats, HTTP methods, and cloud-service characteristics. Cisco CCNA 200-301 v1.1 includes this under Automation and Programmability, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The wrong options mix controller functions with data- plane forwarding or confuse API operations with unrelated management terms. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

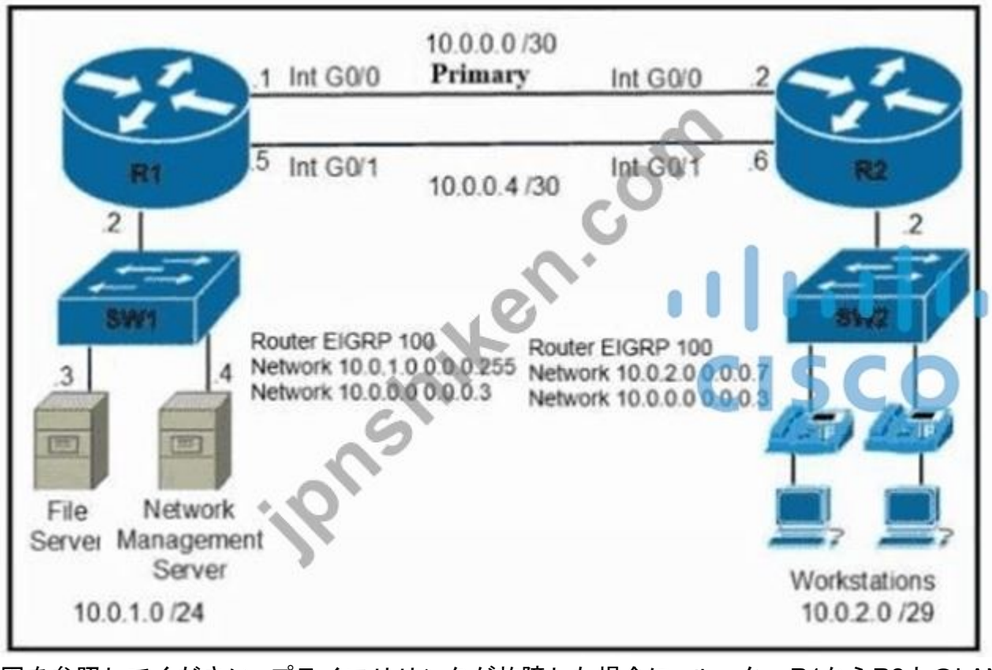
質問: **404**
展示資料を参照してください。



SW1およびSW2のGi0/0ポートは事前に設定済みです。エンジニアには以下の要件が与えられます。
* すべてのPCがレイヤー3レベルで相互に通信できるようにする。
* タグなしトラフィックをVLAN 5を使用するように設定します。
* VLAN 1の使用を無効にします。
これらの要件を満たす構成セットはどれですか？

A. SW1#interface Gi0/1switchport mode trunkswitchport trunk allowed vlan 5,7,9,108switchport trunk native vlan 5interface Gi0/2switchport mode trunkswitchport trunk allowed vlan 5,7,9,108 SW2#interface Gi0/1switchport mode accessswitchport access vlan 7interface Gi0/7switchport mode trunkswitchport trunk allowed vlan 7,9,108
B. SW1#interface Gi0/1switchport mode trunkswitchport trunk allowed vlan 5,7,9,108switchport trunk native vlan 5interface Gi0/2switchport mode accessswitchport trunk allowed vlan 7,9,108 SW2#interface Gi0/1switchport mode accessno switchport access vlan 1switchport access vlan
7インターフェースGi0/7スイッチポートモードトランクスイッチポートトランク許可VLAN 7、9、108スイッチポートトランクネイティブVLAN 5
C. SW#1 - interface Gi0/1 switchport mode trunks switchport trunk allowed vlan 5,7,9,108 switchport trunk native vlan 5 interface Gi0/2 switchport mode trunks switchport trunk allowed vlan 5,7,9,108 SW2# interface Gi0/1 switchport mode accesss switchport access vlan 7 interface Gi0/7 switchport mode trunks switchport trunk allowed vlan 5,7,9,108 switchport trunk native vlan 5
D. SW1#interface Gi0/1switchport mode trunkswitchport trunk allowed vian 5,7,9,108interface Gi0
/2switchport mode trunkswitchport trunk allowed vlan 7,9,108SW2#interface Gi0/1switchport mode trunkswitchport trunk allowed vlan 7interface Gi0/7switchport mode trunkswitchport trunk allowed vlan 5,7,9,108
正解: **C** (コメントを発表する)
SW#1 -interface Gi0/1switchport mode trunkswitchport trunk allowed vlan 5,7,9,108switchport trunk native vlan 5interface Gi0/2switchport mode trunkswitchport trunk allowed vlan 5,7,9,108SW2#interface Gi0/1switchport mode accessswitchport access vlan 7interface Gi0/7switchport mode trunkswitchport trunk allowed vlan 5,7,9,108switchport trunk native vlan 5. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco- consistent configuration or behavior for this wireless scenario.

質問: **405**



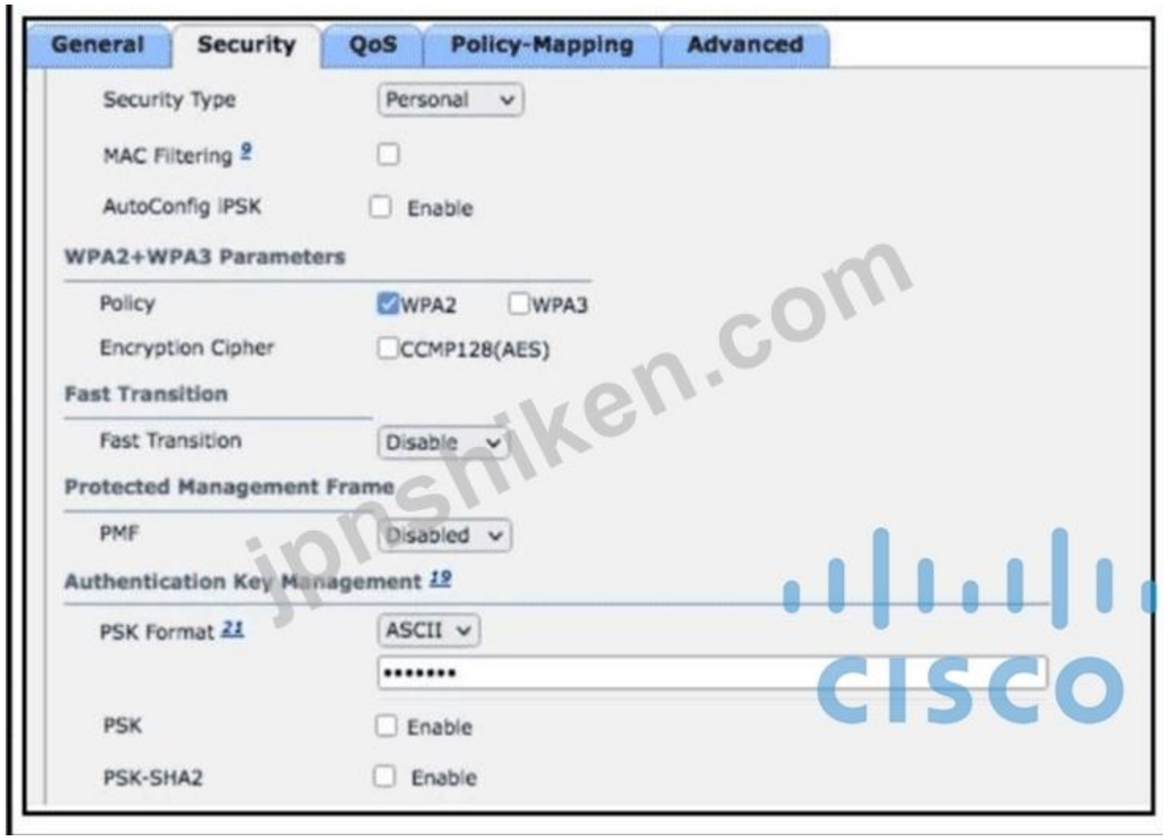
図を参照してください。プライマリリンクが故障した場合に、ルーターR1からR2上のLANネットワークへトラフィックを転送するために、セカンダリルートが必要です。ルーターを設定するには、どのコマンドを入力する必要がありますか？
A. ip route 10.0.2.0 255.255.255.240 10.0.0.7 92

B. ip route 10.0.2.0 255.255.255.248 10.0.0.6 91
C. ip route 10.0.2.0 256.255.255.240 10.0.0.6 91
D. ip route 10.0.2.0 255.255.255.248 null0 93
正解: **B** (コメントを発表する)
ip route 10.0.2.0 255.255.255.248 10.0.0.6 91. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **406**
Cisco IP Phone は、接続された PC からタグなしのデータ トラフィックを受信します。電話によって行われるアクションはどれですか?
A. トラフィックをそのまま通過させます
B. トラフィックをドロップします
C. デフォルトの VLAN でトラフィックにタグを付けます。
D. トラフィックをネイティブ VLAN でタグ付けします。
正解: **A** (コメントを発表する)
It allows the traffic to pass through unchanged. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **407**
展示資料を参照してください。



jpnshiken.com

ユーザーは事前に設定された秘密鍵とSSIDを使用し、安全な鍵ハッシュアルゴリズムが設定されている必要があります。AAAサーバーはユーザー認証方法に使用してはなりません。どの操作でタスクが完了しますか？

A. AutoConfig iPSK を有効にします。

B. SetCCMP128(AES)。

C. PSKフォーマットをキー文字列でHEX形式に設定します。

D. PSK-SHA2を設定します。

正解: **(**正解を表示します**)**

Configure PSK-SHA2.. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **408**

展示資料を参照してください。

ルーターR4は、サーバーへのパスを動的に学習しています。R4がOSPFエリア20を介してR1に接続され、R2のBGPを介してR2に接続され、EIGRP 777を介してR3に接続されている場合、R4のルーティングテーブルにはどのパスがインストールされますか？

A. R1 を経由するパス。OSPF の管理距離は 110 であるため。

B. R2 を経由するパス。IBGP 管理距離は 200 であるため。

C. EBGP管理距離が20であるため、R2を経由するパス

D. R3 を経由するパス。EIGRP の管理距離は OSPF および BGP よりも短いため。

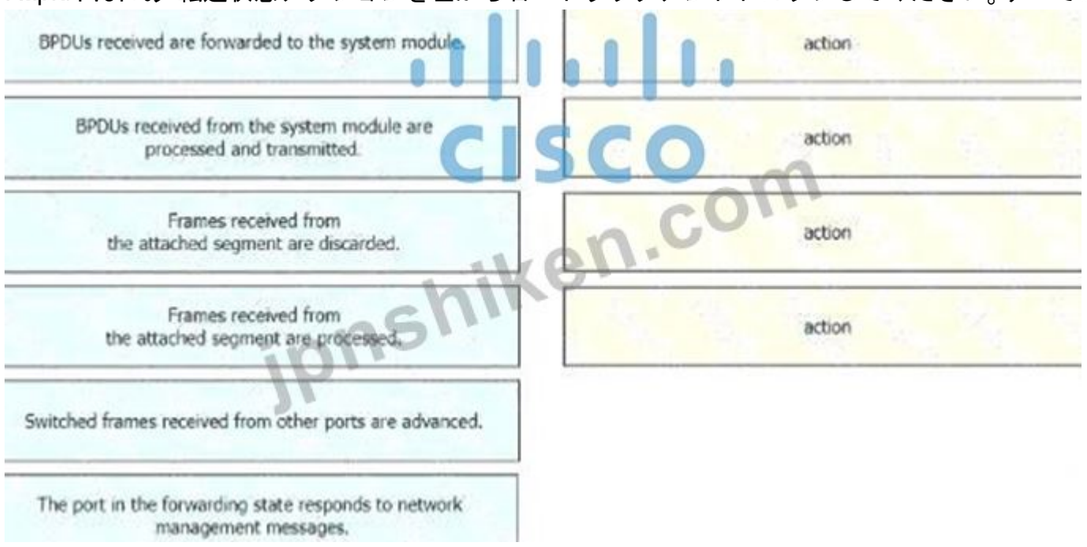
正解: (正解を表示します)

The verified answer is C. When identical prefixes are learned from different routing sources, the router compares administrative distance. eBGP has an administrative distance of 20, which is lower than EIGRP internal 90, OSPF 110, and iBGP 200. Cisco CCNA 200-301 v1.1 places this skill in IP Connectivity, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. The router installs the route with the lowest administrative distance unless more specific prefix matching changes the comparison. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise.

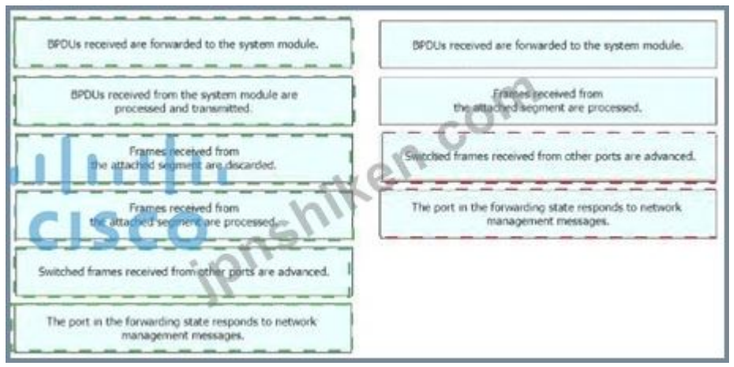
The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **409**

Rapid PVST+の 転送状態アクションを左から右へドラッグアンドドロップしてください。すべてのアクションを使用するわけではありません。



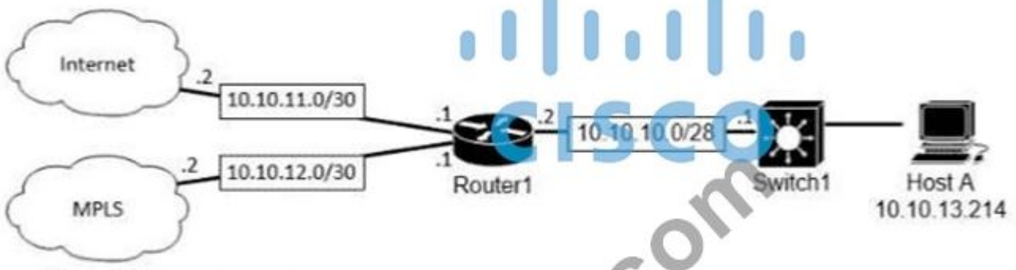
正解:



Explanation:
Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this type test whether each item is matched to the technology that actually performs that role. The reliable method is to classify each term by operating layer, packet behavior, management function, or security purpose before matching it. Several terms in these items are legitimate Cisco networking concepts, but they become wrong when assigned to the wrong protocol or plane. The mapping retained in the document follows that separation: transport behavior is matched to TCP or UDP, wireless or security terms are matched to their mechanisms, and automation items are matched to the correct API or management model. This matters operationally because troubleshooting fails quickly when a forwarding-plane function is treated as a management-plane feature or when a security control is applied to the wrong threat. The shown mapping is therefore retained as the verified response.

質問: **410**
エンジニアが、ローカル ルーターでドメイン名、ユーザー名、およびパスワードを構成しました。
Secure Shell アクセス RSA キーの構成を完了するための次のステップは何ですか?
A. 暗号鍵 Import rsa pem
B. 暗号鍵 pubkey-chain rsa
C. 暗号鍵生成 RSA
D. 暗号鍵ゼロ化 RSA
正解: (正解を表示します)
crypto key generate rsa. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **411**
展示資料を参照してください。




```
Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0

     209.165.200.0/27 is subnetted, 1 subnets
B       209.165.200.224 [20/0] via 10.10.12.2, 03:22:14
     209.165.201.0/27 is subnetted, 1 subnets
B       209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
     209.165.202.0/27 is subnetted, 1 subnets
B       209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
     10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C       10.10.10.0/28 is directly connected, GigabitEthernet0/0
C       10.10.11.0/30 is directly connected, FastEthernet2/0
C       10.10.12.0/30 is directly connected, GigabitEthernet0/1
O       10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O       10.10.13.128/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O       10.10.13.144/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O       10.10.13.160/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O       10.10.13.208/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.10.11.2
```

ルーター1はホストAへのトラフィックにどのプレフィックスを使用しますか？

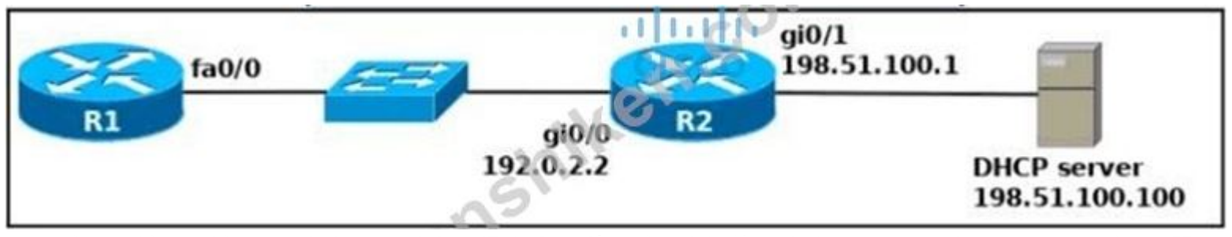
A. 10.10.10.0/28
B. 10.10.13.0/25
C. 10.10.13.144/28
D. 10.10.13.208/29

正解: **D (**コメントを発表する**)**

10.10.13.208/29. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under IP Connectivity, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **412**

展示資料を参照してください。



エンジニアが、R1がDHCPからIP構成を取得するトポロジーを構築します。スイッチとDHCPサーバーの設定が完了し、正しい場合、タスクを完了するためにR1とR2で設定する必要があるコマンドはどれですか？(2つ選択してください)

A. R1(config)# interface fa0/0R1(config-if)# ip helper-address 198.51.100.100

B. R2(config)# interface gi0/0R2(config-if)# ip helper-address 198.51.100.100

C. R1(config)# interface fa0/0R1(config-if)# ip address dhcpR1(config-if)# no shutdown

D. R2(config)# interface gi0/0R2(config-if)# ip address dhcp

E. R1(config)# interface fa0/0R1(config-if)# ip helper-address 192.0.2.2

正解: **(**正解を表示します**)**

Answer B,C is correct: B. R2(config)# interface gi0/0R2(config-if)# ip helper-address 198.51.100.100; C. R1 (config)# interface fa0/0R1(config-if)# ip address dhcpR1(config-if)# no shutdown. IP services questions test the exact function of infrastructure services such as addressing, name resolution, time synchronization, logging, monitoring, and secure management. Cisco CCNA 200-301 v1.1 includes this topic under IP Services, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The distractors name valid services, but they provide a different service function from the one required in the prompt. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **413**

展示資料を参照してください。

```
R1# show ip route

D    192.168.16.0/26 [90/2679326] via 192.168.1.1
R    192.168.16.0/24 [120/3] via 192.168.1.2
O    192.168.16.0/21 [110/2] via 192.168.1.3
i L1 192.168.16.0/27 [115/30] via 192.168.1.4
```

R1は、192.168.16.2宛てのトラフィックに対してどの経路を選択しますか？

A. 192.168.16.0/21

B. 192.168.16.0/24

C. 192.168.16.0/26

D. 192.168.16.0/27

正解: **(**正解を表示します**)**

192.168.16.0/27. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.

Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.

The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **414**
ドメイン ネーム サービス (DNS) の 2 つの役割は何ですか? (2つ選択)
A. より効率的な IP 操作のために、DNS 名のフラットな構造を構築します。
B. デフォルトで、WAN を通過するネットワーク トラフィックを暗号化します。
C. 完全修飾ドメイン名 (FQDN) で IP アドレスを保護することにより、セキュリティを向上させます。
D. アプリケーションが IP アドレスではなく名前でリソースを識別できるようにします。
E. 1 つのホスト名を複数の IP アドレスで共有できます。
正解: **D,E (コメントを発表する)**
DNS lets applications use names instead of forcing users and software to work directly with IP addresses. A client can ask for the address associated with a hostname, and DNS returns the resource records needed to reach that service. DNS can also map one name to multiple IP addresses, which supports simple distribution, redundancy, or service design depending on the record type and client behavior. It does not encrypt WAN traffic by default, and it does not secure IP addresses merely by hiding them behind fully qualified domain names. DNS is hierarchical, not flat, which is why the root, top-level domains, authoritative zones, and host records can scale globally. Cisco CCNA 200-301 v1.1 covers DNS under IP Services because name resolution is required for many network operations, including management access, web services, and application connectivity. The two valid roles here are enabling applications to identify resources by name and allowing a hostname to be associated with more than one IP address.

質問: **415**
ネットワークエンジニアが、認証サーバーの設定と動的インターフェースの作成によって、新しい無線LANの実装を開始します。基本設定を完了するために、次に何をする必要がありますか？
A. 新しい WLAN を作成し、動的インターフェースをそれにバインドします。
B. 管理インターフェースをインストールし、管理IPを追加します。
C. 管理インターフェースでTelnetおよびRADIUSアクセスを有効にします。
D. アクセスポイントの高可用性と冗長性を設定します。
正解: **A (コメントを発表する)**
Create the new WLAN and bind the dynamic interface to it.. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco- consistent configuration or behavior for this wireless scenario.

質問: **416**
共有リンク上の2つのルーター間の接続を提供するために使用されるIPv6アドレスはどれですか？(2つ選択してください)
A. ::ffff:1014:1011/96
B. 2001:701:1046:1111::1/64
C. ;jff06bb43cd4dd111bbff02 4545234d
D. 2002:5121:204b:1111::1/64
E. FF02::0WIFF00:0l)00/104
正解: **(正解を表示します)**
Answer B,D is correct: B. 2001:701:1046:1111::1/64; D. 2002:5121:204b:1111::1/64. For router-to-router IPv6 connectivity on a shared link, each router needs a usable unicast IPv6 address in the same link prefix.
The global unicast-looking addresses in options B and D are the valid choices for that purpose. Multicast addresses such as FF02-based addresses identify groups, not individual router interfaces for normal source

/destination connectivity. IPv4-mapped or malformed addresses do not meet the requirement. Cisco CCNA 200-301 v1.1 Network Fundamentals expects engineers to distinguish unicast, multicast, link-local, and special IPv6 address forms. A shared link between routers can use link-local addresses for some control-plane protocols, but for the addressing choices shown here, the usable unicast interface addresses are the correct selections. The corrected answer is B and D because those addresses can be assigned to router interfaces to support communication across the link.

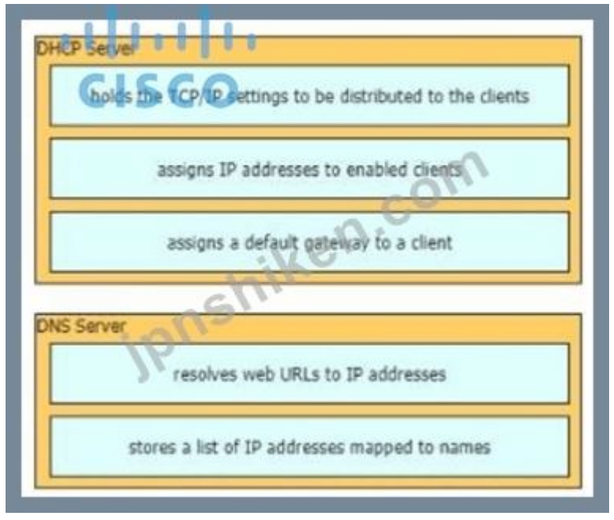
質問: **417**
Cisco WLCへのHTTPアクセスを有効にするコマンドはどれですか？
A. config network secureweb enable
B. 設定証明書生成ウェブ管理
C. config network webmode enable
D. config network telnet enable
正解: **(正解を表示します)**
config network webmode enable. Wireless questions depend on AP mode, WLAN security, RF band selection, controller interfaces, and client roaming or authentication behavior. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong options confuse encryption with authentication, local switching with tunneling, or controller management with client data handling. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco- consistent behavior for this item.

質問: **418**
左側の関数を右側の適切なネットワークコンポーネントにドラッグアンドドロップしてください。

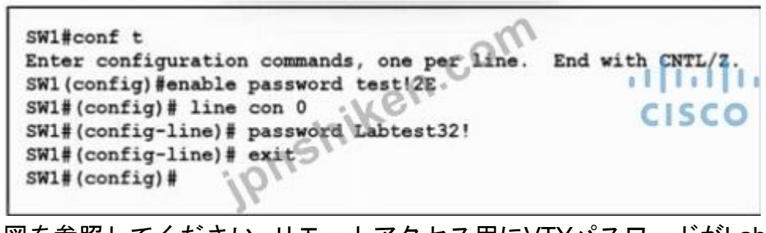
正解:

Explanation:

This matching item tests the basic roles of common network components. A router forwards packets between IP networks and makes Layer 3 path decisions. A Layer 2 switch forwards Ethernet frames within a VLAN using MAC addresses. A Layer 3 switch can perform switching and inter-VLAN routing in hardware. A firewall controls traffic between security zones and may use stateful inspection, policy, and address translation. A wireless access point bridges wireless clients into the wired network, while a wireless LAN controller centrally manages many lightweight APs. Cisco CCNA v1.1 Network Fundamentals begins with exactly this skill: explain the role and function of routers, switches, APs, controllers, servers, endpoints, and security appliances. The reliable way to solve the drag-and-drop is to identify the forwarding layer and administrative role. MAC-frame movement belongs to Layer 2 switching, subnet-to-subnet forwarding belongs to routing, and centralized WLAN control belongs to the WLC.



質問: **419**



図を参照してください。リモートアクセス用にVTYパスワードがLabtest32!に設定されています。SSHアクセスのみを許可し、実行中の設定でパスワードを非表示にするには、どのコマンドが必要ですか？

A. SW1#(config-line)#login local SW1#(config-line)#exit SW1(config)#crypto key generate rsa

B. SW1#(config-line)#login local SW1#(config-line)#exit SW1(config)#enable secret test!2E

C. SW1#(config-line)#transport input ssh SW1#(config-line)#exit SW1(config)#service password- encryption
D. SW1#(config-line)#exit SW1(config)#aaa new-model
正解: (正解を表示します)
SW1#(config-line)#transport input ssh SW1#(config-line)#exit SW1(config)#service password-encryption.
IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **420**
展示資料を参照してください。

エンジニアがスイッチ1とスイッチ2の間でLACPを使用したEtherChannelを設定しています。スイッチ1のみがLACP開始パケットを送信するようにするには、どの設定を適用する必要がありますか？
A. スイッチ 1 (config-if)#channel-group 1 mode onSwrtch2(config-if)#channel-group 1 mode passive
B. Switch1(config-if)#channel-group 1 mode passiveSwitch2(config-if)#channel-group 1 mode active
C. Switch1{config-if)#channel-group 1 mode activeSwitch2(config-if)#channel-group 1 mode passive
D. Switch1(config-if)#channel-group 1 mode onSwitch2(config-if)#channel-group 1 mode active
正解: (正解を表示します)
Switch1{config-if)#channel-group 1 mode activeSwitch2(config-if)#channel-group 1 mode passive.
Switching behavior depends on VLAN tagging, trunk negotiation, STP role selection, EtherChannel mode, and whether a protocol is standards-based or Cisco-specific. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. Incorrect options change existing VLAN reachability, use the wrong negotiation behavior, or apply a feature to the wrong switch function. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem.
The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

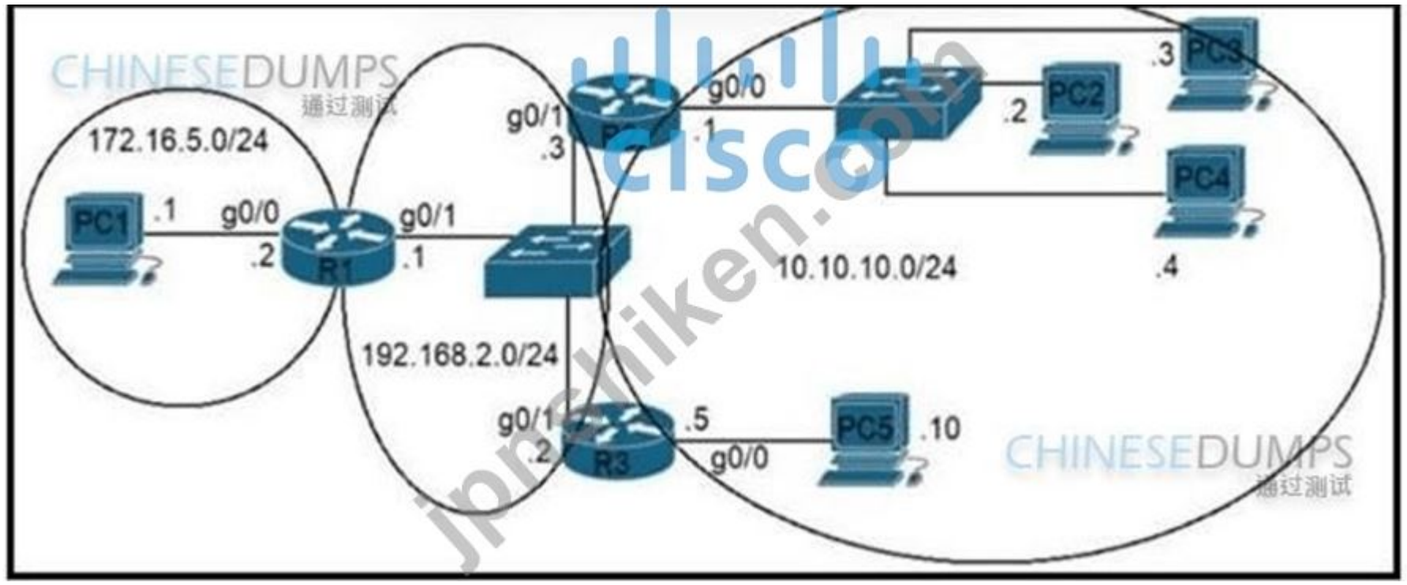
質問: **421**
インターフェースの回線プロトコルのアップ/ダウンイベントを表示するsyslogメッセージログレベルはどれですか？
A. 情報提供

B. デバッグ
C. アラート
D. 通知
正解: **(**正解を表示します**)**
notifications. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **422**
PCのアドレス10.1.1.1をパブリックルーティング可能なアドレスに静的NATバインディングするコマンドはどれですか？
PCに割り当てられたIPアドレスは209.165.200.225ですか？
A. R1(config)#ip nat inside source static 10.1.1.1 209.165.200.225
B. R1(config)#ip nat inside source static 209.165.200.225 10.1.1.1
C. R1(config)#ip nat outside source static 10.1.1.1 209.165.200.225
D. R1(config)#ip nat outside source static 209.165.200.225 10.1.1.1
正解: **A (**コメントを発表する**)**
R1(config)#ip nat inside source static 10.1.1.1 209.165.200.225. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **423**



図を参照してください。ルータR1は現在設定中です。ルータR2とR3は新しい環境に合わせて正しく設定されています。PC1が10.10.10.0/24ネットワーク上のすべてのPCと通信できるようにするには、R1でどの2つのコマンドを設定する必要がありますか？(2つ選択してください。)

A. ip route 10.10.10.0 255.255.255.0 192.168.2.3

B. ip route 10.10.10.10 255.255.255.255 192.168.2.2

C. ip route 10.10.10.10 255.255.255.255 g0/1

D. ip route 10.10.10.8 255.255.255.248 g0/1

E. ip route 10.10.10.0 255.255.255.248 192.168.2.2

正解: **(**正解を表示します**)**

Answer A,E is correct: A. ip route 10.10.10.0 255.255.255.0 192.168.2.3; E. ip route 10.10.10.0 255.255.255.248 192.168.2.2. Routing questions are solved by applying longest-prefix match, administrative distance, metric, and protocol-specific behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Wrong answers either use the wrong prefix, the wrong next hop, or a route source that would not be preferred. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **424**

左側のネットワークプロトコルを、右側の適切なトランスポートサービスにドラッグアンドドロップしてください。

正解:

Explanation:

This drag-and-drop question tests whether the protocol normally uses TCP or UDP as its transport service.

TCP is selected when the application requires connection setup, acknowledgments, sequencing, and retransmission. Protocols such as HTTP, HTTPS, FTP, SSH, Telnet, and SMTP commonly rely on TCP because reliable delivery matters more than minimal overhead. UDP is selected when the application benefits from low overhead, simple request/response behavior, or real-time delivery where late retransmission is not useful. DNS queries, DHCP, TFTP, SNMP polling, NTP, voice media, and many streaming functions commonly use UDP. Some protocols can use both in special cases, but CCNA questions normally expect the standard default transport. Cisco CCNA v1.1 Network Fundamentals includes application protocols and transport-layer behavior. The correct mapping should therefore follow function: reliable session-based applications go to TCP, while lightweight discovery, timing, addressing, and real-time-style exchanges usually go to UDP.

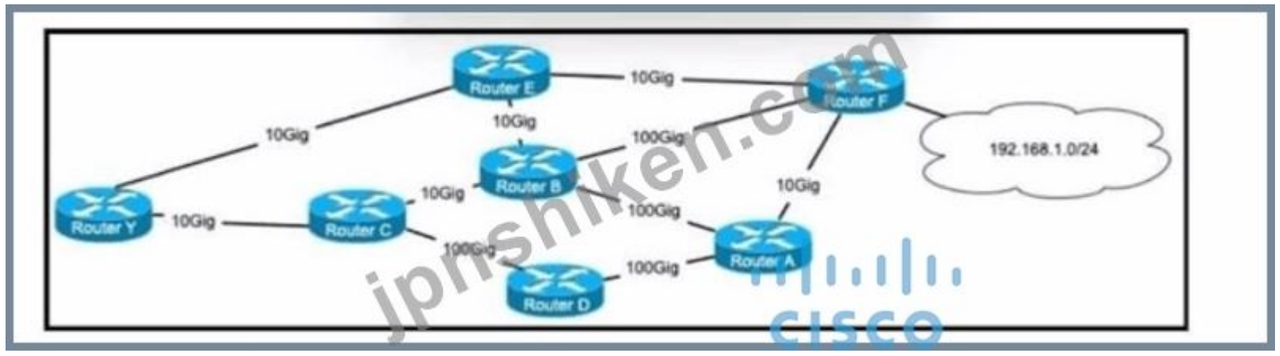
質問: **425**
エンドホストに接続されたスイッチポートでPortFastを設定する2つの理由は何ですか？(2つ選択してください。)
A. ポートで学習した MAC アドレスの数を I に有効にする
B. ポートの動作をトポロジー変更プロセスから保護するため
C. ホストの起動時にポッドがすぐに転送状態に入るようにする
D. ポートがスパニングツリープロトコル操作に参加しないようにする
E. 他のスイッチまたはホストがポートを介して通信するのをブロックする
正解: (正解を表示します)
Answer B,C is correct: B. to protect the operation of the port from topology change processes; C. to enable the pod to enter the forwarding state immediately when the host boots up. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation.
Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol:
LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **426**
信頼性が最も高い WAN トポロジはどれですか?
A. フルメッシュ
B. ポイントツーポイント
C. ハブアンドスポーク
D. スティック上のルーター
正解: (正解を表示します)
full mesh. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong

option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **427**
分割型MACアーキテクチャでは、リアルタイム制御機能はどこで処理されるのでしょうか？
A. 集中型クラウド管理プラットフォーム
B. 中央WLC
C. 個別AP
D. クライアントデバイス
正解: **C (**コメントを発表する**)**
Individual AP. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **428**



図を参照してください。すべてのルーターの基準帯域幅が100Gbの場合、ルーターYはネットワーク192.168.1.0/24に到達するためにどの経路を使用しますか？
A. ルーター C > D > A > B > F
B. ルーター C > D > A > F
C. ルーター E > F
D. ルーター E > B > F
正解: **(**正解を表示します**)**
router C > D > A > B > F. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First- hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

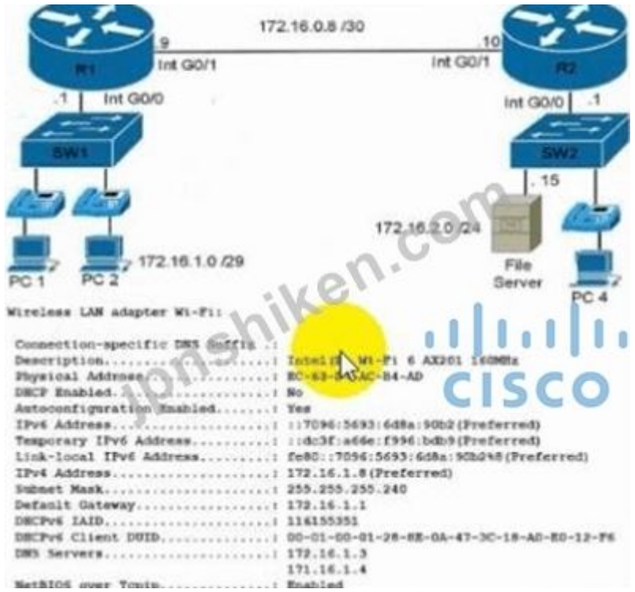
質問: **429**

ネットワーク管理操作における FTP の機能は何ですか?
A. データ リソース間で送信する前にデータを暗号化します。
B. デバイスは直接接続され、UDP を使用してファイル情報を渡します
C. 個別の制御接続とデータ接続を使用して、サーバーとクライアント間でファイルを移動します
D. データ転送時にセッション層で独自のサポートを提供
正解: (正解を表示します)
uses separate control and data connections to move files between server and client. Infrastructure services must be identified by their exact function: monitoring, time, address assignment, file transfer, logging, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under IP Services, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The distractors name real services, but those services do not perform the action requested in the prompt. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **430**
ルーター上で service password-encryption コマンドを入力しました。この設定の効果は何ですか？
A. 実行中の設定ファイル内の平文パスワードを、権限のないユーザーが閲覧することを制限します。
B. VPNトンネル確立時にパスワード交換を暗号化します
C. ネットワーク管理者が平文パスワードを設定できないようにします
D. スイッチ上の不正なPC接続からVLANデータベースを保護します
正解: (正解を表示します)
restricts unauthorized users from viewing clear-text passwords in the running configuration. Automation questions require separating controller roles, API direction, data formats, HTTP behavior, and configuration- management tooling. Cisco CCNA 200-301 v1.1 includes this topic under Security Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario.
The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The incorrect options mix northbound and southbound communication, confuse data serialization with transport, or describe traditional device-by-device management. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **431**
インターフェースのMACアドレスから派生したグローバルユニキャストIPv6アドレスをインターフェースに割り当てるには、どのような操作を行う必要がありますか？
A. ネットワーク上にステートフルなDHCPv6サーバーを設定する
B. インターフェースでSLAACを有効にする
C. EUI-64ビットプロセスを無効化する
D. リンクローカルアドレスを明示的に割り当てる
正解: (正解を表示します)
enable SLAAC on an interface. To derive a global unicast IPv6 address from the interface MAC address, the device must use SLAAC or an explicit EUI-64-based IPv6 configuration. SLAAC receives the IPv6 prefix from router advertisements and builds the interface identifier from the local interface value, historically using the modified EUI-64 process. Stateful DHCPv6 can assign IPv6 addresses, but that does not specifically create the address from the interface MAC address. Disabling EUI-64 would do the opposite of the requirement, and a link-local address is not the requested global unicast address. Cisco CCNA 200-301 v1.1 Network Fundamentals covers this because IPv6 address assignment is a core operational skill. The clue is ' derived from the MAC address. ' That points to SLAAC/EUI-64 behavior, not a DHCPv6 server-created address. The correct action is to enable SLAAC on the interface or use the equivalent EUI-64 address- generation method.

質問: **432**



図を参照してください。初期構成テスト中に、WindowsワークステーションPC1は172.16.2.0/24ネットワークに接続できません。
どの操作で設定が修正されますか？

A. IPアドレスを172.16.1.6に変更し、サブネットマスクを255.255.255.248に変更します。
B. IPアドレスを172.16.1.6に変更し、DNSサーバーを172.16.1.12と172.16.1.13に変更します。
C. IPアドレスを172.16.1.9に変更し、デフォルトゲートウェイを172.16.1.7に変更します。
D. IPアドレスを172.16.1.9に変更し、DNSサーバーを172.16.1.12のみに変更します。
正解: (正解を表示します)

Change the IP addressss to 172.16.1.6 and change the subnet mask to 255.255.255.248.. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **433**

従業員のグループが1人だけのIDバッジを使用して建物に入ると、どのタイプのセキュリティプログラムに違反しますか？

A. 侵入検知
B. ユーザーの認識
C. 物理的アクセス制御
D. ネットワーク認証
正解: (正解を表示します)

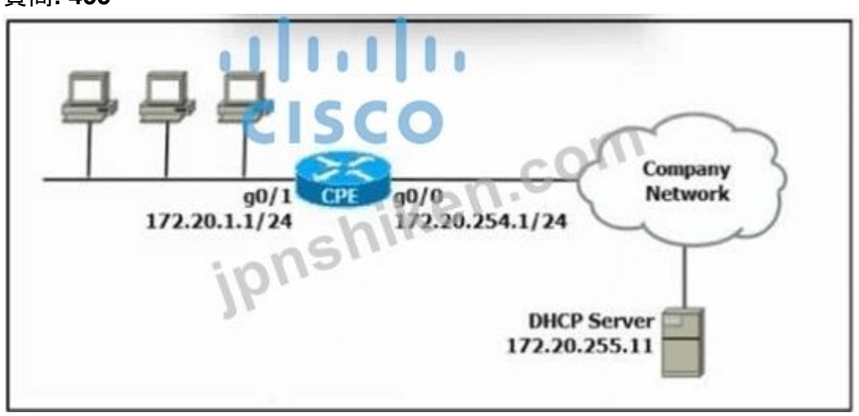
Use C for this item. Using one badge to let multiple employees enter a building is a physical access control violation. Badge readers, locks, turnstiles, guards, and visitor procedures are meant to identify and authorize each person entering a protected facility. In Cisco CCNA 200-301 v1.1, Security Fundamentals questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. Network authorization and intrusion detection are logical controls, and user awareness is training rather than the violated access-control mechanism itself.

A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **434**
展示資料を参照してください。

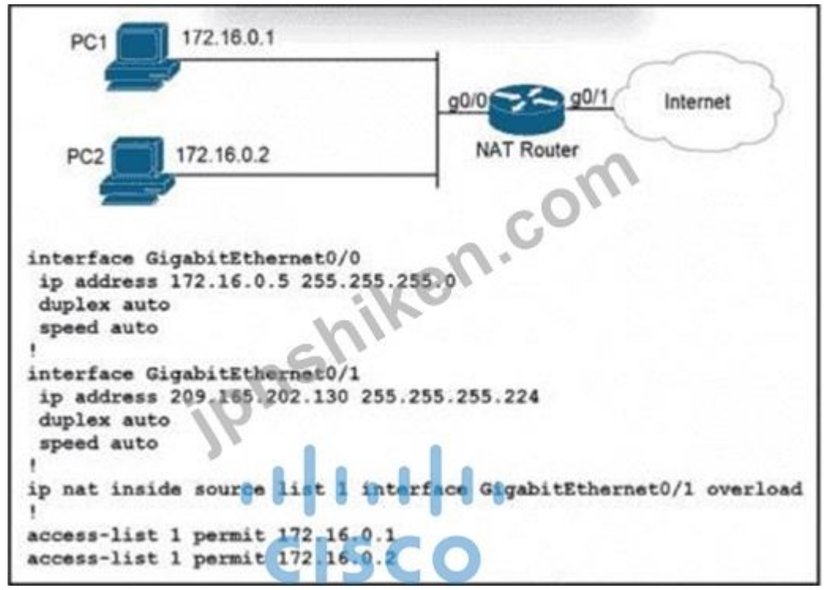
LDAPのドメイン認証情報を使用して最高レベルの暗号化と認証を実現するために、エンジニアが取るべき2つの手順は何ですか？
A. 認証キー管理でPSKを選択します。
B. レイヤー2セキュリティでWPA+WPA2を選択してください
C. レイヤ2セキュリティでStatic-WEP + 802.1Xを選択
D. TKIP暗号化を使用したWPAポリシーを選択します
E. 認証キー管理の下から 802.1X を選択します。
正解: **B,E (**コメントを発表する**)**
Answer B,E is correct: B. Select WPA+WPA2 on Layer 2 Security; E. Select 802.1X from under Authentication Key Management. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **435**



図を参照してください。ネットワークエンジニアは、172.20.1.0 のコンピュータが CPE ルーターに接続できるように設定する必要があります。
/24 ネットワークを使用して、中央の DHCP サーバーから IP 設定を取得します。エンジニアは CPE にどの設定を適用する必要がありますか？
A. インターフェース GigabitEthernet0/1 ip ヘルパーアドレス 172.20.254.1
B. インターフェース GigabitEthernet0/0ip ヘルパーアドレス 172.20.1.1
C. インターフェース GigabitEthernet0/0ip ヘルパーアドレス 172.20.255.1
D. インターフェース GigabitEthernet0/ip ヘルパーアドレス 172.20.255.11
正解: **(**正解を表示します**)**
interface GigabitEthernet0/1ip helper-addresss 172.20.254.1. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **436**



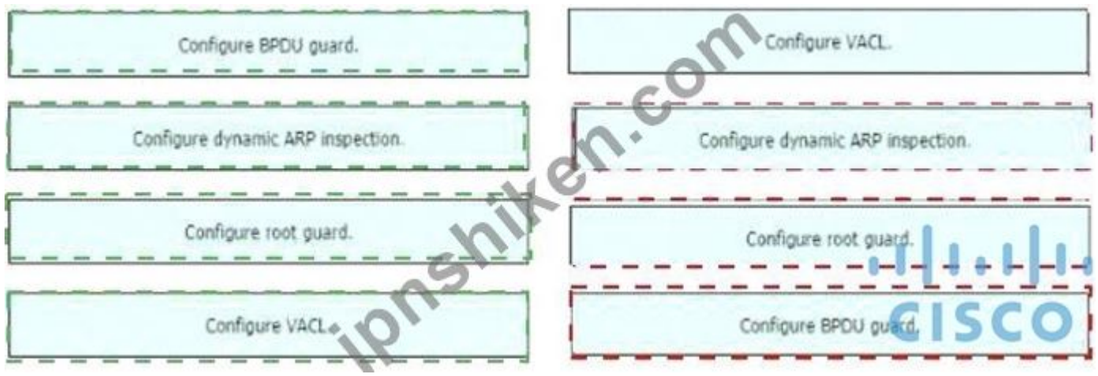
図を参照してください。PC1とPC2がインターネットにアクセスできるようにするには、設定をどのように更新すればよいでしょうか？
A. ip nat inside source コマンドをインターフェース GigabitEthernet0/0 を使用するように変更します。
B. ip nat inside source コマンドから overload キーワードを削除します。
C. 2 番目のアクセス リストの設定番号を変更します。
D. 両方のインターフェースに ip nat inside コマンドと ip nat outside コマンドを追加します。
正解: **(**正解を表示します**)**
Change the ip nat inside source command to use interface GigabitEthernet0/0.. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these

items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

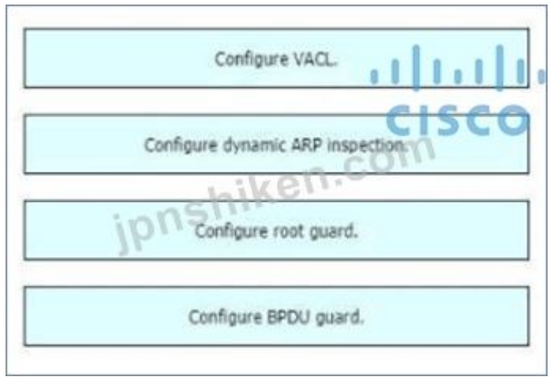
有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **437**
左側の脅威軽減策を、右側のそれらが軽減する脅威または攻撃の種類にドラッグ＆ドロップしてください。

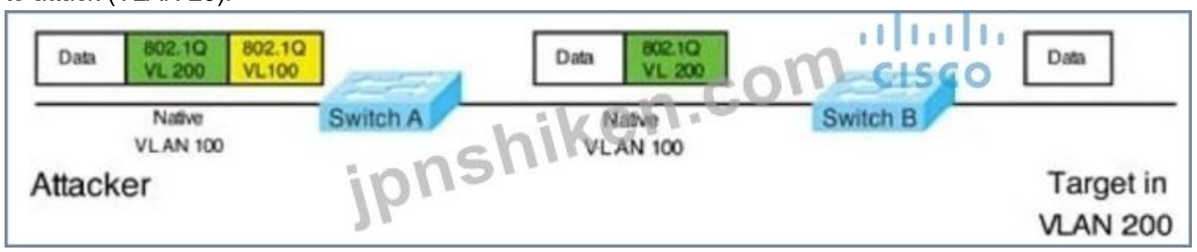
正解:



Explanation:
The matching is based on identifying the attack layer and then choosing the control that blocks that behavior.
Dynamic ARP Inspection validates ARP messages against trusted bindings and is used against ARP spoofing or poisoning, a common man-in-the-middle technique on Layer 2 segments. DHCP snooping builds the trusted binding table and blocks unauthorized DHCP server behavior. Port security limits which MAC addresses can use a switchport, reducing exposure to MAC flooding or unauthorized endpoint attachment.
Changing the native VLAN or using proper trunk controls helps mitigate VLAN hopping and double-tagging attacks, because the attacker relies on trunk/native VLAN behavior to cross VLAN boundaries. Cisco CCNA v1.1 Network Access includes switch security features such as DHCP snooping, DAI, and port security. The practical approach is not to memorize coordinates in a drag-and-drop map. Identify the malicious mechanism first, then map it to the feature that checks or constrains that exact mechanism.



In this attack, the attacking computer generates frames with two 802.1Q tags. The first tag matches the native VLAN of the trunk port (VLAN 10 in this case), and the second matches the VLAN of a host it wants to attack (VLAN 20).



質問: 438

図を参照してください。管理者は、SW_1とプリンタをネットワークに接続する必要があります。SW_2は、SW_1への接続にDTPを使用する必要があります。プリンタは、VLAN 5のアクセスポートとして構成されています。どのコマンドセットで接続が完了しますか？

A. switchport mode dynamic autoswitchport private-vlan association host 5

B. スイッチポートモードダイナミック、オートスイッチポートトランクカプセル化ネゴシエート

C. switchport mode dynamic desirableswitchport trunk allowed vlan add 5

D. switchport mode trunkswitchport trunk pruning vlan add 5

正解: (正解を表示します)

switchport mode dynamic desirableswitchport trunk allowed vlan add 5. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol:

LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **439**
ネットワーク自動化の必要性をサポートする主な要因はどれですか？ 2つ選んでください。）
A. トレーニングの必要性をなくす
B. 自己診断と自己修復への依存度が高まる
C. ポリシーに基づくリソースのプロビジョニング
D. リソース プロビジョニングのための船のエントリ ポイントを提供する
E. ハードウェア フットプリントの削減
正解: **(正解を表示します)**
Answer C,D is correct: C. Policy-derived provisioning of resources; D. Providing a ship entry point for resource provisioning. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Automation and Programmability, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

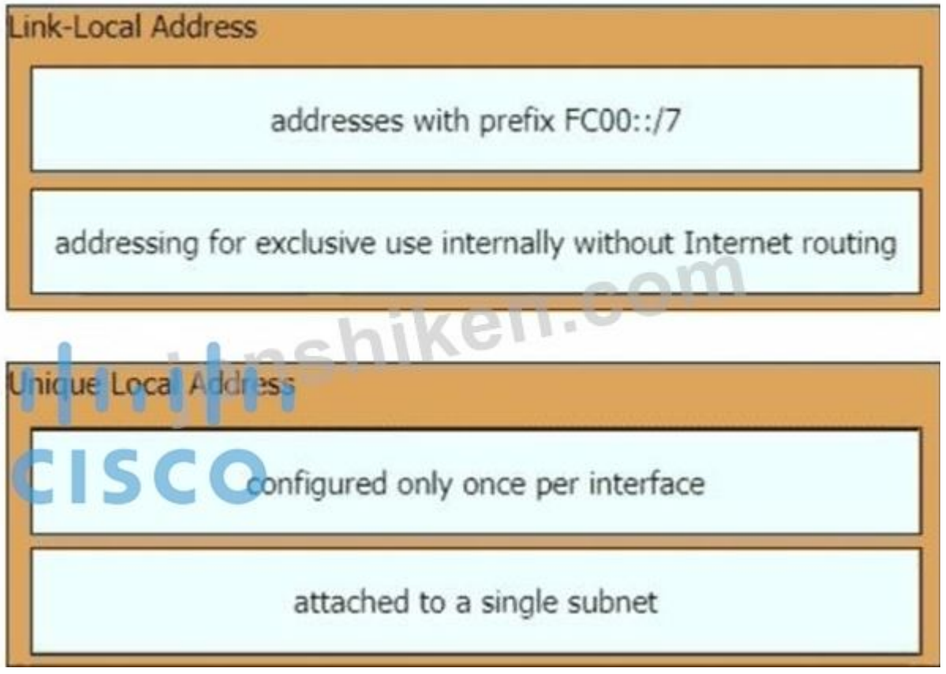
質問: **440**
IPv6アドレスタイプの特性を左側から右側へドラッグアンドドロップしてください。

jpnshiken.com

正解:

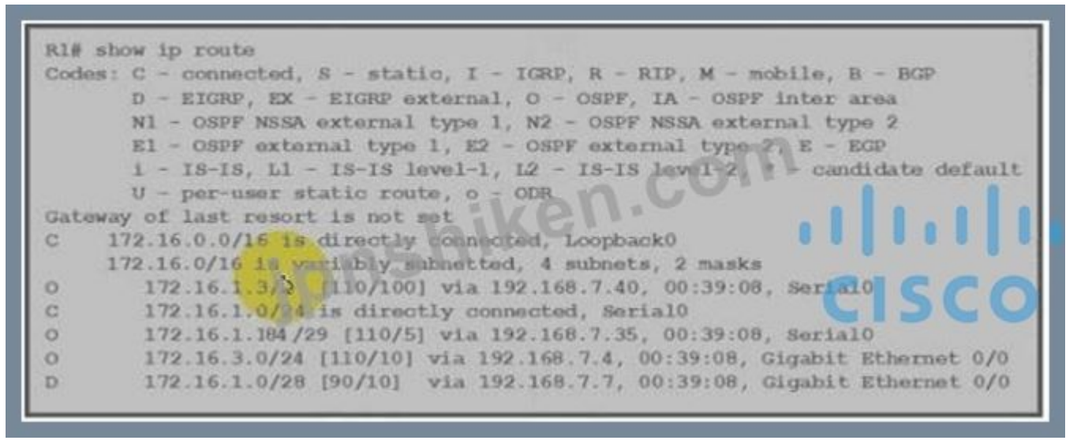
Explanation:

The verified answer is the displayed drag-and-drop mapping. IPv6 address types are identified by prefix and scope. Global unicast is Internet-routable, unique local is private-like, link-local stays on the local link, and multicast reaches a group. Cisco CCNA 200-301 v1.1 places this skill in Network Fundamentals, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. Correct mapping depends on recognizing prefix ranges such as 2000::/3, FC00::/7, FE80::/10, and FF00::/8. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.



質問: 441

展示資料を参照してください。



WANから172.16.1.190のホスト宛ての負荷分散されたトラフィックが流入しています。ルーターはリクエストを転送するためにどのネクストホップを使用しますか？

A. 192.168.7.4

B. 192.168.7.7

C. 192.168.7.35

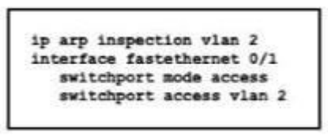
D. 192.168.7.40

正解: **B (**コメントを発表する**)**

192.168.7.7. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **442**

展示資料を参照してください。



この設定による影響は何ですか？

A. スイッチポートインターフェースの信頼状態が信頼不能になります

B. スイッチポートは、インターフェースが別のスイッチに接続されるまで、管理上ダウン状態のままです。

C. ARP ACL が存在しないため、動的 ARP インスペクションは無効になっています

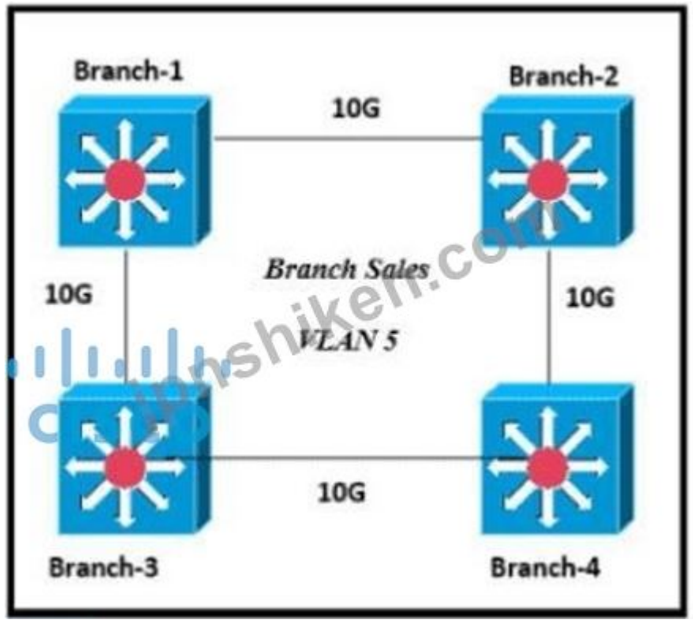
D. スイッチポートは、受信パケットを信頼するか信頼しないかが設定されるまでダウンしたままになります。

正解: **(**正解を表示します**)**

The switch port interface trust state becomes untrusted. The answer follows directly from normal Cisco device behavior and the wording of the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym.

The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **443**
展示資料を参照してください。



VLANスパニングツリー処理に参加しているスイッチは4台のみです。
ブランチ1優先度614440
ブランチ2：優先度9082416
ブランチ3：優先度
ブランチ4 :ルートプライマリ
どのスイッチがVLAN 5の永続的なルートブリッジになりますか？

A. ブランチ-1
B. ブランチ2
C. ブランチ3
D. ブランチ4

正解: **(**正解を表示します**)**

Branch-3. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **444**
展示資料を参照してください。

ルーターR1がネットワークに追加され、10.0.0.64/26と10.0.20.0/24のサブネットが設定されました。しかし、R3上のLAN宛てのトラフィックにアクセスできません。R1で実行すると、R3のLANに到達するための静的ルートを定義するコマンドはどれですか？

A. ip route 10.0.15.0 255.255.255.0 10.0.20.3
B. ip route 10.0.15.0 255.255.255.0 10.0.20.1
C. ip route 10.0.0.64 255.255.255.192 10.0.20.3
D. ip route 10.0.15.0 255.255.255.192 10.0.20.1

正解: **A** (コメントを発表する)

ip route 10.0.15.0 255.255.255.0 10.0.20.3. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **445**
展示資料を参照してください。

エンジニアは、既存のトランクに新しい VLAN を挿入するように求められましたが、以前に設定された内容は何も変更しません。このタスクを実行するコマンドはどれですか？

A. switchport trunk allowed vlan 100-104

B. switchport trunk allowed vlan add 104

C. switchport trunk allowed vlan all

D. switchport trunk allowed vlan 104

正解: **(**正解を表示します**)**

switchport trunk allowed vlan add 104. The keyword add appends a VLAN to the existing allowed VLAN list without replacing the current list. That is the critical detail in the prompt: the engineer must insert the new VLAN without modifying anything previously configured. A command that specifies only VLAN 104 replaces the existing allowed list with VLAN 104, which can interrupt traffic for existing VLANs. The all option allows every VLAN and changes the policy more broadly than requested. Cisco CCNA 200-301 v1.1 Network Access expects engineers to understand the operational difference between setting a trunk allowed list and adding to it. On production trunks, using the wrong command can remove active VLANs and create an outage. The safe command is switchport trunk allowed vlan add 104.

質問: **446**

エンジニアは、2台のルーター間に/30サブネットを構成する必要があります。この条件を満たす使用可能なIPアドレスとサブネットマスクの組み合わせはどれですか？

```
interface e0/0
description to HQ-A371:19452
ip address 209.165.201.2 255.255.255.252

interface e0/0
description to HQ-A371:19452
ip address 10.2.1.3 255.255.255.252

interface e0/0
description to HQ-A371:19452
ip address 172.16.1.4 255.255.255.248

interface e0/0
description to HQ-A371:19452
ip address 192.168.1.1 255.255.255.248
```

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: **(**正解を表示します**)**

A /30 IPv4 subnet provides four total addresses: one network address, two usable host addresses, and one broadcast address. That makes it a traditional fit for a point-to-point link between two routers, where only two interface addresses are required. The subnet mask for /30 is 255.255.255.252. The correct option must therefore contain a usable host address that falls between the subnet ' s network and broadcast

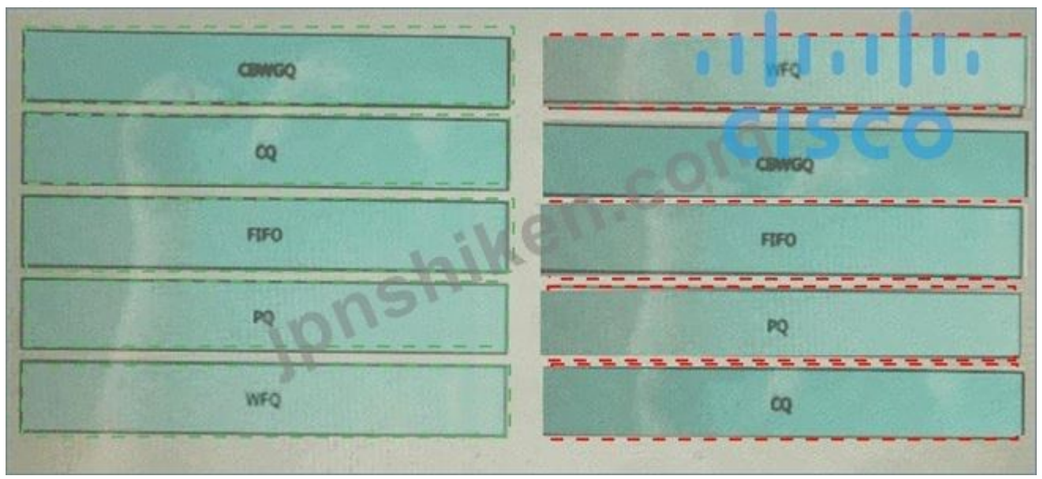
values, paired with the /30 mask. Option A is the combination that satisfies those conditions in the exhibit. Addresses equal to the subnet ID or broadcast address cannot be assigned to router interfaces. Masks that create a larger or smaller subnet do not meet the stated requirement. CCNA v1.1 Network Fundamentals expects fast recognition of subnet size, usable host ranges, and valid interface assignments. The efficient mental check is:
/30 increments by 4, and only the two middle addresses in each block are usable.

質問: **447**
サーバーは仮想環境でネットワークにどのように接続しますか?
A. ネットワークに物理的に接続されているアクセス ポイントへのワイヤレス
B. ネットワーク上の物理スイッチに接続されたケーブル
C. ネットワークに物理的に接続されたアクセス ポイントにリンクする仮想スイッチ
D. ネットワークに物理的に接続されているハイパーバイザー上のソフトウェア スイッチ
正解: **(**正解を表示します**)**
The verified answer is D. In a virtualized server environment, virtual machines connect through a software switch provided by the hypervisor. The hypervisor uplinks that virtual switch to the physical network through one or more physical NICs on the host server. Cisco CCNA 200-301 v1.1 places this skill in Network Fundamentals, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. VMs do not normally connect wirelessly, and they are not each cabled directly to a physical switch. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **448**
スイッチはフレームを転送する際に、CAMテーブル内で何を検索するのでしょうか？
A. 送信元MACアドレスと経過時間
B. 宛先MACアドレスとフラッシュ時間
C. 送信元MACアドレスと送信元ポート
D. 宛先MACアドレスと宛先ポート
正解: **D (**コメントを発表する**)**
destination MAC addresss and destination port. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity.
The selected answer matches Cisco switching operation.

質問: **449**
左側のQoS輻輳管理用語を、右側の説明文にドラッグ＆ドロップしてください。

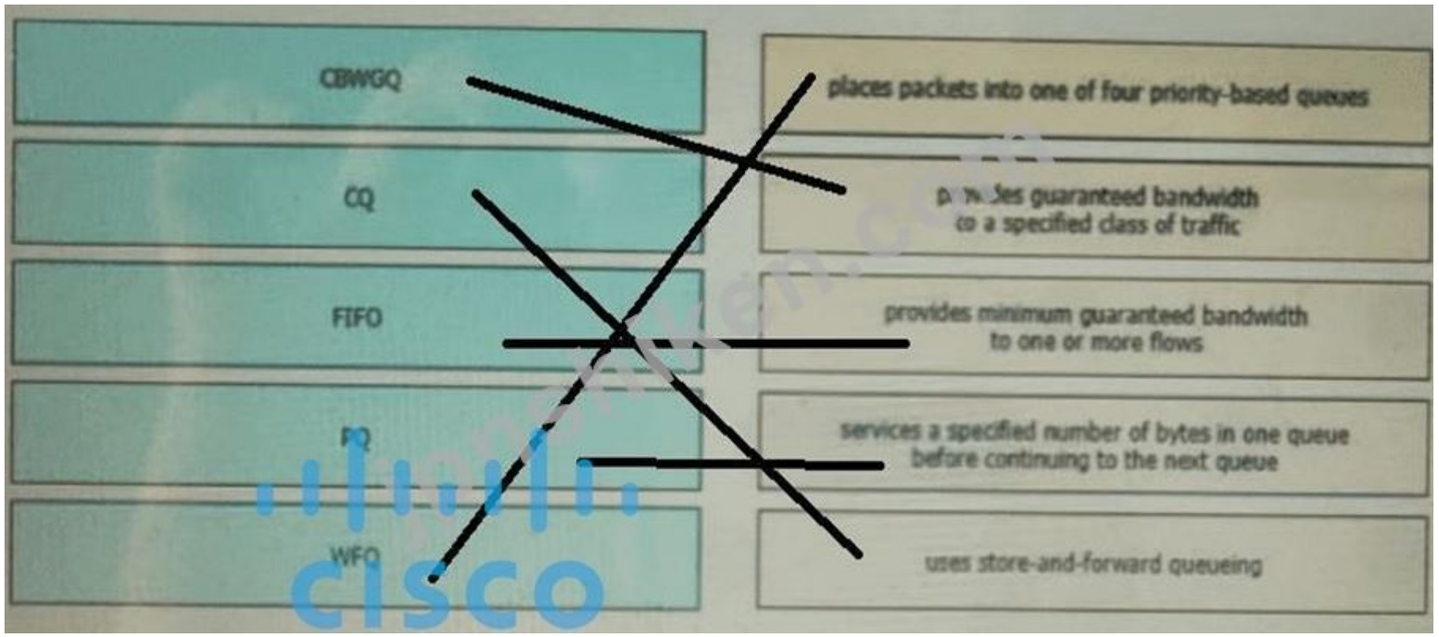
正解:



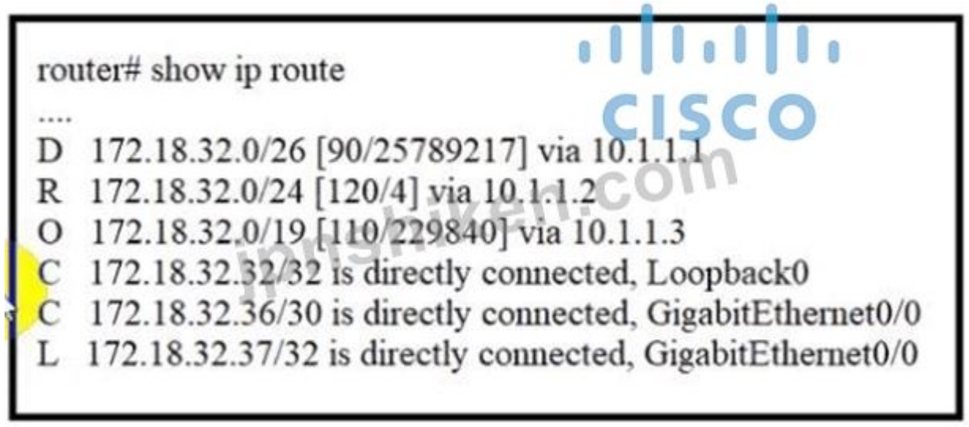
Explanation:

The verified answer is the displayed drag-and-drop mapping. QoS congestion management controls how packets are queued and scheduled when an interface is congested. Terms such as FIFO, priority queuing, weighted fair queuing, class-based WFQ, and low-latency queuing describe different ways to decide which packets leave first. Cisco CCNA 200-301 v1.1 places this skill in IP Services, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command.

Congestion avoidance, classification, and marking are related QoS functions, but they are not the same as queue scheduling during congestion. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.



質問: 450
展示資料を参照してください。



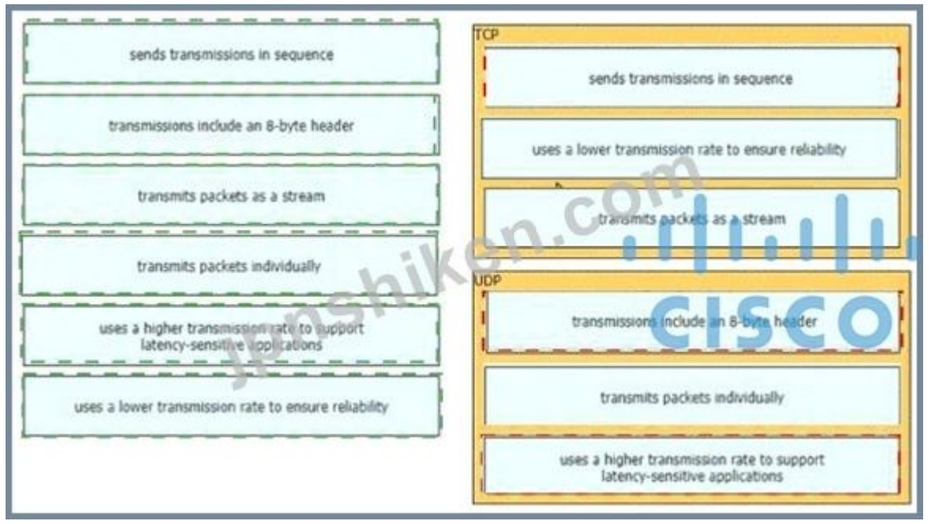
172.18.33.2 から送信されたパケットは、172.18.32.38 宛てです。ルーターはこのパケットをどこに転送しますか？
A. ギガビットイーサネット0/0
B. ループバック0
C. 10.1.1.1
D. 10.1.1.3
正解: (正解を表示します)
GigabitEthernet0/0. Routing questions are solved by applying longest-prefix match, administrative distance, metric, and protocol-specific behavior in the correct order. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. Wrong answers either use the wrong prefix, the wrong next hop, or a route source that would not be

preferred. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: 451

左側のIPプロトコル伝送の説明を、右側のIPトラフィックの種類にドラッグアンドドロップしてください。

正解:



Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this form test whether each protocol, command, service, or architecture term is placed with the function it actually performs. The safest approach is to classify each item by operating layer and purpose before matching it: routing behavior belongs to IP connectivity, wireless modes belong to access, REST methods belong to automation, and AAA functions belong to security services. Several distractors are valid networking terms, but they become wrong when mapped to the wrong plane or protocol. The retained mapping follows Cisco terminology and reflects

how the features are used in implementation and troubleshooting. In practice, this prevents mixing up forwarding behavior with management behavior or authentication with authorization/accounting. The mapping shown in the file is therefore retained as the verified response.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **452**

R1をNTPサーバーとして使用する場合、以下の要件を満たす必要があります。

* NTP認証が有効になっています
* ループバックインターフェース0から送信されたNTPパケット
* NTP 層 2
* NTPパケットはクライアントIPアドレス209.165.200.225のみに許可されます。

R1はどのように設定すべきですか？

A.
```
ntp authenticate
ntp authentication-key 2 md5 CISCO123
ntp source Loopback0
nntp access-group server-only 10
ntp master 2
!
access-list 10 permit 209.165.200.225
```

B.
```
ntp authenticate
ntp authentication-key 2 md5 CISCO123
ntp source Loopback0
ntp access-group server-only 10
ntp stratum 2
!
access-list 10 permit udp host 209.165.200.225 any eq 123
```
C.
```
ntp authenticate
ntp authentication-key 2 sha1 CISCO123
ntp source Loopback0
ntp access-group server-only 10
ntp master 2
!
access-list 10 permit udp host 209.165.200.225 any eq 123
```
D.
```
ntp authenticate
ntp authentication-key 2 md5 CISCO123
ntp interface Loopback0
ntp access-group server-only 10
```

正解: **B** (コメントを発表する)

Option B. Infrastructure services must be identified by their exact function: monitoring, time, address assignment, file transfer, logging, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under IP Services, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The distractors name real services, but those services do not perform the action requested in the prompt. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **453**

ネットワーク管理者は、2 つのサイト間で DHCP サービスを有効にする必要があります。ルーターが DHCPDISCOVER メッセージをサーバーに渡すには、何を構成する必要がありますか?

A. DHCP リレー エージェント
B. DHCP バインディング
C. DHCP プール
D. DHCP スヌーピング

正解: **(**正解を表示します**)**

Answer A is the technically correct selection. A DHCP relay agent forwards DHCP broadcasts across routed boundaries. Because routers do not normally forward broadcasts, the relay receives DHCPDISCOVER from the client subnet and unicasts it to the configured DHCP server. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. A DHCP pool makes the router a server, DHCP binding records leases, and DHCP snooping is a switch security feature. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

質問: **454**

動的に割り当てられた IP アドレスを取得するために IPv4 ホストが使用するプロトコルはどれですか?

A. ARP
B. DHCP
C. CDP
D. DNS

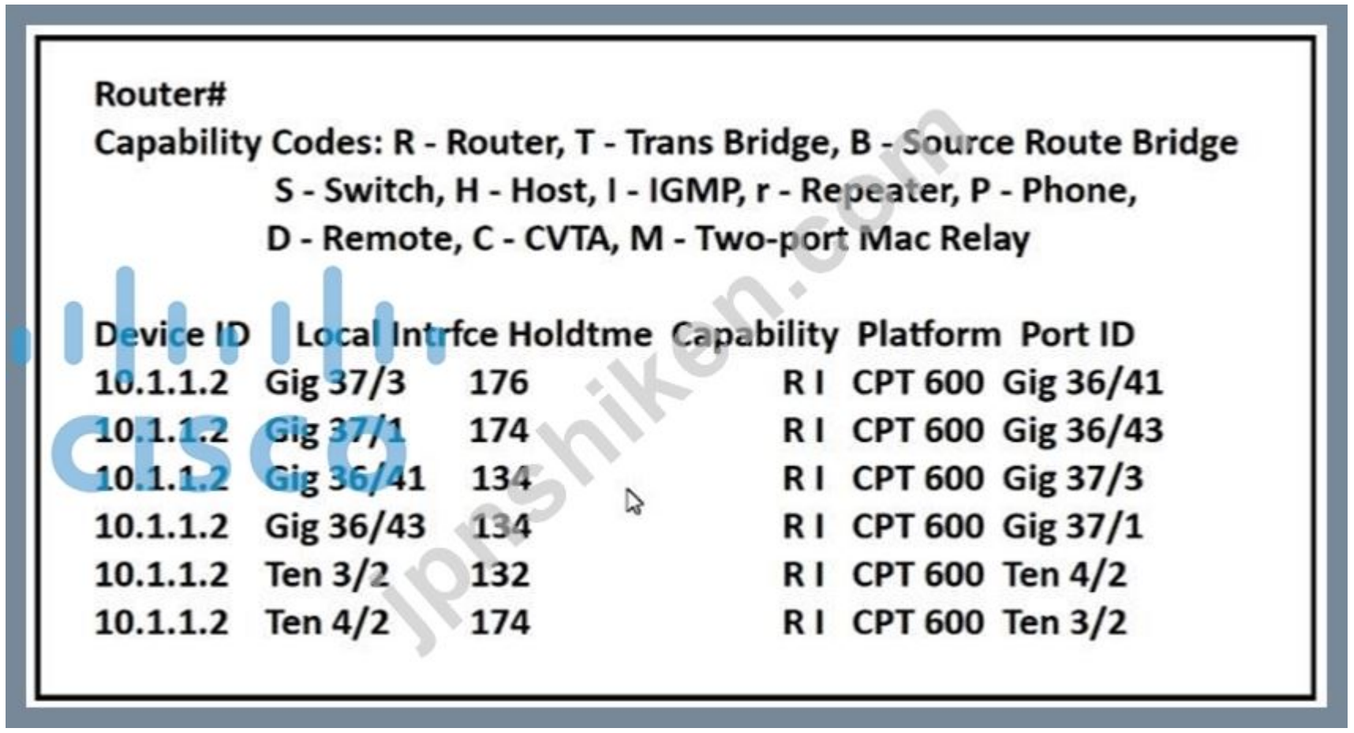
正解: **B** (コメントを発表する)

Use B for this item. IPv4 hosts use DHCP to obtain dynamically assigned IP addressing information. The DHCP process supplies an IP address, subnet mask, default gateway, DNS server, and lease information without manual host configuration. In Cisco CCNA 200-301 v1.1, IP Services questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. ARP resolves IP addresses to MAC addresses, DNS resolves names, and CDP discovers Cisco neighbors. A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **455**
VoIPなど、低遅延が求められるアプリケーションにおいて、UDPがTCPよりも適しているのはなぜですか？
A. UDPはすべてのパケットの確実な配信を保証しますが、TCPは負荷が高い場合にパケットを破棄します。
B. TCPは受信したパケットごとに確認応答を送信し、UDPは確認応答なしで動作します。
C. UDPはパケットが順番に到着するようにシーケンスデータを使用し、TCPはパケットをランダムな順序で受信する機能を提供します。
D. TCPは効率的なパケット配信のために輻輳制御を使用し、UDPはパケット配信のためにフロー制御メカニズムを使用します。
正解: (正解を表示します)
TCP sends an acknowledgment for every packet that is received and UDP operates without acknowledgments.. Network fundamentals questions require careful attention to address scope, media type, cabling limits, topology design, virtualization, cloud service models, and the difference between TCP and UDP. The CCNA 200-301 v1.1 blueprint expects candidates to identify not only definitions but also the operational consequence of each choice. For example, public and private addressing have different routing behavior; fiber and copper use different physical media; TCP and UDP make different reliability tradeoffs; and virtualization abstracts physical resources through a hypervisor. The wrong answers are usually plausible terms from the same area, but they do not match the exact condition described in the question. The selected answer is correct because it is the only option that fits the stated network behavior, design requirement, or physical/logical property. That is the level of precision needed for Cisco troubleshooting and implementation work.

質問: **456**
1分間に60回出現する信号周波数は?
A. 1 Hz 信号
B. 1 GHz 信号
C. 60 Hz 信号
D. 60 GHz 信号
正解: (正解を表示します)
1 Hz signal. Frequency is measured in hertz, where 1 Hz means one cycle per second. A signal that appears
60 times per minute appears once every second, so it is a 1 Hz signal. A 60 Hz signal appears 60 times per second, or 3,600 times per minute. A gigahertz signal cycles billions of times per second, far beyond the count in the question. Cisco CCNA 200-301 v1.1 Network Fundamentals includes basic media and signal concepts because wireless and physical-layer technologies depend on frequency, wavelength, and rate. The corrected answer is 1 Hz signal. The original GHz answer was off by several orders of magnitude and confused cycles per minute with cycles per second.

質問: **457**
展示資料を参照してください。



この出力はどのコマンドで得られますか？

A. show ip route
B. show ip interface
C. インターフェースを表示
D. CDPネイバーを表示
正解: **(**正解を表示します**)**
The command that displays directly connected Cisco neighbors, their local interface, remote interface, platform, and capability information is show cdp neighbor. CDP is Cisco Discovery Protocol, a Layer 2 discovery protocol used by Cisco devices to advertise basic identity and adjacency information to directly connected neighbors. The other choices produce completely different outputs. show ip route displays the routing table. show ip interface displays Layer 3 interface status and IP-related settings. show interface gives physical and data-link interface counters, line protocol state, errors, and bandwidth details. Cisco CCNA 200-
301 v1.1 includes discovery protocols under Network Access because engineers use CDP and LLDP to validate physical topology, switchport connections, voice-phone attachment, and neighbor device identity. CDP is Cisco-proprietary, while LLDP is standards-based. In this question, the exhibit is neighbor-oriented rather than routing-oriented or counter-oriented, so the correct operational command is show cdp neighbor.

質問: **458**
特定のサブネットで First Hop Redundancy Protocol を使用する目的は何ですか?
A. ループのない物理トポロジーを保証
B. 宛先 IP アドレス指定に基づいてトラフィックをフィルタリングします
C. ネットワーク上のホストにデフォルト ルートを送信します。
D. ルーター間でマルチキャスト hello メッセージを転送します
正解: **(**正解を表示します**)**

forwards multicast hello messages between routers. IP services questions require matching the service to its exact operational role, such as logging, address assignment, file transfer, monitoring, redundancy, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management-plane function. The distractors are real technologies, but they solve different infrastructure problems. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

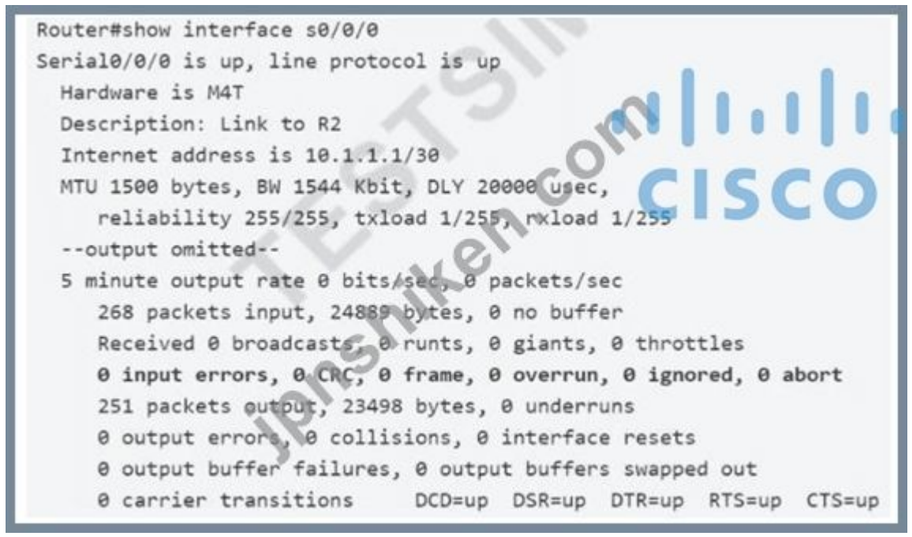
質問: **459**
展示資料を参照してください。

```
R_1# show ip route
     ....
D    192.168.20.0/26 [90/24513456] via 10.10.10.1
R    192.168.20.0/24 [120/5] via 10.10.10.2
O    192.168.0.0/19 [110/219414] via 10.10.10.13
B    192.168.0.0/16 is variably  subnetted, 4 subnets, 4 masks
D    192.168.20.0/27 [90/4123710] via  10.10.10.12
D    192.168.20.0/25  [90/14464211] via 10.10.10.11
S.    0.0.0.0/0 [1/0] via 10.10.10.14
```

パケットは192.168.10.1から宛先IPアドレス192.168.20.75へ流れています。ルーターはパケットに対してどのネクストホップを選択しますか？
A. 10.10.10.1
B. 10.10.10.11
C. 10.10.10.12
D. 10.10.10.14
正解: **B (**コメントを発表する**)**
10.10.10.11. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **460**
スイッチに入るフレームは、フレーム チェック シーケンスに失敗します。インクリメントされる 2 つのインターフェイス カウンタはどれですか? (2つ選んでください)
A. ラント
B. 巨人
C. フレーム
D. CRC
E. 入力エラー
正解: **D,E (**コメントを発表する**)**
A frame that fails the Ethernet Frame Check Sequence is counted as a CRC error and also contributes to input errors. The FCS field is the Ethernet trailer's error-detection value; the receiver recalculates the value and compares it with the frame's received FCS. If the values do not match, the frame is considered corrupted and is discarded. Cisco interface counters commonly report that condition under CRC, while

the broader input errors counter includes CRC and other receive-side problems such as runts, giants, frame errors, overrun, ignored, and no-buffer conditions. Runts and giants are size-related counters, not the direct result of the FCS failure described in the question. The frame counter is not the best paired answer here. In CCNA 200-301 v1.
1 Network Fundamentals, this maps to Ethernet operation and interface troubleshooting. The verified answers are D and E: CRC and input errors. Reference: Cisco interface counter interpretation and Ethernet FCS behavior.



質問: 461
SDN環境におけるノースバウンドAPIの機能は何ですか？
A. 構成のための分散処理をサポートします。
B. グローバルなプロビジョニングと構成に依存します。
C. ソフトウェアをアップグレードし、ファイルを復元します。
D. オーケストレーションおよびネットワーク自動化サービスを提供します。
正解: **(正解を表示します)**
It provides orchestration and network automation services.. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE. JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact with a controller, while southbound APIs allow the controller to communicate with network devices.
NETCONF and RESTCONF are configuration/management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to-device communication with application-to-controller communication or confuse a data format with a protocol. Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers. The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

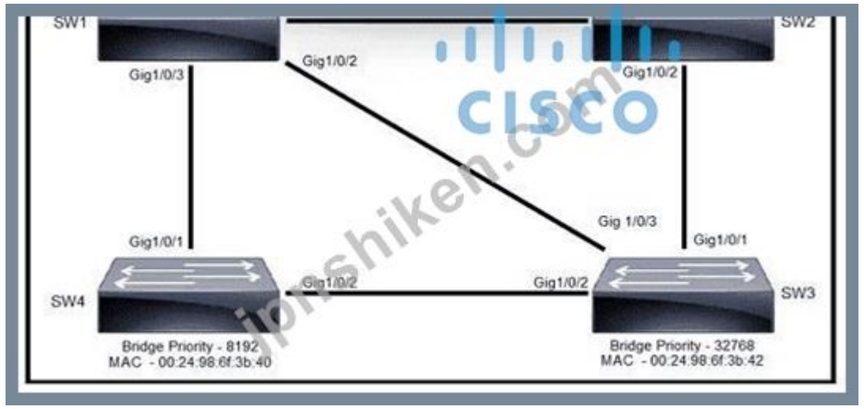
質問: 462
これらの基準に基づいてルーターとスイッチを接続する場合、どのタイプのケーブルを使用する必要がありますか？
* ピン1と2は受信機、ピン3と6は送信機です。
* MDi-Xの自動検出は利用できません
A. ストレートスルー
B. ロールオーバー
C. クロスオーバー

D. コンソール
正解: **C** (コメントを発表する)
crossover. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **463**
光ファイバーケーブルと銅線ケーブルを区別する2つの事実は何ですか？(2つ選択してください。)
A. 温度や湿度の変化に対する感度が高い。
B. より遠くまで信号を伝送します。
C. PoEデバイスのために、より遠くまで電流を伝送します。
D. パッチケーブルを購入する方が安価です。
E. より高度なスループットオプションを提供します。
正解: (正解を表示します)
Answer A,B is correct: A. It has a greater sensitivity to changes in temperature and moisture.; B. It carries signals for longer distances.. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE. JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact with a controller, while southbound APIs allow the controller to communicate with network devices. NETCONF and RESTCONF are configuration/management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to-device communication with application-to-controller communication or confuse a data format with a protocol. Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers. The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

質問: **464**
宛先ネットワークへ
トラフィックを送信するために使用されるインターフェースはどれですか？
10.249.210.56/25 [90/6144] via G0/15
10.249.210.56/25 [90/45053] via G0/13
10.249.210.56/25 [110/3693] via G0/16
10.249.210.56/25 [110/360] via G0/12
A. G0/16
B. G0/15
C. G0/13
D. G0/12
正解: (正解を表示します)
G0/15. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **465**
展示資料を参照してください。



Rapid PVST+モー ドは、各スイッチで同じVLAN上で動作します。この場合、どちらのスイッチがルートブリッジとなり、その理由はなぜでしょうか？

A. SW2、MACアドレスが最も高いため
B. SW3、優先順位が最も高いため
C. SW4。優先順位が最も高く、MACアドレスが低いため。
D. SW1、優先順位が最も低く、MACアドレスが最も高いため
正解: (正解を表示します)

SW4, because its priority is highest and its MAC address is lower. The spanning-tree root bridge is elected by the lowest bridge ID, and the bridge ID begins with bridge priority. In the exhibit, SW4 has the lower configured priority compared with SW3, making SW4 the root bridge even before MAC address tie-breakers matter. A higher priority value is worse, not better, for root election. Cisco CCNA 200-301 v1.1 Network Access expects engineers to remember that the lowest priority wins; only if priorities tie does the lowest MAC address decide. The corrected answer is the option naming SW4. The wording in the option may be imperfect, but the device selection is driven by the lowest priority shown in the exhibit.

質問: **466**
展示資料を参照してください。

指定されたWindows PCは、www.cisco.comのホストのIPアドレスを要求しています。この要求はどのIPアドレスに送信されますか？

A. 192.168.1.226
B. 192.168.1.100
C. 192.168.1.254
D. 192.168.1.253

正解: **(**正解を表示します**)**

192.168.1.253. The answer follows from normal Cisco device behavior and the operating clue in the scenario.
Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The other options use adjacent terms, wrong-layer behavior, or configuration that would not produce the requested result. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

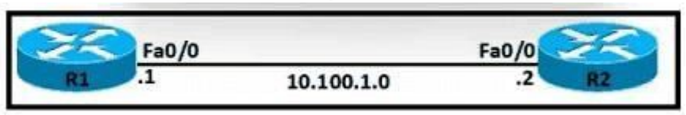
質問: **467**

QoSにおいてネットワークトラフィックを分類する目的は何ですか？

A. パケットのクラス識別子をパケットヘッダーの専用フィールドに書き込みます。
B. クラスに応じたサービストラフィック

C. ネットワークデバイス上でトラフィックマッチングルールを設定します
D. 特定の処理を受けるトラフィックの種類を識別します
正解: **D** (コメントを発表する)
Identifies the type of traffic that will receive a particular treatment. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **468**
展示資料を参照してください。



OSPFネイバー関係は、以下のガイドラインに従って設定する必要があります。
* R1はR2とのみネイバー関係を確立することが許可されています
* R1はDR選挙には決して参加しない
* R1はルーターIDとして10.1.1.1を使用します
どの構成を使用すべきですか？

A.
```
ip address 10.1.1.1 255.255.255.255
interface FastEthernet0/0
 ip address 10.100.1.1 255.255.255.252
 ip ospf priority 100
 ip access-group 102 in

outer ospf 10
 log-adjacency-changes
 network 10.1.1.1 0.0.0.0 area 0
 network 10.100.1.0 0.0.0.3 area 0
 ospf router-id 10.1.1.1

ccess-list 102 permit 88 host 10.100.1.2 host 224.0.0.
ccess-list 102 deny 88 any any
```

B.
```
interface Loopback0
 ip address 10.1.1.1 255.255.255.255

interface FastEthernet0/0
 ip address 10.100.1.1 255.255.255.252
 ip ospf priority 0
 ip access-group 102 in

router ospf 10
 log-adjacency-changes
 network 10.1.1.1 0.0.0.0 area 0
 network 10.100.1.0 0.0.0.3 area 0
 router-id 10.1.1.1

access-list 102 permit 88 host 10.100.1.2 host 224.0.0.5
access-list 102 deny 88 any any
access-list 102 permit ip any any
```

C.

D.

正解: **B** (コメントを発表する)

Option. The correct OSPF configuration must satisfy all three stated constraints at the same time. First, R1 must use a router ID of 10.1.1.1, which is supported by the loopback address and router-id setting in the option. Second, R1 must never participate in a DR election, so the FastEthernet interface must use ip ospf priority 0. Third, R1 must form an OSPF relationship only with R2, which is addressed by the access list permitting OSPF protocol 89 from host 10.100.1.2 to 224.0.0.5 while denying other traffic. Cisco CCNA 200-301 v1.1 IP Connectivity expects engineers to combine OSPF adjacency requirements, DR election behavior, and control-plane filtering. Options with priority 100 make R1 likely to become DR, and options with broader ACLs fail the neighbor-restriction requirement. Therefore Option B is the verified configuration.

質問: **469**

アクセス ポイントが PoE スイッチ ポートに接続されている場合、電力割り当てに自動モードと静的モードを使用する利点は何ですか?

A. ケーブルの 4 つのペアすべてが使用されます。

B. デバイスが受電デバイスであることを検出します

C. アクセスポイントのデフォルトレベル

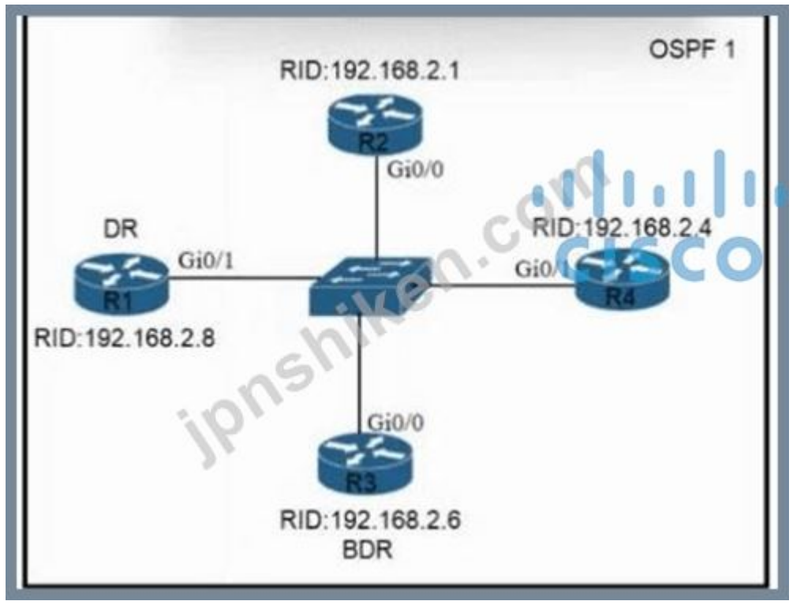
D. 同時に電力ポリシングが有効

正解: **B** (コメントを発表する)

It detects the device is a powered device. In PoE auto mode, the switch detects that the connected endpoint is a powered device and allocates power based on negotiation and device requirements. Static mode reserves power whether the device actually needs that amount or not, which can waste available PoE budget on a switch. Power policing is a related feature but it is not the basic advantage of auto mode over static mode.

Cisco CCNA 200-301 v1.1 Network Access includes PoE behavior because access points, IP phones, and cameras depend on switch-provided power. The corrected answer is that auto mode detects the powered device. That is the operational reason auto allocation is generally preferred for access points and other PoE endpoints when the switch can negotiate and manage power dynamically.

質問: **470**



図を参照してください。ネットワーク内のすべてのルータは設定済みです。R2 は DR である必要があります。エンジニアがデバイスを接続した後、R1 が DR に選出されました。ネットワークで R2 が DR に選出されるには、R2 にどのコマンド シーケンスを設定する必要がありますか？

A. R2(config)#interface gi0/0 R2(config-if)#ip ospf priority 100
B. R2(config)#router ospf 1 R2(config-router)#router-id 192.168.2.7
C. R2(config)#router ospf 1 R2(config-router)#router-id 10.100.100.100
D. R2(config)#interface gi0/0 R2(config-if)#ip ospf priority 1
正解: **A (**コメントを発表する**)**
R2(config)#interface gi0/0 R2(config-if)#ip ospf priority 100. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **471**
ネットワーク エンジニアは、これらの要件を満たすために、アドレス ブロック 10.70.128.0/19 を使用して 2 つの新しいサブネットを構成する必要があります。
- 最初のサブネットは 24 のホストをサポートする必要があります
- 2 番目のサブネットは 472 のホストをサポートする必要があります
- 両方のサブネットで、可能な限り最長のサブネット マスクを使用する必要があります。
アドレスブロック
新しいサブネットを構成し、ルーター インターフェイスの各サブネットで最初に使用可能なアドレスを使用するという要件を満たすために使用する必要がある 2 つの構成はどれですか? (2つ選択)
A. インターフェイス VLAN 1234
IP アドレス 10.70.159.1 255.255.254.0
B. インターフェイス VLAN 1148
IP アドレス 10.70.148.1 255.255.254.0
C. インターフェイス VLAN 4722

IP アドレス 10.70.133.17 255.255.255.192
D. インターフェイス VLAN 3002
IP アドレス 10.70.147.17 255.255.255.224
E. インターフェイス VLAN 155
IP アドレス 10.70.155.65 255.255.255.224
正解: (正解を表示します)
Answer B,D is correct: B. interface vlan 1148ip address 10.70.148.1 255.255.254.0; D. interface vlan 3002ip address 10.70.147.17 255.255.255.224. Cisco routers select forwarding paths by longest-prefix match first, then administrative distance and metric when comparable routes compete. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The wrong choices either do not match the destination, use the wrong next hop, or fail to provide the intended primary/backup behavior. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **472**
ルート ポートの選択プロセスで最初に使用される基準は何ですか?
A. ローカル ポート ID
B. ルート ブリッジへの最小パス コスト
C. 最下位のネイバーのブリッジ ID
D. 最下位のネイバーのポート ID
正解: (正解を表示します)
This item is the same STP concept as the previous one: root port selection begins with the lowest total path cost to the root bridge. A switch evaluates each possible path toward the root and selects the port that gives the lowest cumulative STP cost. If multiple ports tie on cost, the switch then applies the STP tie-breakers in order. It compares the lowest neighbor bridge ID, then the lowest neighbor port ID, and finally the lowest local port ID if needed. The exam often repeats this rule because engineers must troubleshoot blocked links by understanding exactly why a port was selected. Cisco CCNA 200-301 v1.1 Network Access includes spanning-tree operation, root bridge behavior, and root port selection. The first criterion is not local port ID or neighbor information. Those are secondary tie-breakers. The correct first criterion is the lowest path cost to the root bridge.

質問: **473**
オフィスには 8 フロアがあり、1 フロアあたり約 30 ～ 40 人のユーザーがいます。
アドレス空間を効率的に使用するには、ルーターのスイッチ仮想インターフェイスでどのコマンドを構成する必要がありますか?
A. IP アドレス 192.168.0.0 255.255.0.0
B. IP アドレス 192.168.0.0 255.255.254.0
C. IP アドレス 192.168.0.0 255.255.255.128
D. IP アドレス 192.168.0.0 255.255.255.224
正解: (正解を表示します)
ip address 192.168.0.0 255.255.254.0. Eight floors with roughly 30 to 40 users each require an address block large enough for about 320 hosts, plus growth and reserved addresses. A /23 provides 512 total IPv4 addresses and 510 usable host addresses, which is far more efficient than a /16 while still large enough for the building. A /25 supports only 126 usable hosts, and a /27 supports only 30 usable hosts, which is too small for a floor with up to 40 users if each floor needs its own subnet. Cisco CCNA 200-301 v1.1 Network Fundamentals requires subnet sizing by usable host count, not by guessing at classful ranges. The subnet mask
255.255.254.0 corresponds to /23. It fits the stated requirement with reasonable efficiency and avoids the massive waste of 255.255.0.0. Therefore, the correct router SVI addressing choice is the /23 option.

質問: **474**
ネットワーク上の過剰なトラフィックを調査したところ、インターフェースにIPv4 ACLが適用されているにもかかわらず、そのインターフェースへのすべての受信パケットが許可されているように見えることが判明した。
この動作を引き起こす設定ミスはどれですか？(2つ選択してください)
A. パケットが許可ステートメントに一致しません
B. アクセス テストで一致する許可ステートメントが高すぎます
C. 一致する許可ステートメントの定義が広すぎる
D. ACLが空です
E. アクセスリスト内で一致する拒否ステートメントが上位にあります
正解: **B,C (コメントを発表する)**
Answer B,C is correct: B. A matching permit statement is too high in the access test; C. A matching permit statement is too broadly defined. The answer follows directly from normal Cisco device behavior and the wording of the scenario. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **475**
FHRP の利点を 2 つ挙げてください。2つ選んでください。）
A. デフォルト ゲートウェイの自動フェイルオーバーを有効にします。
B. 複数のデバイスがネットワーク内のクライアントの単一の仮想ゲートウェイとして機能できるようにします。
C. 複数のポートをバンドルして帯域幅を増やすことができます。
D. レイヤ 2 ネットワークでのループを防止します。
E. 暗号化されたトラフィックを許可します。
正解: **A,B (コメントを発表する)**
Answer A,B is correct: A. They enable automatic failover of the default gateway.; B. They allow multiple devices to serve as a single virtual gateway for clients in the network.. The answer follows directly from normal Cisco device behavior and the wording of the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem.
The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **476**
Cisco WLCにおけるコンソールポートの主な目的は何ですか？
A. 非同期トランスポートによるインバンド管理
B. IPトランスポートを介した帯域外管理
C. IPトランスポートを介したインバンド管理
D. 非同期トランスポートによる帯域外管理
正解: **(正解を表示します)**

out-of-band management via an asynchronous transport. Wireless questions depend on AP mode, WLAN security, RF band selection, controller interfaces, and client roaming or authentication behavior. Cisco CCNA
200-301 v1.1 includes this under Network Access, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong options confuse encryption with authentication, local switching with tunneling, or controller management with client data handling. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **477**
既存のテーブルまたはビューを変更する CRUD 操作はどれですか?
A. 読む
B. 作成
C. 置換
D. 更新
正解: **D (**コメントを発表する**)**
In CRUD terminology, update is the operation that modifies an existing record, table entry, object, or view.
Create adds something new, read retrieves existing information, update changes existing information, and delete removes it. Some APIs use replace or patch semantics, but the CRUD term being tested for modification is update. Cisco CCNA 200-301 v1.1 Automation and Programmability includes CRUD because REST APIs and controller-based platforms use these concepts constantly. For example, an HTTP GET commonly maps to read, POST often maps to create, PUT or PATCH may map to update, and DELETE maps to delete. The wording says ' modifies an existing table or view, ' which rules out create and read. Replace is not one of the standard CRUD letters. The correct CRUD operation is update. Therefore, D is correct.

質問: **478**
展示資料を参照してください。

jpnshiken.com

ネットワークエンジニアは新しい無線LANを構成しており、RADIUSサーバーではなく静的パスワードを認証に使用するように指示されています。構成を完了するために、エンジニアは他にどのような作業を行う必要がありますか？

A. Crable PSKEnable iod 1s

B. WPA2ポリシーを選択し、PMFEを無効にし、PSKを有効にします。

C. WPAポリシーを選択してPSKを有効にする

D. WPAポリシーを選択 WRASポリシーを選択

正解: **(**正解を表示します**)**

Select WPA2 PolicyDisable PMFEnable PSK. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **479**

プライベートIPv4アドレスの範囲はどの機能を実行しますか？

A. 複数の企業がそれぞれ同じアドレスを競合なしで使用できるようにします

B. エンタープライズネットワークの外部からホストに直接接続を提供します

C. プライベート範囲アドレス指定を使用してインターネットに到達するためにNATが必要ないことを保証します

D. すべての外部ホストのインターネットへの安全な通信を可能にします

正解: **(**正解を表示します**)**

Private IPv4 address ranges allow different organizations to reuse the same internal address space without creating global internet conflicts. RFC 1918 reserves 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 for private use. These addresses are not meant to be routed on the public internet. That reuse is one reason enterprises, homes, labs, and cloud networks can all use addresses such as 10.1.1.0 internally. When private hosts need internet access, NAT or another translation design is normally required. Cisco CCNA 200-301 v1.1 includes private addressing and NAT under IP Services because these concepts appear constantly in enterprise networks. The wrong answers imply that private addressing provides direct external reachability or removes the need for NAT, which is exactly backwards. Private addressing conserves public IPv4 space and avoids the need for every internal host to consume a globally unique address. Therefore, A correctly states the function.

質問: **480**
ゼロデイエクスプロイトとは何ですか?
A. 修正プログラムが公開される前に新たなネットワーク脆弱性が発見された場合
B. 犯人が二者間の会話に介入し、データを盗み取ったり改ざんしたりすることです。
C. ネットワークが悪意のあるトラフィックで飽和状態になり、リソースと帯域幅が過負荷になる状態です。
D. 攻撃者が SQL サーバーに悪意のあるコードを挿入した場合です。
正解: **(**正解を表示します**)**
It is when a new network vulnerability is discovered before a fix is available. Security questions require separating identity, authorization, accounting, encryption, management access, and physical protection. Cisco CCNA 200-301 v1.1 includes this under Security Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The distractors protect a different surface or represent weaker/deprecated methods. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **481**
アクセスポイントが固有のSSIDを1つ提供し、クライアントデータと管理トラフィックを転送し、自律モードで動作する場合、どのタイプの有線ポートが必要ですか？
A. デフォルト
B. アクセス
C. トランク
D. ラグ
正解: **B (**コメントを発表する**)**
Access. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **482**
SNMPエージェントはどのような機能を実行しますか？

A. NMSからの要求に応じてMIB変数に関する情報を送信します
B. 壊滅的なシステムイベントに関する情報をリモートネットワークノードに要求します。
C. ネットワーク内のレイヤ3デバイス間のルーティングを管理します
D. ネットワークデバイスとTACACS+ま　たはRADIUSサーバー間のユーザー認証を調整します。
正解: **(**正解を表示します**)**
it sends information about MIB variables in response to requests from the NMS. Infrastructure services must be identified by their exact function: monitoring, time, address assignment, file transfer, logging, or traffic treatment. Cisco CCNA 200-301 v1.1 includes this under IP Services, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The distractors name real services, but those services do not perform the action requested in the prompt. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **483**
IT部門の管轄外にあるオフィススペースに設置されたネットワークポートを悪用から保護するための推奨事項を2つ挙げてください。(2つ選択してください。)
A. ポートでPortFast機能を有効にする
B. ポートベース認証を実装する
C. 静的ARPエントリを設定する
D. ポートを固定速度に設定する
E. 未使用のポートをシャットダウンします
正解: **(**正解を表示します**)**
Answer B,E is correct: B. implement port-based authentication; E. shut down unused ports. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Network Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **484**
APIキーは、レート制限を実施するためにどのように使用されますか？
A. クライアントが受信を希望するデータ形式の種類を指定します。
B. APIリクエストがたどるべきネットワークパスを定義します
C. APIリクエストで送信されるデータを暗号化する
D. 各クライアントアプリケーションを一意に識別するため
正解: **D (**コメントを発表する**)**
to uniquely identify each client application. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco- consistent configuration or behavior for this wireless scenario.

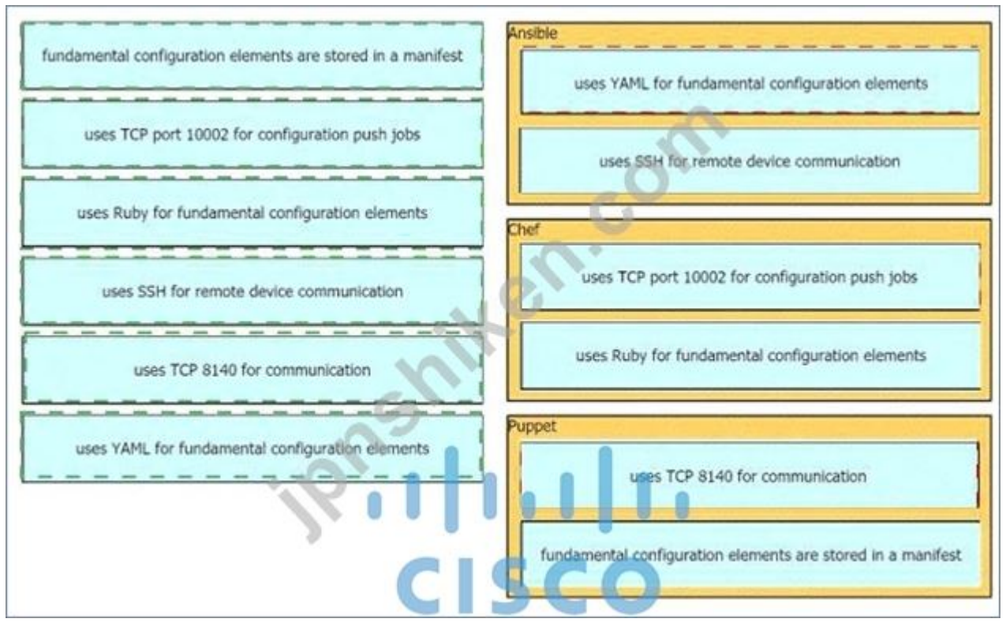
質問: **485**

オンサイトのサービスデスク技術者は、ユーザーのWindowsコンピュータ上のIPアドレスとDNSサーバー情報を確認する必要があります。技術者は、ユーザーのコンピュータのコマンドプロンプトにどのコマンドを入力する必要がありますか？
A. ipconfig /all
B. ifconfig -a
C. インターフェースを表示
D. netstat -r
正解: **(**正解を表示します**)**
ipconfig /all. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **486**
VRRP グループ 1 で使用される仮想 MAC アドレスはどれですか?
A. 0050.0c05.ad81
B. 0007.c061.bc01
C. 0000.5E00.0101
D. 0500.3976.6401
正解: **C (**コメントを発表する**)**
The verified answer is C. VRRP virtual MAC addresses use the format 0000.5E00.01xx, where xx is the VRRP group ID in hexadecimal. For group 1, the virtual MAC is 0000.5E00.0101. Cisco CCNA 200-301 v1.
1 places this skill in IP Connectivity, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. The other MAC addresses do not match the VRRP reserved virtual-router MAC format. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise.
The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

質問: **487**
左側の説明文を、右側の適切な構成管理技術にドラッグ＆ドロップしてください。

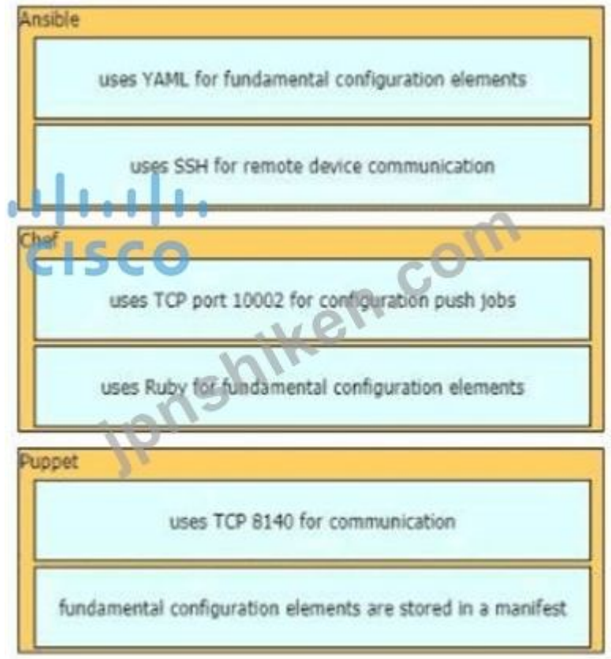
正解:



Explanation:

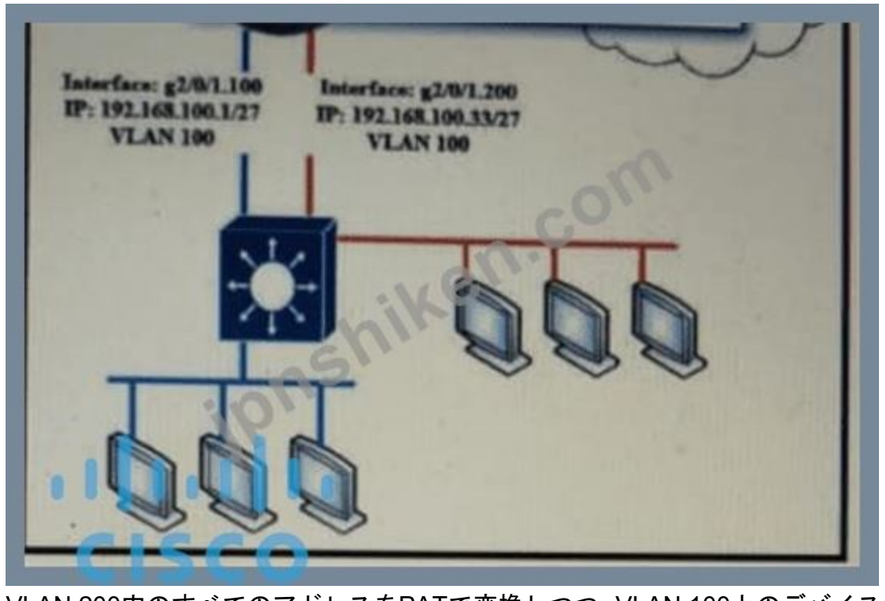
The drag-and-drop mapping is based on each tool's normal configuration-management model. Ansible is agentless, built around playbooks, and commonly uses SSH over TCP port 22 to communicate with managed nodes. Puppet uses a declarative model and stores configuration logic in manifests, typically written with Puppet's Ruby-influenced language and saved as .pp files. Chef uses recipes and cookbooks and is associated with a client/server automation model; Chef Push Jobs also uses a command channel for remote execution.

The important CCNA 200-301 v1.1 Automation and Programmability lesson is not to memorize marketing language but to separate the operating models: Ansible focuses on simple agentless execution, Puppet emphasizes declarative manifests, and Chef organizes configuration into recipes and cookbooks. The existing mapping follows those technology roles. Reference: Cisco CCNA automation objectives covering configuration management tools and common network automation characteristics.

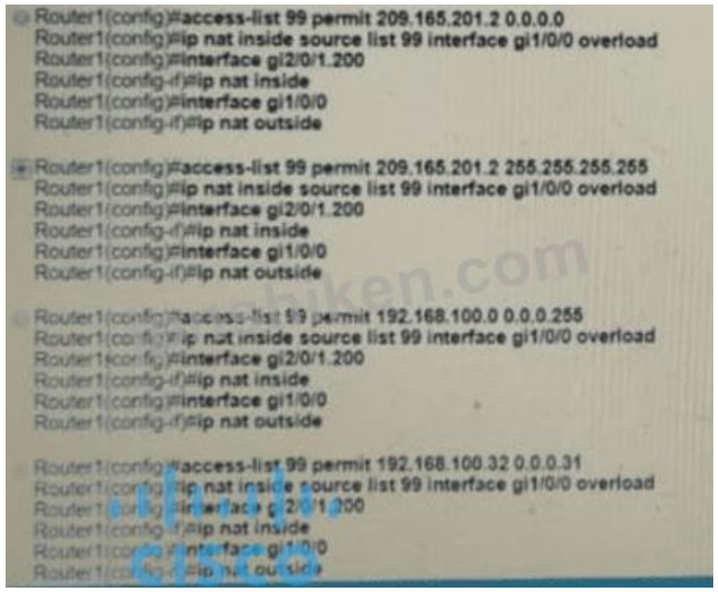


質問: 488

別添資料を参照してください。



VLAN 200内のすべてのアドレスをPATで変換しつつ、VLAN 100上のデバイスが独自のIPアドレスを使用できるようにするには、ルーターにどの設定を適用する必要がありますか？

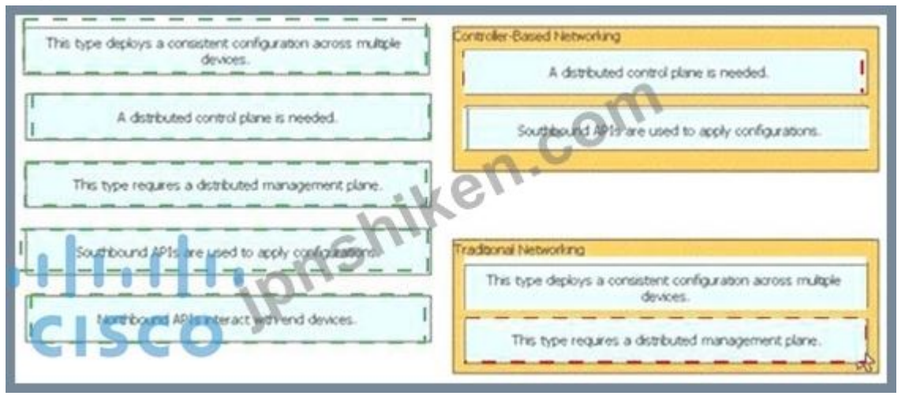


A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解: **D** (コメントを発表する)

Option D. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

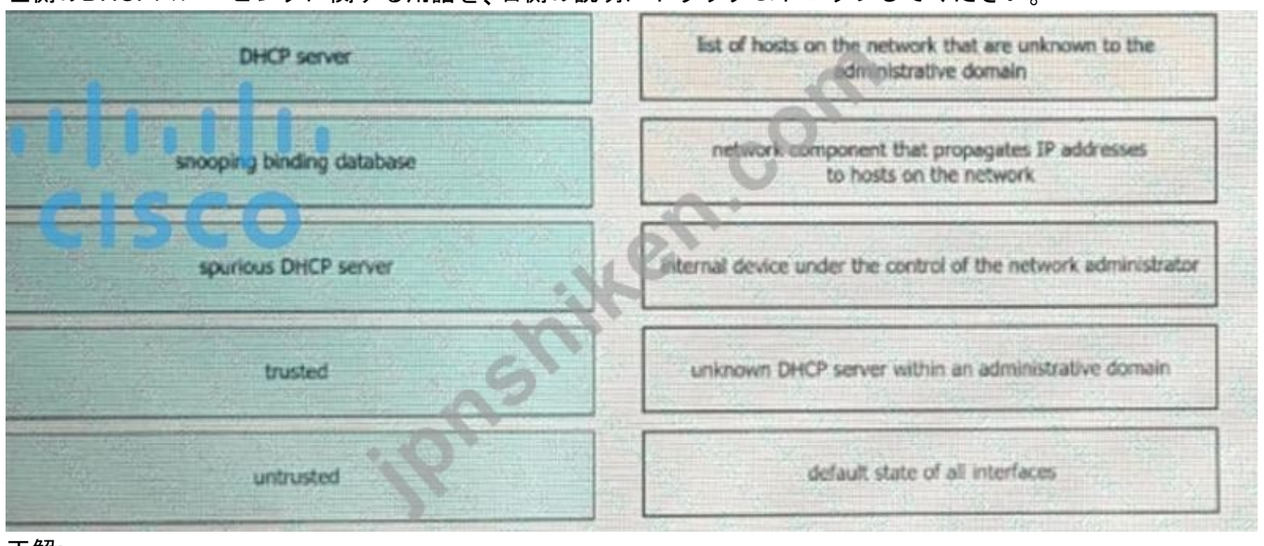
質問: **489**
左側のネットワークに関する記述を、右側の対応するネットワークの種類にドラッグ＆ドロップしてください。すべての記述が使用されるわけではありません。

正解:

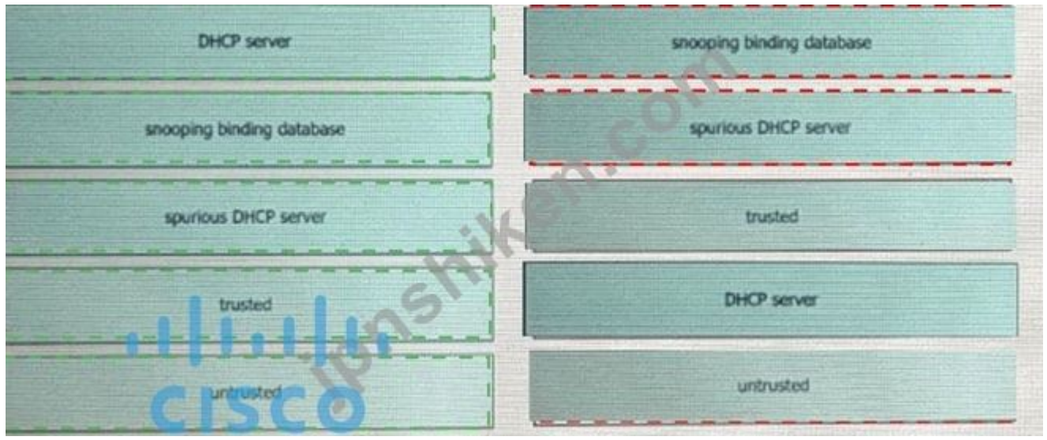


Explanation:
Answer the displayed drag-and-drop mapping is the technically correct selection. The networking statements must be matched to the correct architecture or networking type based on function. Traditional networking, controller-based networking, on-premises, cloud, or hybrid models differ by where services run, how devices are managed, and where control is centralized. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. The safest approach is to match operational responsibility rather than similar wording. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.

質問: **490**
左側のDHCPスヌーピングに関する用語を、右側の説明にドラッグ＆ドロップしてください。

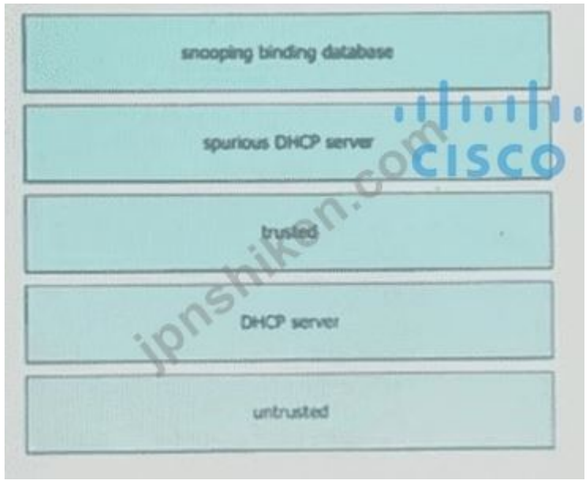


正解:



Explanation:

Answer the displayed drag-and-drop mapping is the technically correct selection. DHCP snooping builds a trusted binding table from legitimate DHCP exchanges. Trusted ports face valid DHCP servers, untrusted ports face clients, and the binding database becomes the source of truth for features such as Dynamic ARP Inspection and IP Source Guard. This aligns with Cisco CCNA 200-301 v1.1 because the exam blueprint requires engineers to recognize operational behaviour from configuration symptoms and topology requirements. Ordinary MAC learning does not validate DHCP messages, and trunking or STP alone cannot prevent a rogue DHCP server from handing out false gateways. Treat the distractors carefully: most are real Cisco terms, but they solve a different problem or operate at a different layer. The selected answer is the one that would be used by an engineer on the device or in the design to produce the outcome stated in the question.



質問: **491**

管理対象ノードとの通信時にデフォルトで TCP ポート 22 を使用する構成管理メカニズムはどれですか?

A. アンシブル

B. パイソン

C. パペット

D. シェフ

正解: **(**正解を表示します**)**

Ansible. Automation questions require separating controller roles, API direction, data formats, HTTP behavior, and configuration-management tooling. Cisco CCNA 200-301 v1.1 includes this topic under Automation and Programmability, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The incorrect options mix northbound and southbound communication, confuse data serialization with transport, or describe

traditional device-by-device management. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **492**
REST APIの基本認証において、認証情報を伝えるためにHTTPリクエストのどの部分が使用されますか？
A. クッキー
B. コンテンツタイプ
C. 認証
D. 受け入れる
正解: **(正解を表示します)**
accept. IP services questions are about the supporting protocols that make a network manageable and usable:
DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

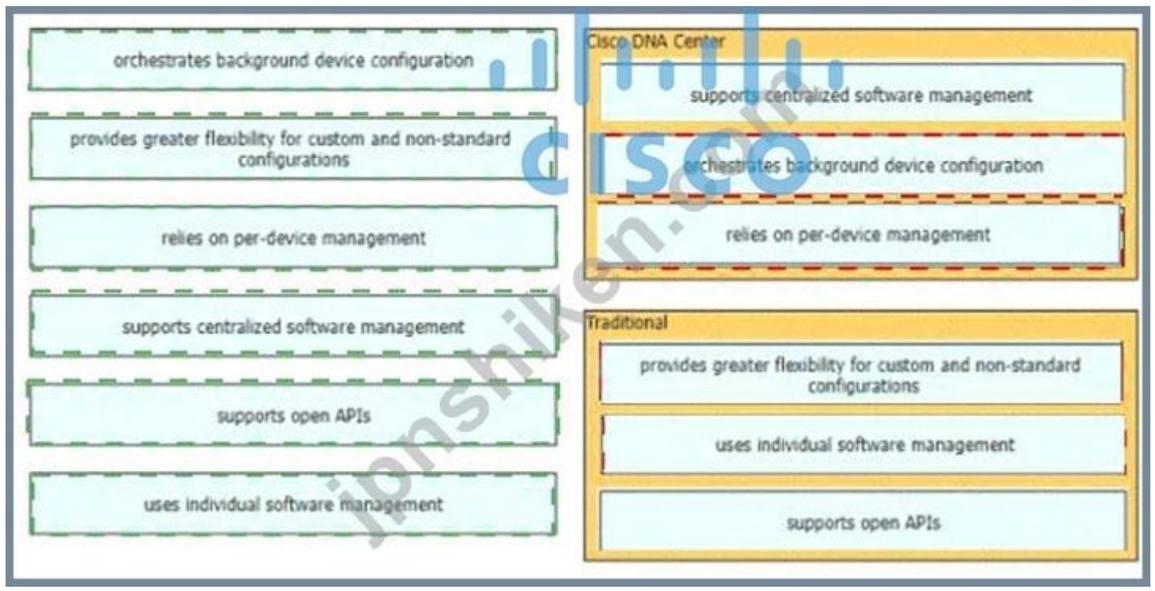
質問: **493**
展示資料を参照してください。

```
Cat9300# show cdp
Global CDP information:
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
   Sending CDPv2 advertisements is enabled
```

隣接するデバイスがスイッチCat9300を迅速に検出できるようにするには、どのような対策を講じる必要がありますか？
A. スイッチ Cat9300 で cdp timer 10 コマンドを設定します。
B. 隣接するデバイスに接続するポートでポートファストを有効にします。
C. スイッチ Cat9300 で cdp holdtime 10 コマンドを設定します。
D. スイッチ Cat9300 の隣接機器で cdp timer 10 コマンドを設定します。
正解: **(正解を表示します)**
Configure the cdp timer 10 command on switch Cat9300.. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

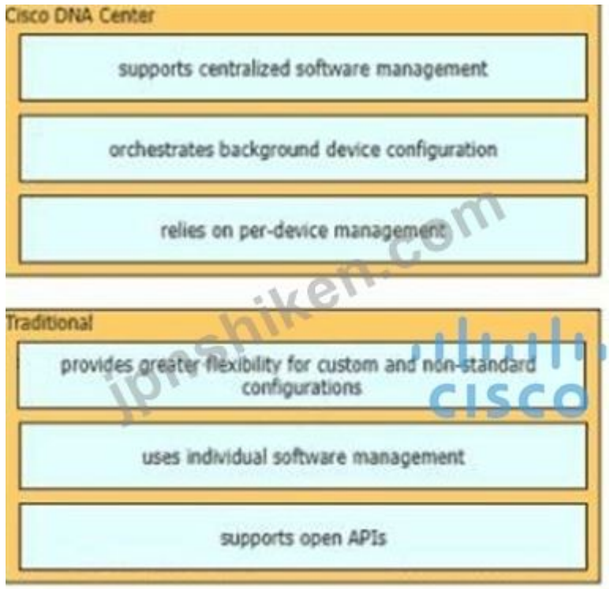
質問: **494**
左側のデバイス管理技術の特性を、右側の対応する展開タイプにドラッグアンドドロップしてください。

正解:



Explanation:

Cisco CCNA 200-301 v1.1 Network Fundamentals questions of this form test whether each protocol, command, service, or architecture term is placed with the function it actually performs. The safest approach is to classify each item by operating layer and purpose before matching it: routing behavior belongs to IP connectivity, wireless modes belong to access, REST methods belong to automation, and AAA functions belong to security services. Several distractors are valid networking terms, but they become wrong when mapped to the wrong plane or protocol. The retained mapping follows Cisco terminology and reflects how the features are used in implementation and troubleshooting. In practice, this prevents mixing up forwarding behavior with management behavior or authentication with authorization/accounting. The mapping shown in the file is therefore retained as the verified response.



質問: **495**
展示資料を参照してください。

192.168.10.33 ホストへのルートのメトリックは何ですか？

A. 84
B. 110
C. 192
D. 193

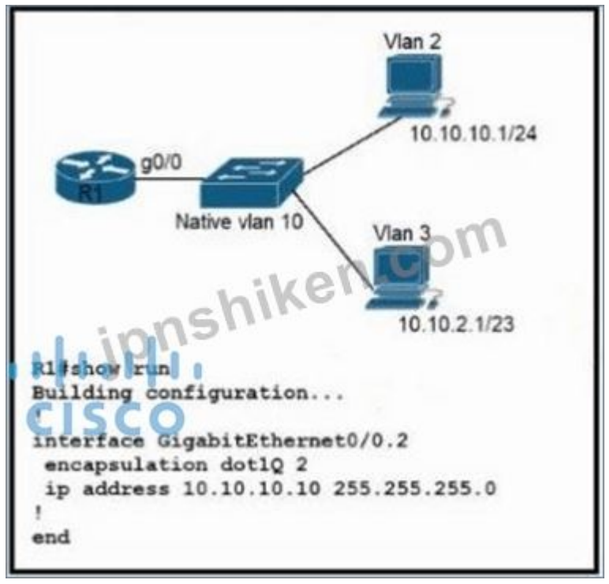
正解: (正解を表示します)

110. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In

production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates. Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability. The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **496**
ネットワークエンジニアが、認証サーバーの設定と動的インターフェースの作成によって、新しい無線LANの実装を開始します。基本設定を完了するために、次に何をする必要がありますか？
A. 管理インターフェースをインストールし、管理IPを追加します。
B. アクセスポイントの高可用性と冗長性を設定します。
C. 管理インターフェースでTelnetおよびRADIUSアクセスを有効にします。
D. 新しい WLAN を作成し、動的インターフェースをそれにバインドします。
正解: **(**正解を表示します**)**
Create the new WLAN and bind the dynamic interface to It.. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco- consistent configuration or behavior for this wireless scenario.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**1813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **497**


図を参照してください。スイッチとPCの設定は完了しています。
VLAN 2とVLAN 3が相互に通信できるようにするには、どの設定を適用する必要がありますか？

A. インターフェース GigabitEthernet0/0 IPアドレス 10.10.2.10 255.255.252.0
B. インターフェース GigabitEthernet0/0.3 カプセル化 dot1Q ネイティブ IP アドレス 3 10.10.2.10 255.255.252.0
C. インターフェース GigabitEthernet0/0.10 カプセル化 dot1Q 3
D. インターフェース GigabitEthernet0/0.3 カプセル化 dot1Q 10 IPアドレス 10.10.2.10 255.255.252.0
正解: **(**正解を表示します**)**
interface GigabitEthernet0/0.3 encapsulation dot1Q 3 native ip addresss 10.10.2.10 255.255.252.0. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **498**
展示資料を参照してください
。

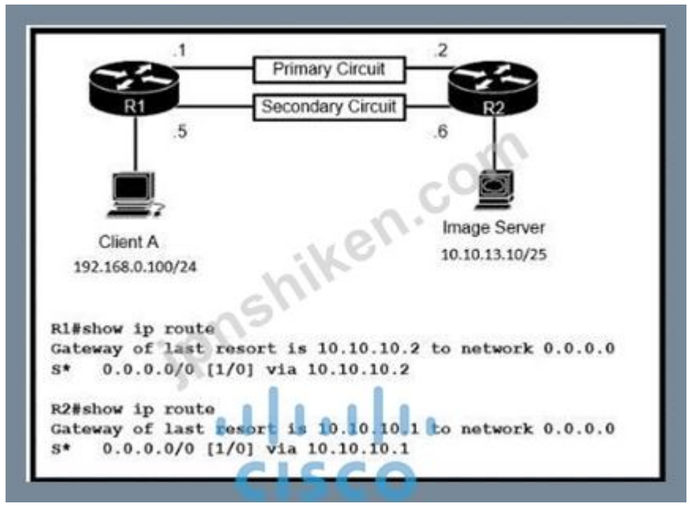
```
   Known via "connected", distance 0, metric 0 (connected, via interface)
   Routing Descriptor Blocks:
   * directly connected, via Ethernet0/1
       Route metric is 0, traffic share count is 1

CPE# ping 203.0.113.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

CPE# show ip route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
B*    0.0.0.0/0 [20/0] via 198.51.100.1, 00:02:07
      198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.51.100.0/30 is directly connected, Ethernet0/0
L        198.51.100.2/32 is directly connected, Ethernet0/0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/30 is directly connected, Ethernet0/1
L        203.0.113.2/32 is directly connected, Ethernet0/1
```

CPE に新しい静的ルートを設定した後、エンジニアは新しい設定が正常に動作していることを確認するために、一連のコマンドを入力しました。静的デフォルトルートはいつルーティングテーブルにインストールされますか？
A. 203 0 113.1 がネクストホップとして到達できなくなったとき B. 外部 BGP で学習したデフォルトルートが無効になったとき
B. BGP を介して 203.0 113 1 へのルートが学習された場合
C. 外部 BGP 上のデフォルト ルートのネクスト ホップが変更されたとき
正解: **A (**コメントを発表する**)**
when 203 0 113.1 is no longer reachable as a next hop B. when the default route learned over external BGP becomes invalid. Cisco forwarding uses longest-prefix match first, then administrative distance and metric when multiple sources compete. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Wrong choices either do not match the destination prefix, point to the wrong next hop, or fail to create the required primary or backup route. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **499**

WPA3が前世代の規格よりも高いセキュリティレベルを提供できるのは、どのような仕組みによるものですか？
A. 事前共有キーにおける特殊文字のサポート
B. SAEパスワードベースの鍵交換
C. 自動デバイスペアリング
D. 証明書ベースの認証
正解: **(正解を表示します)**
SAE password-based key exchange. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band.
The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities.
Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right- looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **500**



図を参照してください。ルータR1とR2は、それぞれLANインターフェースが設定されています。2つの回線は動作しており、WAN経由でアクセス可能です。プライマリ回線がダウンした場合にフェイルオーバー冗長性を確立するコマンドセットはどれですか？

R1(config)#**ip route 10.10.13.10 255.255.255.255 10.10.10.2**
R2(config)#**ip route 192.168.0.100 255.255.255.255 10.10.10.1**
R1(config)#**ip route 0.0.0.0 0.0.0.0 10.10.10.6 2**
R2(config)#**ip route 0.0.0.0 0.0.0.0 10.10.10.5 2**
R1(config)#**ip route 10.10.13.10 255.255.255.255 10.10.10.6**
R2(config)#**ip route 192.168.0.100 255.255.255.255 10.10.10.5**
R1(config)#**ip route 0.0.0.0 0.0.0.0 10.10.10.6**
R2(config)#**ip route 0.0.0.0 0.0.0.0 10.10.10.5**

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
正解: (正解を表示します)
The working routing table already shows a primary default route over the primary circuit. To establish failover, the backup path must be installed as a floating static route: a static route with the same destination but a higher administrative distance than the primary static route. Option B adds default routes through the secondary-circuit next hops and sets the administrative distance to 2. Because a normal static route has an administrative distance of 1, the router keeps the primary route in the routing table while it is reachable. If the primary next hop or exit path becomes unavailable, the route with AD 2 is then selected and traffic moves to the secondary circuit. The host-specific route options do not provide general default-route failover for all traffic, and a second default route without a higher administrative distance could create unwanted equal-cost forwarding. CCNA 200-301 v1.1 expects this distinction under static routing and IP Connectivity. Reference:
Cisco static route and floating static route behavior.

質問: **501**
ネットワーク上のエンドポイントの機能は何ですか？
A. ネットワーク上の VLAN 間でトラフィックを転送します
B. サーバーとクライアントデバイスをネットワークに接続します
C. ユーザーがデータを記録してタイルサーバーに送信することを可能にする
D. 建物内のユーザーに無線サービスを提供する
正解: (正解を表示します)
allows users to record data and transmit to a tile server. Wireless design and security require separating AP mode, WLAN identity, RF behavior, authentication, and encryption. Cisco CCNA 200-301 v1.1 includes this under Network Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The distractors confuse wireless standards, security mechanisms, controller settings, or RF design practices. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **502**
展示資料を参照してください。

どの設定であれば、ルーターR14とR86がOSPFv2隣接関係を確立しつつ、ルーター間でOSPF情報を交換するための中心点として機能することができますか？

A.

```
R14#
interface Loopback0
ip ospf 10 area 0

interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip ospf network broadcast
ip ospf 10 area 0
ip mtu 1500

router ospf 10
ip ospf priority 255
router-id 10.10.1.14

R86#
interface Loopback0
ip ospf 10 area 0

interface FastEthernet0/0
ip address 10.73.65.66 255.255.255.252
ip ospf network broadcast
ip ospf 10 area 0
ip mtu 1500
```

B.

```
R14#
nterface FastEthernet0/0
p address 10.73.65.65 255.255.255.252
p ospf network broadcast
p ospf priority 255
p mtu 1500

outer ospf 10
outer-id 10.10.1.14
etwork 10.10.1.14 0.0.0.0 area 0
etwork 10.73.65.64 0.0.0.3 area 0
R86#
nterface FastEthernet0/0
p address 10.73.65.66 255.255.255.252
p ospf network broadcast
p mtu 1500

outer ospf 10
outer-id 10.10.1.86
etwork 10.10.1.86 0.0.0.0 area 0
etwork 10.73.65.64 0.0.0.3 area 0
```

C.

```
R14#
interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip ospf network broadcast
ip ospf priority 0
ip mtu 1400

router ospf 10
router-id 10.10.1.14
network 10.10.1.14 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0
R86#
interface Loopback0
ip address 10.10.1.86 255.255.255.255
```

D.

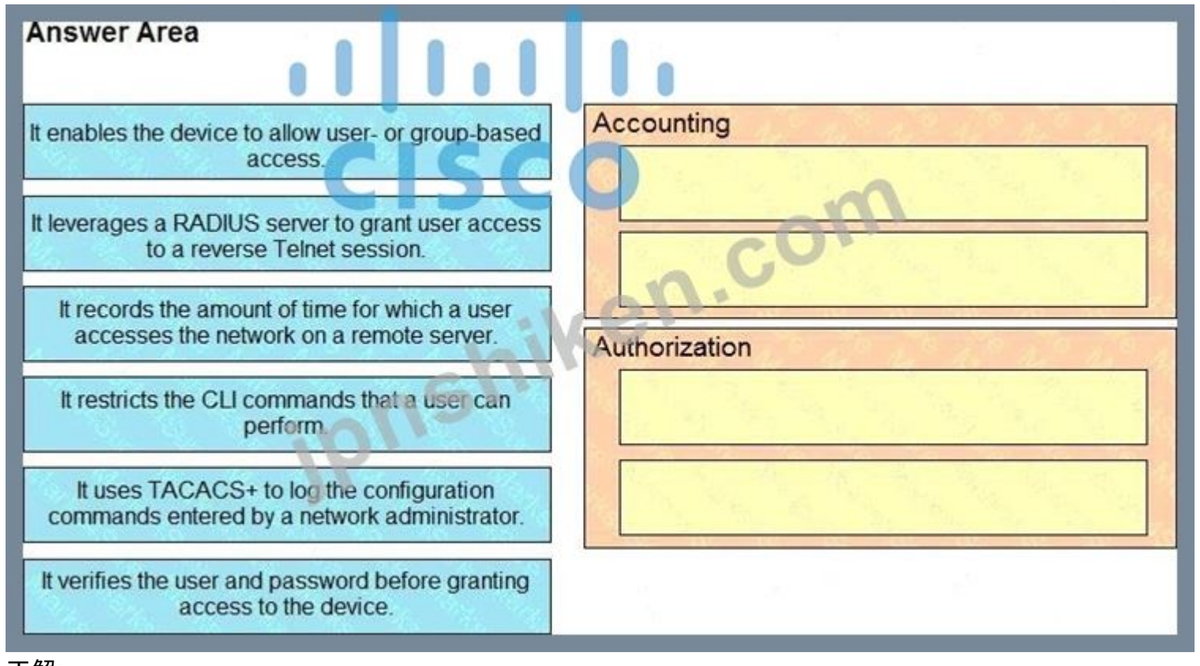
```
R14#
nterface FastEthernet0/0
p address 10.73.65.65 255.255.255.252
p ospf network broadcast
p ospf priority 255
p mtu 1500

outer ospf 10
outer-id 10.10.1.14
etwork 10.10.1.14 0.0.0.0 area 0
etwork 10.73.65.64 0.0.0.3 area 0
R86#
nterface FastEthernet0/0
p address 10.73.65.66 255.255.255.252
p ospf network broadcast
p mtu 1400

outer ospf 10
outer-id 10.10.1.86
etwork 10.10.1.86 0.0.0.0 area 0
```

正解: (正解を表示します)

Option D. OSPF operation depends on area membership, network type, timers, router ID, priority, and whether a DR/BDR election occurs. Cisco CCNA 200-301 v1.1 includes this under IP Connectivity, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. Incorrect choices either use the wrong OSPF role, omit a required adjacency condition, or apply a setting that does not affect the stated behavior. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

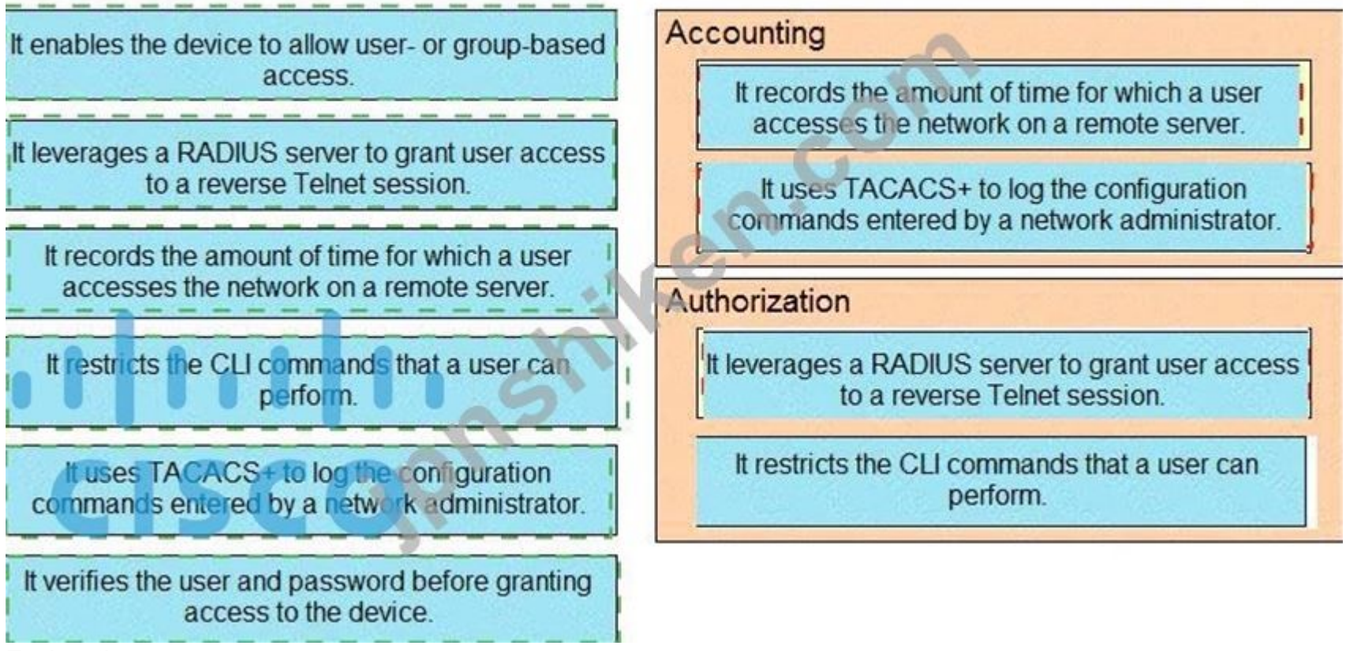
質問: **503**

左側のAAA機能を、右側の対応するAAAセキュリティサービスにドラッグ＆ドロップしてください。すべてのオプションを使用するわけではありません。



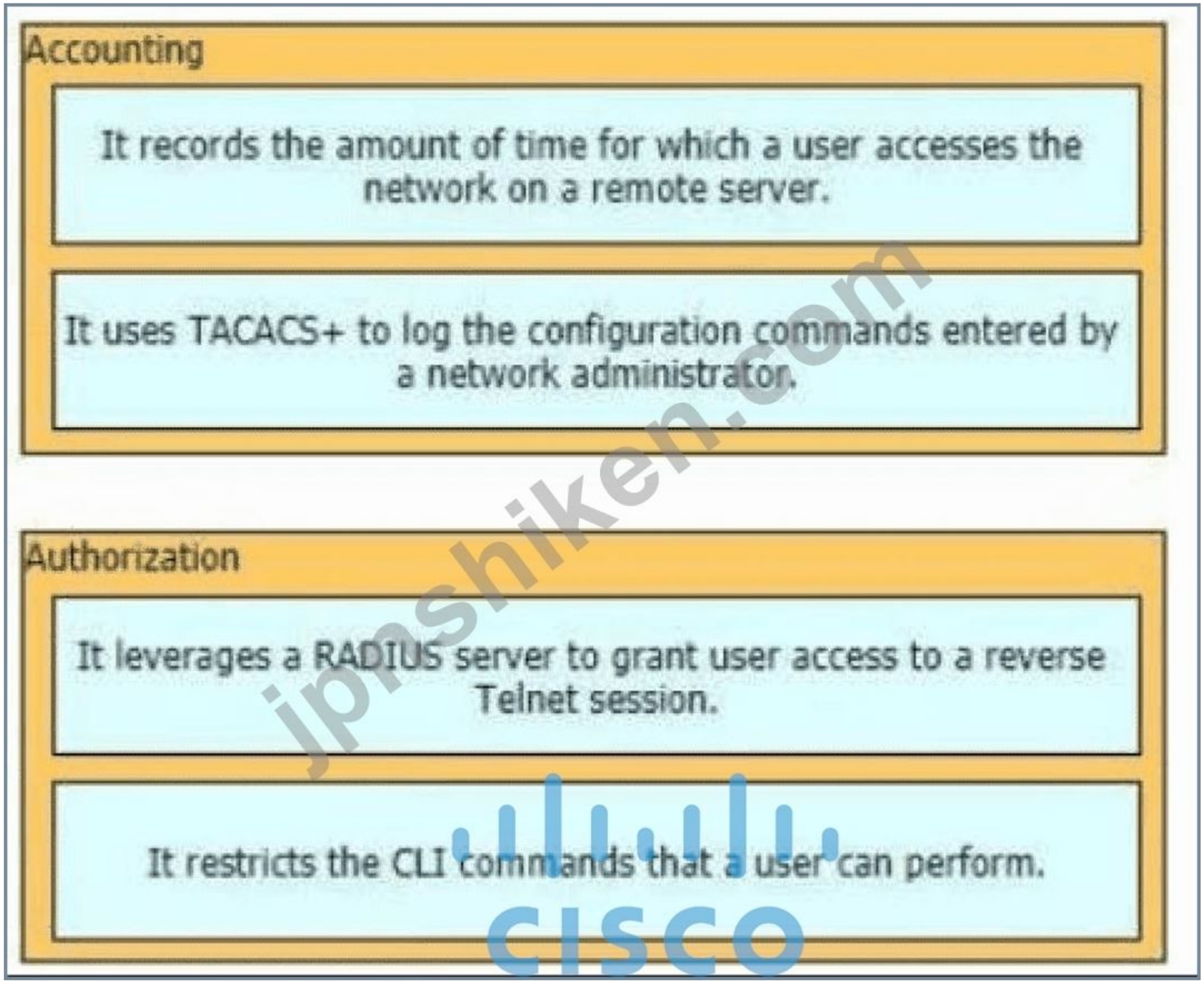
正解:

Answer Area



Explanation:

Cisco CCNA 200-301 v1.1 Security Fundamentals drag-and-drop items test whether each protocol, address type, API action, or infrastructure component is matched to its real function. The correct way to solve these is to classify every item by layer, scope, and operational behavior before matching it. Several distractors are legitimate networking terms, but they are wrong when placed under the wrong protocol family or management model. The retained mapping preserves the Cisco distinctions between TCP and UDP behavior, AAA functions, IPv6 address scopes, device-management approaches, and REST operations. In implementation work, these distinctions matter because applying a feature at the wrong layer or associating a control with the wrong service creates broken configurations and wasted troubleshooting effort. The shown mapping is therefore retained as the verified response.



質問: **504**
エンジニアは、スイッチのデフォルト VLAN に構成されている未使用のポートを保護するよう求められます。
要求を満たす 2 つのステップはどれですか? (2つ選んでください)

A. EtherChannel のポートを構成します。
B. ポートを管理シャットダウンします。
C. ポート タイプをアクセスとして構成し、VLAN 99 に配置します。
D. ポートをトランク ポートとして構成します。
E. Cisco Discovery Protocol を有効にします
正解: **(**正解を表示します**)**
Unused switch ports should not remain active in the default VLAN. The proper hardening approach is to administratively shut them down and move them into an unused access VLAN, often called a parking, black- hole, or unused VLAN. Shutting the port stops an attacker from plugging in and immediately gaining Layer 2 connectivity. Moving the port out of VLAN 1 reduces the impact if someone later enables the port accidentally. EtherChannel is irrelevant because it aggregates links; it does not protect idle user-facing ports.
Trunking unused ports is actively dangerous because it could expose multiple VLANs. CDP can disclose device information and is not a protection method for unused ports. Cisco CCNA v1.1 Network Access and Security Fundamentals overlap here: secure access-layer design includes disabling unused interfaces, avoiding the default VLAN for user access, and limiting unintended Layer 2 exposure. Therefore, B and C are the correct operational steps.

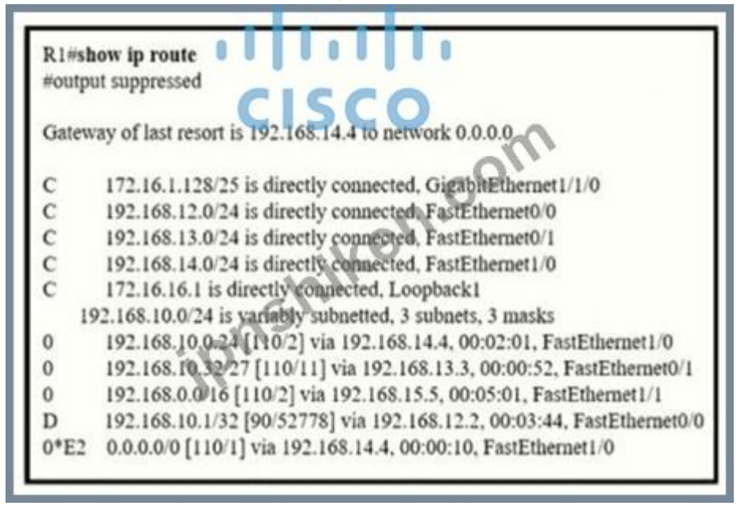
質問: **505**
RFC 1918 アドレス空間が定義されたのはなぜですか?
A. パブリック IPv4 アドレッシングを節約する
B. パブリック IPv6 アドレス空間を保持
C. 重複する IP アドレスのインスタンスを減らす
D. NAT プロトコルをサポート
正解: **A (**コメントを発表する**)**
Use A for this item. RFC 1918 private address space was defined to conserve public IPv4 addresses.
Organizations can reuse private ranges internally and translate at the edge with NAT when Internet access is needed. In Cisco CCNA 200-301 v1.1, Network Fundamentals questions frequently test the practical boundary between similar features: what the feature does, where it is configured, and what problem it is meant to solve. It was not designed to preserve IPv6 space or eliminate overlap between private organizations.
A clean way to validate the answer is to map the wording of the scenario to the actual device function. If the feature supplies addressing, forwarding, authentication, trunking, route selection, or controller communication, the answer must match that function exactly rather than a nearby protocol name.

質問: **506**
多要素認証の主な機能は何ですか？
A. 3つの認証要素を使用してエンドユーザーの権限を識別する
B. 2つの認証要素を使用してエンドユーザーを認証および認可する
C. 2つ以上の認証要素を使用してエンドユーザーの身元を確認する
D. 2つの認証要素を使用してエンドユーザーのアクセス権限を検証します
正解: **(**正解を表示します**)**
Confirming end-user identity using two or more authentication factors. Security questions in CCNA 200-301 v1.1 require matching the control to the threat or access requirement. Authentication proves identity, authorization controls what the user can do, and accounting records activity. Firewalls inspect and permit or deny traffic based on policy, while ACLs match packet fields in a defined order. VPN and IPsec questions require knowing whether the design protects unicast traffic, supports tunneling, or encrypts the original packet. Password and SSH questions depend on IOS behavior, including encrypted secrets, local users, domain names, and cryptographic images. The incorrect choices often use a valid technology in the wrong role or provide weaker protection. The selected answer is the Cisco-consistent control because it directly satisfies the access, confidentiality, or threat-mitigation requirement stated in the question.

質問: **507**
組織のセキュリティプログラムの一環として、物理的なアクセス制御を実施する行動はどれですか？
A. コンソールポートのパスワードを設定する
B. ネットワーク機器で有効化パスワードを設定する
C. リモートロケーションでのシステムログのバックアップ
D. 主要インフラを監視するためのIPカメラの設置
正解: **D** (コメントを発表する)
setting up IP cameras to monitor key infrastructure. Layer 2 switching behavior is driven by VLAN membership, MAC learning, trunk encapsulation, STP state, and EtherChannel negotiation. Cisco switches learn source MAC addresses on ingress, flood unknown unicasts within the same VLAN, and forward known unicasts only out the port associated with the destination MAC address. Trunk and EtherChannel questions must be solved on the logical interface and with the correct negotiation protocol: LACP uses active/passive, PAgP uses desirable/auto, and static mode uses on. STP and PortFast questions depend on whether the port is intended for an endpoint or part of the switched topology. The wrong choices usually apply the correct feature to the wrong port type or violate the required negotiation behavior. Cisco CCNA 200-301 v1.1 emphasizes these details because a single incorrect Layer 2 setting can create loops, VLAN leaks, or failed host connectivity. The selected answer matches Cisco switching operation.

質問: **508**
通常のアクセス ポイント トラフィックを通過させるためにスイッチに接続する WLC ポートはどれですか?
A. 冗長性
B. コンソール
C. 配信システム
D. サービス
正解: (正解を表示します)
The correct response is C. A WLC distribution system port connects to the wired network and carries normal AP and client traffic. This port type is used for data-plane and control-plane connectivity between the controller, APs, and upstream switching infrastructure. For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. Console and service ports are for management access, and a redundancy port is for HA communication. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **509**
展示資料を参照してください。



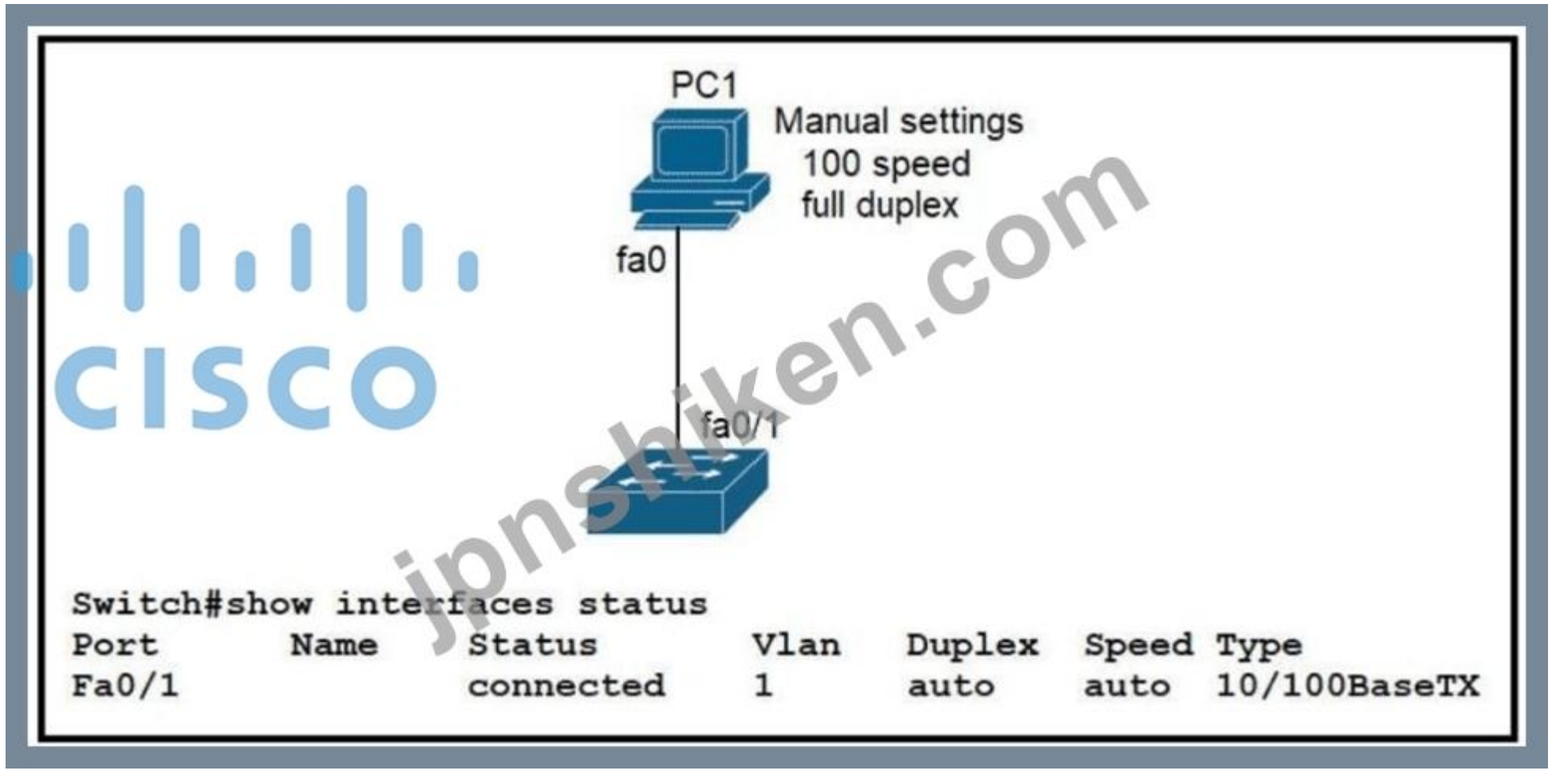
R1が172.161.1宛てのパケットを受信した場合、R1はそのパケットをどのIPアドレスに送信するでしょうか？
A. 192.168.12.2
B. 192.168.13.3
C. 192.168.14.4
D. 192.168.15.5
正解: **C** (コメントを発表する)
192.168.14.4. The scenario should be solved by matching the described behavior to the Cisco feature that actually performs it. Cisco CCNA 200-301 v1.1 includes this topic under Network Fundamentals, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario.
The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The other options are real networking terms or plausible phrases, but they operate at a different layer, solve a different problem, or do not create the outcome described. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **510**
CAPWAP(Control and Provisioning of Wireless Access Points)プロトコルを使用して無線LANコントローラと通信するために、アクセスポイント(AP)はどのモードに設定する必要がありますか？
A. 橋
B. ルート
C. 自律的
D. 軽量
正解: **D** (コメントを発表する)
lightweight. Wireless designs depend on the correct access point mode, WLAN security method, controller function, RF band behavior, and client authentication process. Cisco CCNA 200-301 v1.1 includes this topic under Network Access, so the answer must be validated against normal Cisco device behavior and the operational wording of the scenario. The key is not simply recognizing a familiar acronym; it is identifying what the feature does, where it is configured, and what result it produces. The wrong options confuse authentication with encryption, autonomous behavior with controller-based operation, or management functions with client data forwarding. In a real network, selecting the wrong option would either leave the feature nonfunctional, create a forwarding or security gap, or send troubleshooting in the wrong direction. The selected answer is the only one that matches the stated requirement and the way Cisco switching, routing, services, security, wireless, or automation functions are expected to operate. This is why the verified answer remains the best technical choice for the question.

質問: **511**
ポートが err-disabled ステートになる原因は何ですか?
A. レイテンシー
B. ポートセキュリティ違反
C. ポートで発行されたシャットダウン コマンド
D. ポートに何も接続されていません
正解: **B** (コメントを発表する)
The verified answer is B. A port security violation can place a switchport into the err-disabled state. In shutdown violation mode, the switch disables the interface to stop unauthorized MAC address use. Cisco CCNA 200-301 v1.1 places this skill in Network Access, where the exam expects a working understanding of how the feature behaves on real Cisco networks, not just a memorized command. Latency, an administratively shut interface, or an unplugged cable do not describe the err-disable trigger in the question. In production, this distinction matters because a misapplied command or design choice usually creates an outage, a security gap, or unnecessary troubleshooting noise. The correct choice matches the control-plane, data-plane, wireless, security, or services behaviour described in the scenario and should be preferred over options that merely sound related.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:
JPNshiken」

質問: **512**
展示資料を参照してください。



PC1とスイッチ間のリンクは確立されていますが、パフォーマンスが低下しています。どのインターフェースの状態がパフォーマンスの問題を引き起こしているのでしょうか？
A. インターフェースでデュプレックスの不一致が発生しています
B. スイッチインターフェースの光ファイバーに問題があります。
C. インターフェースの速度に不一致があります。
D. インターフェースの型が一致しません
正解: **(**正解を表示します**)**
There is a duplex mismatch on the interface. The answer follows directly from normal Cisco device behavior and the wording of the scenario. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the exam expects engineers to recognize the device behavior that actually produces the required outcome. The question is best solved by reading the operational clue rather than choosing a familiar acronym. The other choices are either adjacent technologies, wrong-layer functions, or settings that would not produce the stated result. In a production network, the wrong choice would normally create an outage, leave a management or security gap, or send troubleshooting toward the wrong subsystem. The selected answer is the one that matches the control-plane, data-plane, wireless, security, services, or automation mechanism described in the question. That is why it remains the verified answer for this item.

質問: **513**

RESTベースのAPIによって実行されるアクションに適したHTTPメソッドはどれですか？(2つ選択してください。)
A. 削除
B. リダイレクト
C. POST
D. 取得
E. PUT
正解: (正解を表示します)
Answer C,D is correct: C. POST; D. GET. Automation questions require recognizing controllers, APIs, data structures, HTTP methods, and the split between policy/control and forwarding. Cisco CCNA 200-301 v1.1 includes this under Automation and Programmability, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Distractors mix data-plane work with controller responsibilities or confuse REST method names and JSON syntax. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco- consistent behavior for this item.

質問: **514**
展示資料を参照してください。

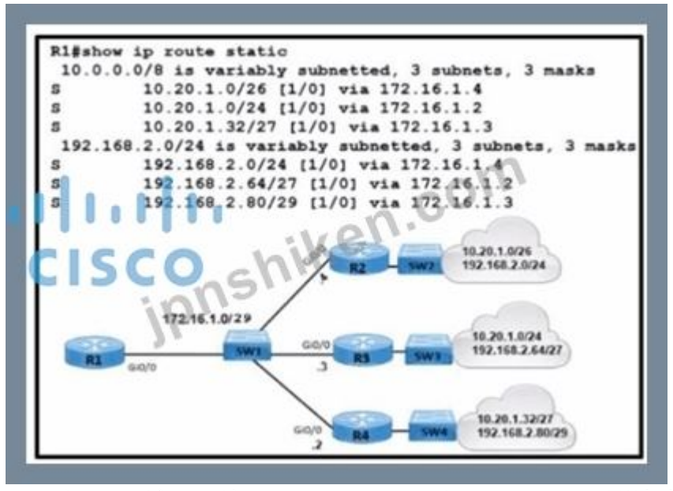
```
cisco_ospf_vrf {"R1 default":
    ensure => 'present',
    auto_cost => '100',
}
```

出力にはどのような構成が表されていますか？
A. Ansible
B. JSON
C. Chef
D. Puppet
正解: (正解を表示します)
The represented configuration is Puppet. Puppet configuration commonly uses manifests written in Puppet ' s declarative language, and the syntax is different from JSON, Ansible playbooks, or Chef recipes. Ansible usually uses YAML playbooks and tasks. JSON is a data encoding format with braces, name-value pairs, arrays, and strict syntax rules. Chef uses recipes and cookbooks and is Ruby-oriented. Puppet is known for declarative resource definitions that describe the desired state of managed nodes. Cisco CCNA 200-301 v1.1 Automation and Programmability does not require a deep Puppet administration skill set, but it does expect recognition of major configuration-management tools and their basic characteristics. When the exhibit shows Puppet-style resources/manifests rather than a JSON object or Ansible YAML structure, the correct classification is Puppet. The verified answer is D.

質問: **515**
機械学習はネットワークセキュリティにどのような利点をもたらしますか？
A. リアルタイムの脅威検出を改善します
B. パスワードの複雑性要件を強制します
C. ファイアウォールルールセットを管理します
D. VPNアクセス権限を制御します
正解: (正解を表示します)

It improves real-time threat detection. Security questions in CCNA 200-301 v1.1 require matching the control to the threat or access requirement. Authentication proves identity, authorization controls what the user can do, and accounting records activity. Firewalls inspect and permit or deny traffic based on policy, while ACLs match packet fields in a defined order. VPN and IPsec questions require knowing whether the design protects unicast traffic, supports tunneling, or encrypts the original packet. Password and SSH questions depend on IOS behavior, including encrypted secrets, local users, domain names, and cryptographic images. The incorrect choices often use a valid technology in the wrong role or provide weaker protection. The selected answer is the Cisco-consistent control because it directly satisfies the access, confidentiality, or threat- mitigation requirement stated in the question.

質問: **516**
重複しない Wi-Fi チャネルの要件は何ですか?
A. 異なるセキュリティ設定
B. 不連続な周波数範囲
C. 異なる伝送速度
D. 一意の SSID
正解: **(**正解を表示します**)**
discontinuous frequency ranges. Wireless design and security require separating AP mode, WLAN identity, RF behavior, authentication, and encryption. Cisco CCNA 200-301 v1.1 includes this under Network Access, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The distractors confuse wireless standards, security mechanisms, controller settings, or RF design practices. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

質問: **517**
展示資料を参照してください。


ルーターR1がIPアドレス192.168.2.86と10.20.1.50に到達するための正しいネクストホップは何ですか？
A. 172.16.1.4
B. 172.16.1.1
C. 172.16.1.2
D. 172.16.1.3
正解: **(**正解を表示します**)**

172.16.1.3. Cisco routing logic is deterministic: a router first matches the most specific destination prefix, then uses administrative distance when competing route sources advertise the same prefix, and finally evaluates the protocol metric when multiple paths remain inside the same routing protocol. First-hop redundancy protocols add a separate default-gateway resiliency function for hosts on a LAN. The other choices in this question either point to the wrong route-selection rule, confuse a protocol metric with administrative distance, or apply a Layer 2 concept where a Layer 3 forwarding decision is required. In production, that mistake would create blackholing, asymmetric routing, or a backup path that never activates.
Cisco CCNA 200-301 v1.1 tests this because route selection is fundamental to troubleshooting reachability.
The selected answer matches the behavior Cisco routers use when forwarding traffic or maintaining gateway redundancy.

質問: **518**
SSIDで使用できる文字の最大長はどれくらいですか？
A. 16
B. 32
C. 48
D. 64
正解: **(**正解を表示します**)**
32. Cisco wireless design separates RF behavior, client authentication, encryption, AP operating mode, and controller management. A WLC centralizes WLAN configuration and AP control, while lightweight APs use CAPWAP to register and exchange control/data information with the controller. Security choices such as WPA2/AES and WPA3/SAE are not interchangeable with older mechanisms such as WEP, TKIP, or RC4. RF questions also depend on channel planning: adjacent cells should avoid overlapping channels, and 5-GHz preference features reduce congestion in the 2.4-GHz band. The incorrect options generally confuse AP mode, authentication, encryption, or controller responsibilities. Cisco CCNA 200-301 v1.1 includes these items because wireless failures often come from using the right-looking feature in the wrong part of the WLAN design. The selected answer is the Cisco-consistent configuration or behavior for this wireless scenario.

質問: **519**
10GBase-SRインターフェースと10GBase-LRインターフェースに共通する特性はどれですか？
A. どちらも伝送に光ファイバーケーブル媒体を必要とします。
B. どちらも伝送にUTPケーブル媒体を必要とします。
C. どちらもシングルモードファイバーを使用しています。
D. 両方ともマルチモードファイバータイプを使用しています。
正解: **(**正解を表示します**)**
Both require fiber cable media for transmission.. Network fundamentals questions require recognizing address scope, media type, connector form factor, topology, and cloud or private addressing behavior. Cisco CCNA
200-301 v1.1 includes this under Network Fundamentals, where the expected skill is to identify the feature that actually creates the observed behavior or meets the configuration goal. The wording usually contains the decisive clue: a prefix length, a VLAN role, a protocol version, a wireless security standard, or a management- plane function. The incorrect choices may be plausible terms, but they do not match the scope, medium, or topology described. In an operational network, choosing the wrong option would typically cause failed connectivity, insecure management, poor wireless behavior, or incorrect forwarding. The selected answer matches the Cisco configuration model and is retained as the verified answer.

質問: **520**
クライアントが同じ SSID のアクセス ポイント間をローミングするときに送信される 802.11 管理フレーム タイプはどれですか?
A. 再関連付けリクエスト
B. プローブ要求
C. 認証リクエスト
D. アソシエーション リクエスト

正解: (正解を表示します)
The correct response is A. A client roaming between APs on the same SSID sends a reassociation request.
The frame tells the new AP that the client was previously associated elsewhere and is moving within the ESS.
For Cisco CCNA 200-301 v1.1, the important point is the mechanism, not a generic description of the technology. Probe requests discover networks, authentication requests start 802.11 authentication, and association requests are used for an initial association rather than roaming reassociation. When this appears in a network, the symptom normally confirms the answer: the route installed, the state selected, the packet forwarded, the wireless client behaviour, or the management workflow will follow this rule. That is why this answer is the best fit for the scenario and not just a plausible networking term.

質問: **521**
SDNネットワークにおいて、制御プレーンとデータプレーンを分離することの利点は何ですか？
A. ネットワーク全体の複雑さを軽減します
B. データクエリを制御プレーンに制限する
C. コストを削減します
D. 仮想マシンの作成をデータプレーンにオフロードします
正解: (正解を表示します)
decreases overall network complexity. Switching questions depend on MAC learning, VLAN membership, trunking, STP election, and EtherChannel behavior. Cisco CCNA 200-301 v1.1 includes this under Automation and Programmability, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. Wrong answers misapply a Layer 2 rule or configure the wrong logical interface. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **522**
デバッグ プロセスがオンになっているデバイスによって異常に多数の syslog メッセージが生成された場合に、他のメッセージを許可しながらデバッグ メッセージが syslog 経由で送信されるのを防ぐアクションはどれですか。
A. アクセス リストを使用して syslog メッセージをフィルタリングします。
B. グローバル コンフィギュレーション モードでログ モニターをオフにします。
C. コンソールへのログ記録を無効にします。
D. ログ トラップの重大度レベルを情報に設定します。
正解: (正解を表示します)
Set the logging trap severity level to informational.. IP services questions are about the supporting protocols that make a network manageable and usable: DHCP supplies addressing information, DNS resolves names, NAT translates address spaces, NTP synchronizes time, syslog records events, SNMP monitors devices, and QoS classifies or prioritizes traffic. Cisco IOS commands are precise; a similar-looking command can configure a client, a relay, a pool, or a server role depending on context. The incorrect options typically name real services but solve a different operational problem. Cisco CCNA 200-301 v1.1 includes these topics because production networks fail just as often from broken services as from broken routing. The chosen answer is the one that performs the exact function in the scenario, whether that is file transfer, address assignment, logging level selection, monitoring security, or traffic treatment.

質問: **523**
QoSにおいてネットワークトラフィックを分類する目的は何ですか？
A. クラスに応じてトラフィックを処理します
B. 特定の処理を受けるトラフィックの種類を識別します
C. パケットのクラス識別子をパケットヘッダーの専用フィールドに書き込みます
D. ネットワークデバイス上でトラフィックマッチングルールを設定します
正解: **B** (コメントを発表する)

identifies the type of traffic that will receive a particular treatment. IP services questions require matching the protocol or service to its exact role in monitoring, addressing, traffic treatment, or application access. Cisco CCNA 200-301 v1.1 includes this under IP Services, where the expected skill is selecting the feature that actually produces the requested network behavior. The wording normally gives the clue: protocol family, address scope, trunk state, route preference, security mode, API method, or controller role. The wrong choices name real services but solve a different operational problem. In production, choosing the wrong option would typically cause failed client access, a broken route, insecure management, or an automation workflow that targets the wrong interface. The selected answer is the Cisco-consistent behavior for this item.

質問: **524**
SDNコントローラとネットワーク上で動作するアプリケーション間の通信には、どの技術が適していますか？
A. REST API
B. OpenFlow
C. 南向きAPI
D. NETCONF
正解: **A (**コメントを発表する**)**
REST API. Automation and programmability questions test whether the engineer can separate data format, transport method, controller role, and API direction. REST commonly uses HTTP methods such as GET, POST, PUT, and DELETE. JSON represents structured data with objects, arrays, strings, numbers, Booleans, and null values. Northbound APIs allow applications to interact with a controller, while southbound APIs allow the controller to communicate with network devices. NETCONF and RESTCONF are configuration
/management protocols, not generic forwarding behaviors. The incorrect choices often mix controller-to- device communication with application-to-controller communication or confuse a data format with a protocol.
Cisco CCNA 200-301 v1.1 includes this area because modern network operations increasingly rely on APIs and centralized controllers. The selected answer matches the correct API direction, data representation, or HTTP operation for the scenario.

質問: **525**
1000BASE-LX/LH と 1000BASE-ZX インターフェースの違いは何ですか?
A. 1000BASE-ZX は 1000km までのリンクでサポートされ、1000BASE-LX/LH は 70km までのリンクで動作します。
B. 1000BASE-LX/LH はマルチモードおよびシングルモード ファイバーと相互運用し、10008ASE-ZX はマルチモードの調整パッチ ケーブルが必要です。
C. 1000BASE-LX/LH は 10km までのリンクでサポートされ、1000BASE-ZX は 10km までのリンクで動作します。
70キロ
D. 1000BASE-ZX は、マルチモード ファイバーを介してデュアルレート 100M/1G 10Km SFP と相互運用します。
1000BASE-LX/LH はシングルレートのみ対応。
正解: **(**正解を表示します**)**
1000BASE-LX/LH is supported on links up to 10km, and 1000BASE-ZX operates over links up to 70 km.
The answer follows from normal Cisco device behavior and the operating clue in the scenario. Cisco CCNA
200-301 v1.1 includes this under Network Fundamentals, where the expected skill is identifying the mechanism that actually satisfies the scenario. The wording usually gives the decisive clue: a protocol number, a route prefix, a control-plane role, a wireless security method, or a management command. The other options use adjacent terms, wrong-layer behavior, or configuration that would not produce the requested result. In a real network, selecting the wrong option would usually produce a failed adjacency, broken client connectivity, insecure management access, or an incorrect forwarding path. The selected answer matches the Cisco behavior and configuration model required by the question, so it is retained as the verified answer for this item.

有効的な**200-301J**問題集はJPNTest.com提供され、**200-301J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-301J**試験問題集を提供します。JPNTest.com 200-301J試験問題集はもう更新されました。ここで**200-301J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-301J-mondaishu　**813**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」