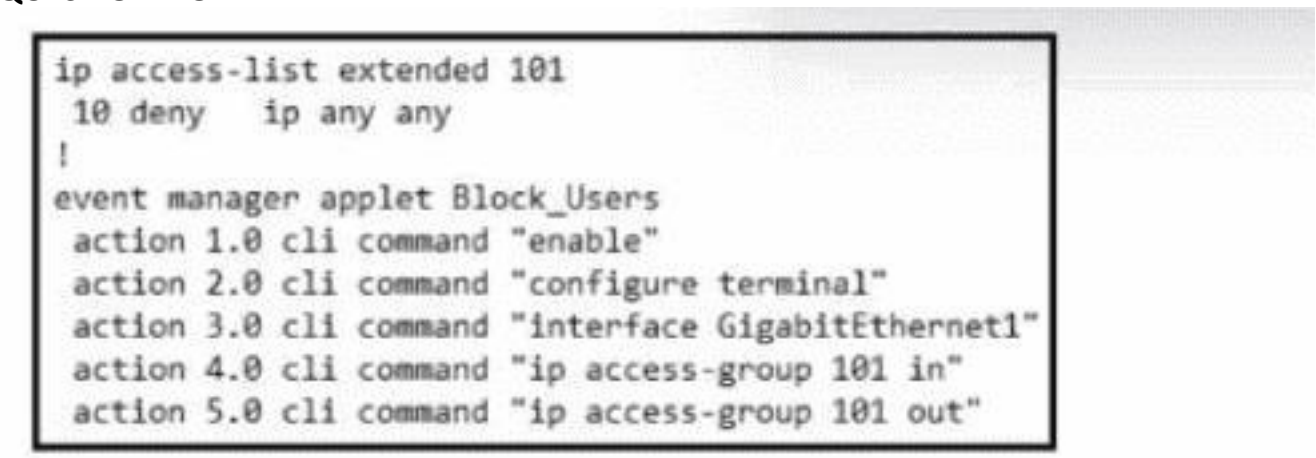
**Exam** : **350-401J**

**Title** : Implementing and Operating Cisco Enterprise Network Core Technologies (350-401日本語版)

**Vendor** : Cisco

**Version** : DEMO

**QUESTION NO: 1**




展示を参照してください。エンジニアがアクセスリストを適用するためのEEMスクリプトを作成します。スクリプトを完成させるには、どのステートメントを追加する必要がありますか？

**A.** イベントなし

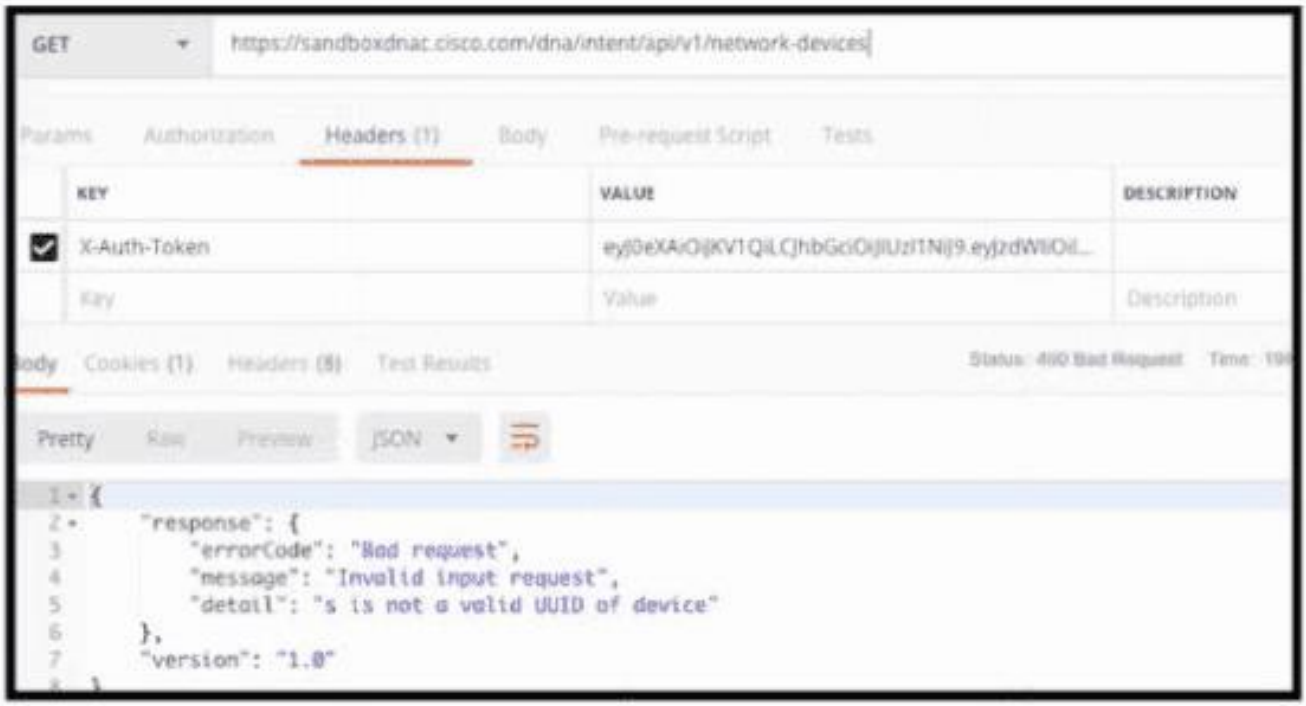
**B.** action 6.0 cli command "ip access-list extended 101"

**C.** action 2.1 cli command "ip access-list extended 101"

**D.** action 3.1 cli command "ip access-list extended 101"

***Answer:*** A

**QUESTION NO: 2**



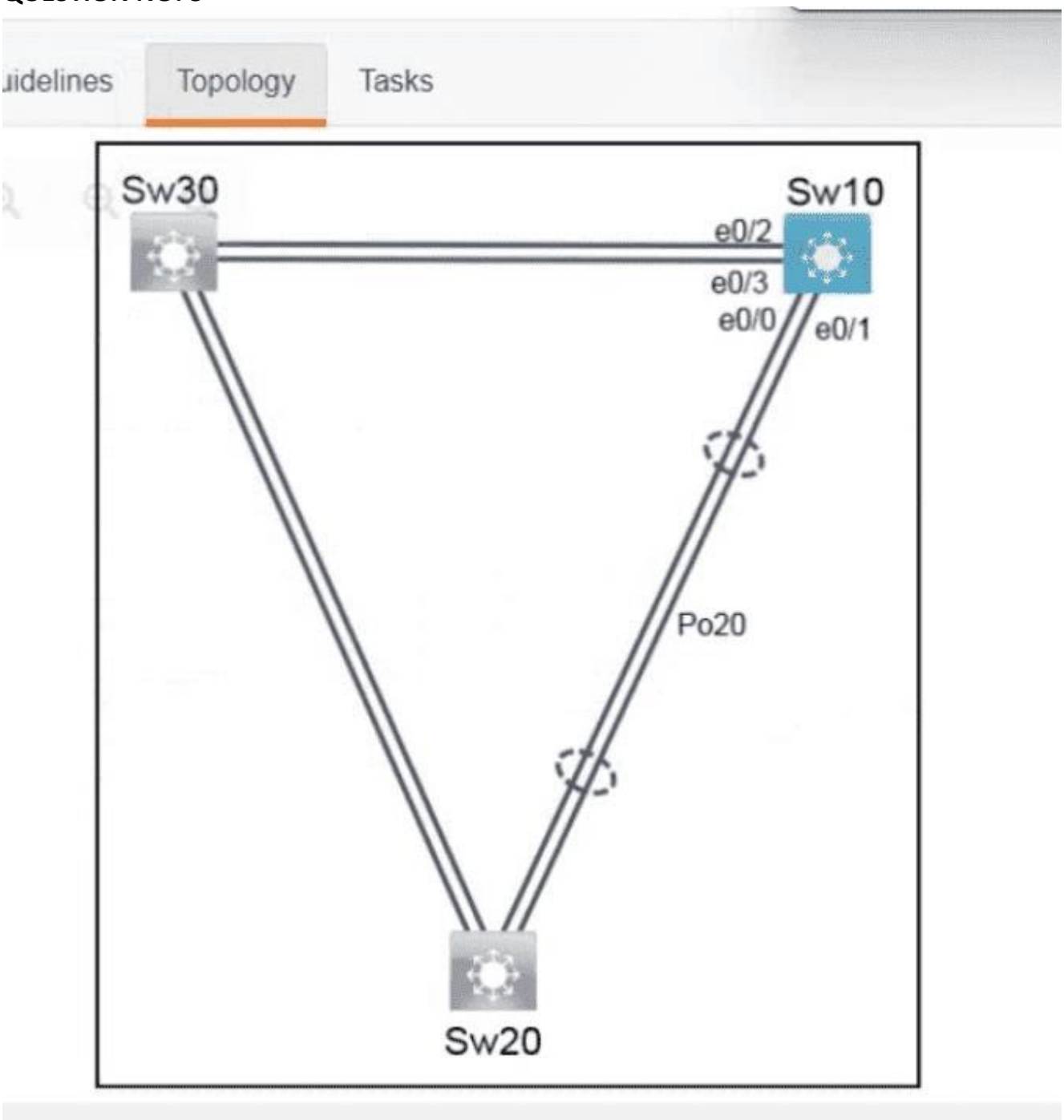

添付資料を参照してください。POSTMAN は、Cisco Catalyst Center(旧 DNA Center)APIからネットワークデバイス情報を取得しようとしていることを示しています。問題は何でしょうか？

**A.** トークンの有効期限が切れました

**B.** URI文字列が正しくありません

**C.** 認証に失敗しました
**D.** JSONペイロードに不正なUUIDが含まれています
***Answer:*** D

**QUESTION NO: 3**



Complete the tasks below by making changes to Sw10 only. No access is provided to Sw20 or Sw30.

**Task 1**

Sw20 is actively attempting to negotiate an 802.1 trunking EtherChannel with Sw10 using LACP, but the channel is not functional. Resolve the issues on Sw10.

**Task 2**

Modify the spanning tree configuration to ensure that Sw10 is always the root for VLAN 20.

***Answer:***

See the solution below in Explanation:

Explanation:

Solution:

Sw10

config t

no int po20

int et0/0

channel-group 20 mode active

no shut

spanning-tree vlan 20 pri 0

wr

Verification:-

```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------------
------------
20     Po20(SU)         LACP      Et0/0(P)
```

**QUESTION NO: 4**

スイッチ ポートで MAC 認証バイパス機能を使用する必要があるのはいつですか?

**A.** 認証が必要であるが、接続されたホストが802.1Xをサポートしていない場合

**B.**
接続されたホストが802.1Xをサポートしており、ユーザー資格情報ではなくMACアドレスに基づいて認証する必要がある場合
**C.** MACアドレスに基づいて特定のホストの認証をバイパスする必要がある場合
**D.** 接続されたホストが制限付き802.1Xをサポートしている場合
***Answer:*** A

**QUESTION NO: 5**
ワイヤレスクライアントがローミングするかどうかを決定するデバイスはどれですか？
**A.**ワイヤレスクライアント
**B.**無線LANコントローラー
**C.**アクセスポイント
**D.**WCSロケーションサーバー
***Answer:*** A

**QUESTION NO: 6**
顧客は、異なるパスワードを使用して IoT デバイスを認証するために単一の SSID を使用したいと考えています。この要件を満たすには、Cisco ISE と組み合わせてどのレイヤー 2 セキュリティ タイプを設定する必要がありますか?
**A.** アイデンティティPSK
**B.** 高速遷移
**C.** 中央Web認証
**D.** Cisco 集中キー管理
***Answer:*** A

**QUESTION NO: 7**
基本的なAPI認証において、スニファ攻撃から認証情報を保護するセキュリティオプションはどれですか？
**A.** クライアントとサーバー間のVPN接続
**B.** 通信にはTLSまたはSSLを使用します。
**C.** APIを認証するためのAAAサービス
**D.** 次世代ファイアウォール
***Answer:*** B
Explanation:
The correct answer is B. TLS or SSL for communication.
In basic API authentication, credentials (such as username and password) are often transmitted using Base64 encoding, which is not encrypted. This makes them vulnerable to sniffer (packet capture) attacks if sent over an unencrypted channel.
* TLS (Transport Layer Security) and its predecessor SSL provide encryption of the communication channel.
* This ensures that even if packets are captured, the credentials remain confidential and unreadable.
* Cisco documentation emphasizes that APIs (RESTCONF, HTTP-based APIs) should use HTTPS (HTTP over TLS) to secure credentials in transit.

* A. VPN connection between client and server While a VPN encrypts traffic, it is not specifically required for API authentication security. The standard and expected method is TLS/HTTPS.
* C. AAA services to authenticate the API AAA controls who can access, but it does not encrypt credentials in transit.
* D. next-generation firewall A firewall provides traffic filtering and threat protection but does not directly secure credential transmission in basic API authentication.
* Basic Authentication = NOT secure by itself
* Always pair it with HTTPS (TLS encryption)
Rule to remember:
If credentials travel over the network # encrypt with TLS

**QUESTION NO: 8**
Cisco SD-Access 展開では、どのノードに VXLAN カプセル化のサポートが必要ですか?
**A.** コアノード
**B.** 配布ノード
**C.** 境界ノード
**D.** 集約ノード
***Answer:*** C

**QUESTION NO: 9**
ある企業が最近、NETCONFの代わりにRESTCONFを使用することを決定しました。多くのNETCONFスクリプトには、<edit-config>（create）という操作が含まれています。これらのステートメントを置き換えるには、どのRESTCONF操作を使用する必要がありますか？
**A.** CREATE
**B.** POST
**C.** GET
**D.** PUT
***Answer:*** B

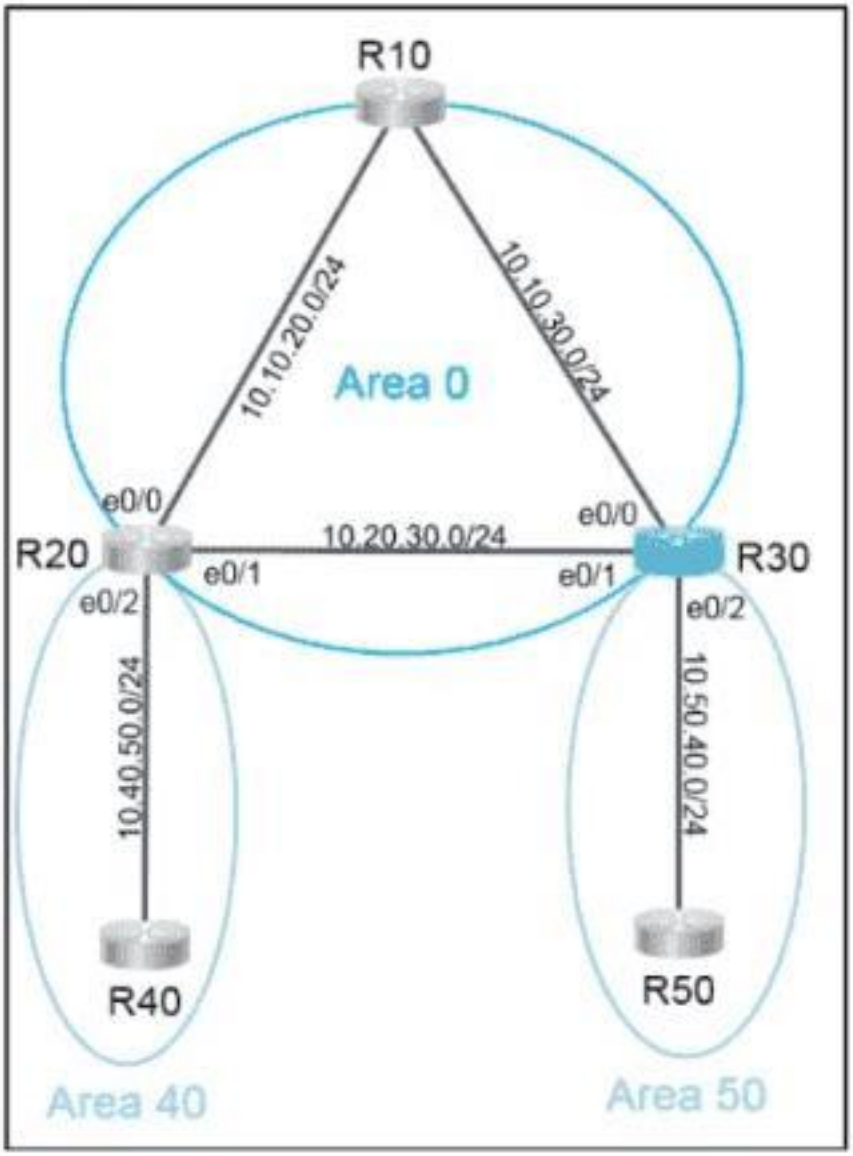
**QUESTION NO: 10**
OSPFとEIGRPの違いは何ですか？
**A.** OSPFはIPプロトコル番号88を使用します。EIGRPはIPプロトコル番号89を使用します。
**B.** OSPF はデフォルトのハロータイマーとして 5 秒を使用します。EIGRP はデフォルトのハロータイマーとして 10 秒を使用します。
**C.** OSPF は管理距離 115 を使用します。EIGRP は管理距離 160 を使用します。
**D.** OSPF はマルチキャストアドレス 224.0.0.5 と 224.0.0.6 を使用します。EIGRP はマルチキャストアドレス 224.0.0.10 を使用します。
***Answer:*** D
Explanation:
The correct answer is D.
OSPF and EIGRP use different multicast addresses for exchanging routing information:
* OSPF uses:

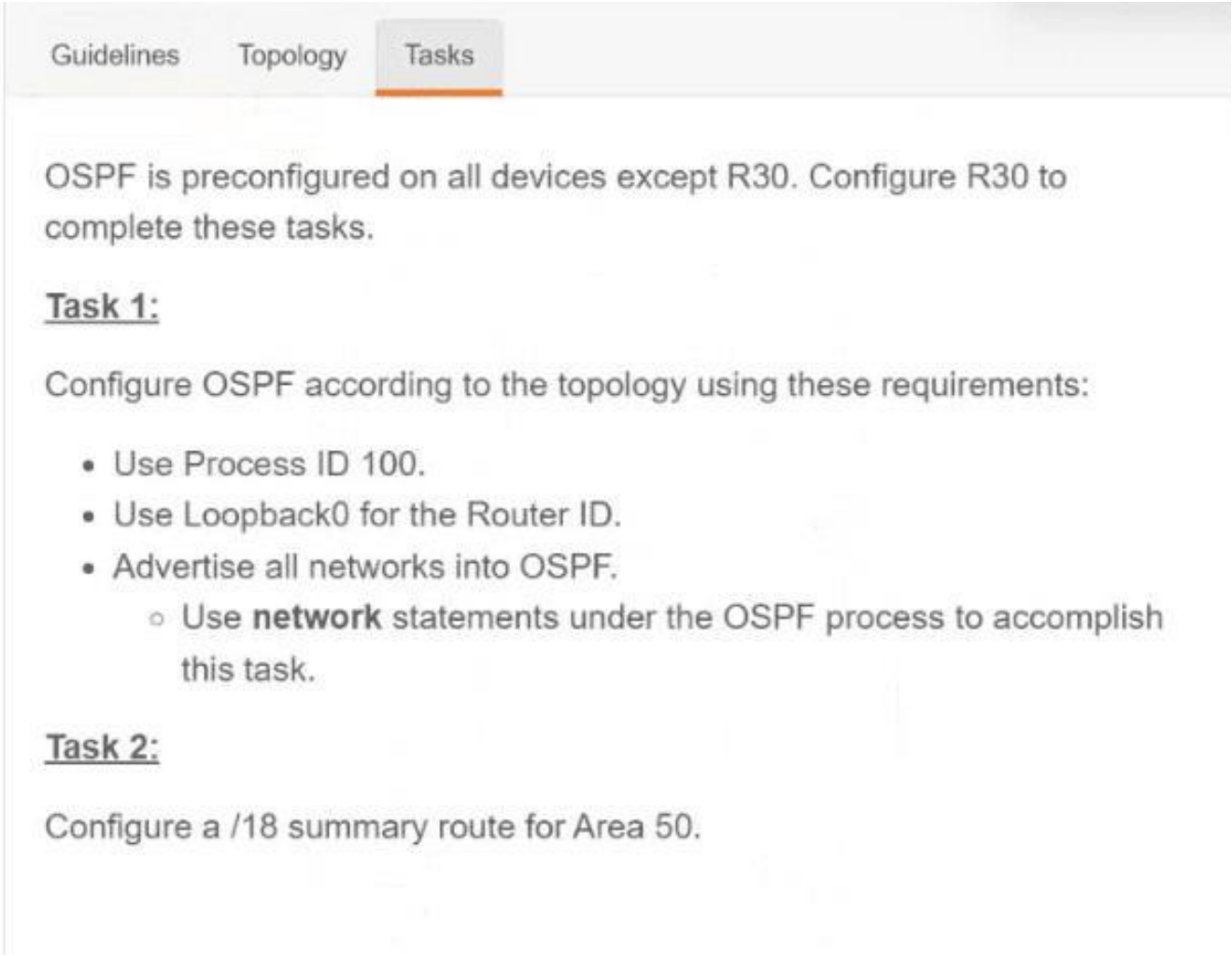
* 224.0.0.5 # AllSPFRouters
* 224.0.0.6 # AllDRouters
* EIGRP uses:
* 224.0.0.10
This is a well-known operational difference between the two protocols and is commonly tested in Cisco ENCOR.
* A. OSPF uses IP protocol number 88. EIGRP uses IP protocol number 89. This is reversed.
* EIGRP = IP protocol 88
* OSPF = IP protocol 89
* B. OSPF uses a default hello timer of 5 seconds. EIGRP uses a default hello timer of 10 seconds. This is incorrect.
* On most broadcast and point-to-point networks, OSPF default hello = 10 seconds
* EIGRP default hello = 5 seconds on high-speed links
* C. OSPF uses an administrative distance of 115. EIGRP uses an administrative distance of 160. This is also incorrect.
* OSPF AD = 110
* EIGRP internal AD = 90
* EIGRP external AD = 170
Memorize these protocol identifiers:
* OSPF
* Protocol number: 89
* Multicast: 224.0.0.5 / 224.0.0.6
* EIGRP
* Protocol number: 88
* Multicast: 224.0.0.10

**QUESTION NO: 11**
高密度ワイヤレス環境で各ユーザーの帯域幅を増やすには、どのソリューションを使用する必要がありますか?
**A.** アンテナのサイズを大きくします。
**B.** 各 AP のセルのサイズを大きくします。
**C.** 必須の最小データ レートを上げます。
**D.** 送信電力を増加させます。
***Answer:*** C

**QUESTION NO: 12**

Topology Tasks





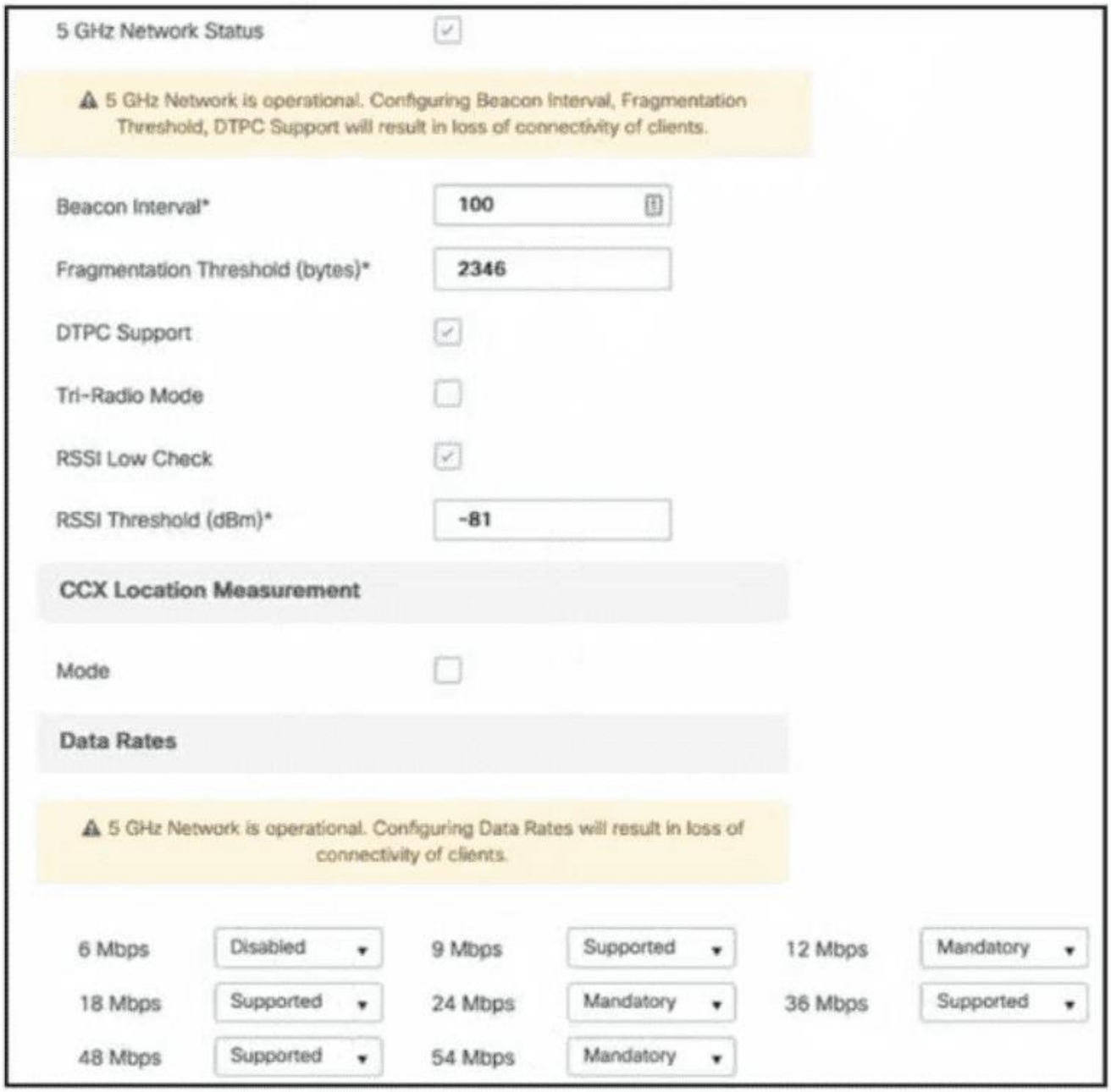

***Answer:***
See the solution below in Explanation:
Explanation:
Solution:
R30
Config t
router ospf 100
router-id 10.0.1.30
int ran lo0 , e0/0-1
ip ospf 100 a 0
exit
int et0/2
ip ospf 100 a 50
exit
router ospf 30
area 50 range 10.10.0.0 255.255.192.0
area 50 range 10.50.0.0 255.255.192.0
end
wr

**QUESTION NO: 13**

データ モデリング言語を使用して API クライアント
アプリケーションを開発する利点は何ですか?
**A.** 互換性の向上
**B.** 機能拡張が容易
**C.** より強力なセキュリティ特性
**D.** リソース要件が低い
***Answer:*** B

**QUESTION NO: 14**
Cisco DNA Center サウスバウンド API の機能は何ですか?
**A.** ServiceNow などの 10 個の ITSM サービスに接続します。
**B.** 管理者が Cisco DNA Center への API 呼び出しを行うことを許可します。
**C.** アラートがトリガーされると、Cisco DNA CenterからWebhookを送信します。
**D.** Cisco DNA Center
からシスコ以外のデバイスを管理するためのサポートが追加されました。
***Answer:*** D

**QUESTION NO: 15**




展示を参照してください。多くのワイヤレスクライアントがマルチキャストオーディオを確実に受信できないという報告が顧客から寄せられています。
この問題を解決するには、どのようなアクションを実行すればよいですか?

**A.** 24 Mbps および 54 Mbps のデータ レートを [サポート] に設定します。
**B.** RSSIしきい値を-67dBmに設定します。
**C.** 断片化しきい値を1250バイトに設定する
**D.** RSSI Low チェックを無効にします。
***Answer:*** A

**QUESTION NO: 16**
Cisco SD-Access ソリューションでは、拡張ノードが単一のエッジ ノードに接続するためにどのプロトコルが使用されますか?

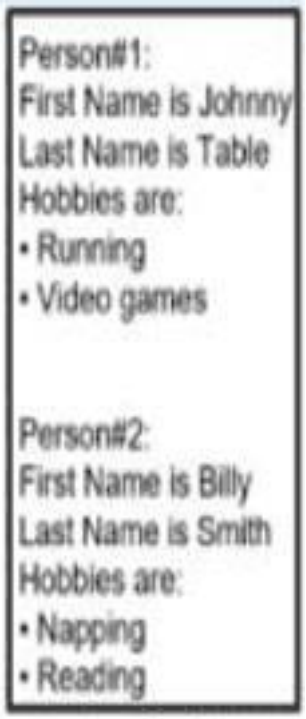
**A.** VXIAN
**B.** IS-IS

**C.** 802.1
**D.** CTS
***Answer:*** C

**QUESTION NO: 17**
無線信号の電力を 1 ミリワットを基準にして測定する単位はどれですか?
**A.** dBi
**B.** mW
**C.** dBw
**D.** dBm
***Answer:*** D

**QUESTION NO: 18**
管理者がトラブルシューティングに使用する pcap ファイルを生成できる AP モードはどれですか?
**A.** Sniffer
**B.** Local
**C.** H-REAP
**D.** Monitor
***Answer:*** A

**QUESTION NO: 19**
展示品を参照してください。




このデータからどの JSON 構文が派生されますか?

{[{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Hobbies': 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Hobbies': 'Reading'}]}

{'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': 'Running', 'Video games'}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': 'Napping', 'Reading'}]}

{'Person': [{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}

{[{'First Name': 'Johnny', 'Last Name': 'Table', 'Hobbies': ['Running', 'Video games']}, {'First Name': 'Billy', 'Last Name': 'Smith', 'Hobbies': ['Napping', 'Reading']}]}

**A.** オプションA
**B.** オプションB
**C.** オプションC
**D.** オプションD
***Answer:*** C

**QUESTION NO: 20**
ワイヤレス管理者は、ISE を外部 RADIUS サーバとして使用する新しい Web 認証企業 SSID を作成する必要があります。認証が完了したら、ゲスト VLAN を指定する必要があります。
ISE サーバーがゲスト VLAN を指定できるようにするには、どのアクションを実行する必要がありますか?
**A.** RADIUS プロファイリングを設定します。
**B.** AAA ポリシー名を設定します。
**C.** ネットワーク アクセス制御状態を有効にします。
**D.** AAA オーバーライドを有効にします。
***Answer:*** D

**QUESTION NO: 21**
サイト間ワイヤレス接続にはどのタイプのアンテナを使用すればよいですか?
**A.** 全方向
**B.** パッチ
**C.** 双極子
**D.** 八木
***Answer:*** D

**QUESTION NO: 22**
インターネット エッジで次世代ファイアウォールを使用することで導入される 2 つの新しいセキュリティ機能はどれですか?
（2つ選択してください。）
**A.** 統合侵入防止
**B.** VPN
**C.** アプリケーションレベルの検査
**D.** ステートフルパケットインスペクション
**E.** NAT
***Answer:*** A C

**QUESTION NO: 23**

MACsec の特徴は何ですか?
**A.** 8021AEは暗号化と認証サービスを提供する
**B.**
8021AEは、成功した802IXセッションからのマスターセッションキーに基づいて暗号化キーをネゴシエートするMKAプロトコルを使用して、ホストとスイッチの間にあります。
**C.** 802.1AEは、Diffie-Hellmanアルゴリズム（匿名暗号化モード）で生成されたキーを使用して、MKAプロトコルを使用してホストとスイッチ間で構築されます。
**D.** 8021AEはCisco AnyConnect NAMとSAPプロトコルを使用してネゴシエートされます
***Answer:*** B

**QUESTION NO: 24**

```
client.connect(sd, port=22, username=username, password=password, allow_agent=False)
stdin, stdout, stderr = client.exec_command('show lld neighbors\n')
u = 0
for u in stdout:
    if 'Router' not in u and 'Capability' not in u and 'Repeater' not in u:
        if 'Device ID' not in u and 'displayed' not in u:
            u101 = u.split()
            if len(u101) != 0:
                u2.append(u101)
    if 'displayed:' in u:
        cx = u.split()
        c0 = cx[3]
d1 = {'x0': u1, 'c0': c0}
```

展示を参照してください。このPythonスクリプトによって何が達成されるのでしょうか？
**A.** show lldp neighbors からの出力を標準出力に表示します。
**B.** show lldp neighbors からネイバー数を辞書リストに読み取ります。
**C.** show lldp neighbors から取得したレイヤ 3 ネイバーを端末画面に表示します。
**D.** show lldp neighbors からの出力を配列オブジェクトに読み取ります。
***Answer:*** B

**QUESTION NO: 25**
REST API
セッションに誤ったパスワードが適用されたリクエストに対する正しい応答はどの HTTP ステータス コードですか?
**A.** HTTPステータスコード 200
**B.** HTTPステータスコード 302
**C.** HTTPステータスコード401
**D.** HTTP ステータス コード: 504
***Answer:*** C

**QUESTION NO: 26**
キャンパスのレイヤー 3 インフラストラクチャを設計する際のベスト プラクティスを 2 つ挙げてください。(2 つ選択してください。)
**A.** 集約レイヤーからコアレイヤーへのルートを要約します。

**B.** アクセス レイヤーから集約レイヤーに向かって要約します。
**C.** 非トランジットリンクにパッシブインターフェースを設定します。
**D.** コア部分にセキュリティ機能を実装します。
**E.** ECMP ルーティングの Cisco Express Forwarding ロード バランシング ハッシュを調整します。
***Answer:*** A E

**QUESTION NO: 27**

```
event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.3 get-type next entry-op gt entry-val 80 poll-interval 5
!
action 1.0 cli command "enable"
action 2.0 syslog msg "high cpu"
action 3.0 cli command "term length 0"
```

展示を参照してください。エンジニアは、show process cpu sortedコマンドの出力をファイルに追加するスクリプトを作成する必要があります。
**A.** action 4.0 syslog command "show process cpu sorted | append flash:high-cpu-file"
**B.** action 4.0 cli command "show process cpu sorted | append flash:high-cpu-file"
**C.** action 4.0 ens-event "show process cpu sorted | append flash:high-cpu-file"
**D.** action 4.0 publish-event "show process cpu sorted | append flash:high-cpu-file"
***Answer:*** B

**QUESTION NO: 28**
サードパーティ アプリケーションに HTTP サービスへの制限付きアクセスを許可する認証フレームワークはどれですか?
**A.** IPsec
**B.** GRE
**C.** 基本認証
**D.** OAuth 2.0
***Answer:*** D

**QUESTION NO: 29**
データ モデリング言語を採用することの利点は何ですか?
**A.** 多数のデバイスを管理するためにマシンフレンドリーなコードを導入する
**B.** ステータスサブスクリプション用のSNMPなどの管理プロトコルの使用を強化する
**C.** モデルに関するベンダー中心のアクションを使用して管理プロセスを拡張する
**D.** ベンダーおよびプラットフォーム固有の構成を、広く互換性のある構成にリファクタリングする
***Answer:*** D

**QUESTION NO: 30**
YANG モジュールの利点は何ですか?

**A.** パフォーマンスを向上させるためのエンコードを備えた密結合モデル
**B.** 共通モデルまたは業界モデルによって提供される、より容易なマルチベンダー相互運用性
**C.** 変更できない固定モジュールを持つことでエコシステムの断片化を回避する
**D.** メンテナンスとサポートを簡素化するための単一のプロトコルとモデルの結合
***Answer:*** B

**QUESTION NO: 31**
有効な JSON ファイルを表示する展示物はどれですか?
**A.**

```
{
      "hostname": "edge_router_1"
      "interfaces": {
            "GigabitEthernet1/1"
            "GigabitEthernet1/2"
            "GigabitEthernet1/3"
      }
}
```

**B.**

```
{
      "hostname": "edge_router_1",
      "interfaces": {
            "GigabitEthernet1/1",
            "GigabitEthernet1/2",
            "GigabitEthernet1/3",
      },
}
```

**C.**

```
{
    "hostname": "edge_router_1"
    "interfaces": [
        "GigabitEthernet1/1"
        "GigabitEthernet1/2"
        "GigabitEthernet1/3"
    ]
}
```

**D.**

```
{
    "hostname": "edge_router_1",
    "interfaces": [
        "GigabitEthernet1/1",
        "GigabitEthernet1/2",
        "GigabitEthernet1/3"
    ]
}
```

***Answer:*** D

**QUESTION NO: 32**
マルチベンダー環境でデータ モデルを活用する利点は何ですか?
**A.** 構成と管理への統一されたアプローチの促進
**B.** バイナリエンコードプロトコルによる通信セキュリティの向上
**C.** 管理対象デバイスにかかるCPU負荷を軽減
**D.** 構成と実行時状態データの区別を削除する
***Answer:*** A

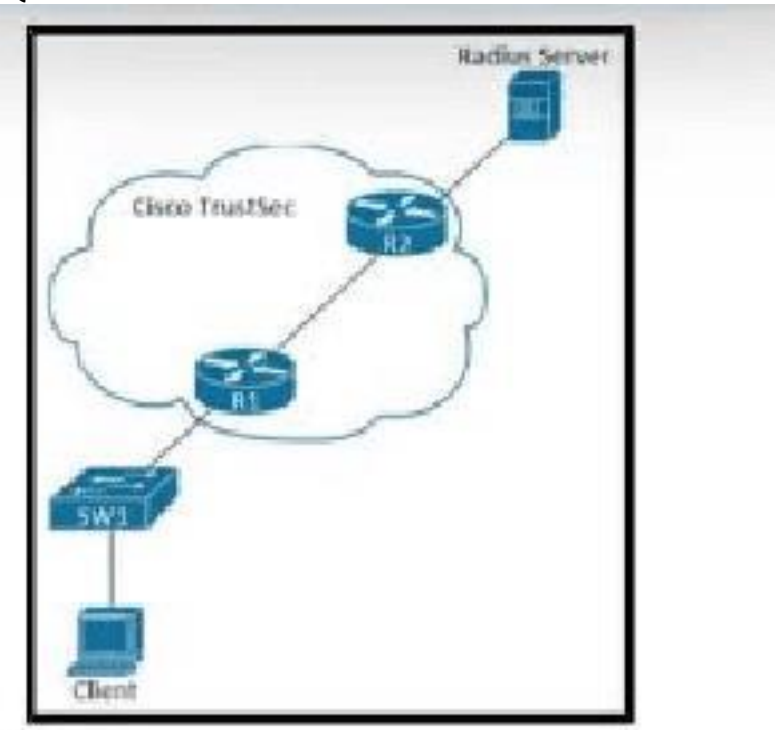
**QUESTION NO: 33**

| R1 | R2 |
|---|---|
| key chain cisco123<br>key 1<br>key-string Cisco123! | key chain cisco123<br>key 1<br>key-string cisco123! |
| Ethernet0/0 - Group 10<br>State is Active<br>8 state changes, last state change 00:02:49<br>Virtual IP address is 192.163.0.1<br>Active virtual MAC address is 0000.0c07.ac0a | Ethernet0/0 - Group 10<br>State is Active<br>17 state changes, last state change 00:02:17<br>Virtual IP address is 192.168.0.1<br>Active virtual MAC address is 0000.0c07.ac0a |

エンジニアが冗長構成で新しいルーターのペアを設置しています。ハードウェア障害が発生した場合でもトラフィックが中断されないことを保証するプロトコルはどれですか？

**A.** HSRPv1
**B.** GLBP
**C.** VRRP
**D.** HSRPv2
***Answer:*** A

**QUESTION NO: 34**




図を参照してください。ネットワークデバイスアクセス制御を使用する場合、どのデバイスがサプリカントとみなされますか？
**A.** クライアント
**B.** SW1
**C.** RADIUSサーバー
**D.** R1
***Answer:*** A
Explanation:
The correct answer is A. client.
In Cisco 802.1X / network admission control terminology, the supplicant is the endpoint device or client software requesting access to the network. Cisco documentation describes 802.1X as a client-server access control model in which the client must be authenticated before gaining ac cess, and the network device relays authentication messages between the supplicant and the authentication server.
* Client = Supplicant
* SW1 = Authenticator
* RADIUS server = Authentication server
* R1 = transit/network infrastructure device, not the supplicant
The supplicant is the device that is trying to join the network and provide credentials. In the diagram, that is the client. Cisco also defines the three 802.1X entities as supplicant system,

authentication system, and authentication server system, with the supplicant being the endpoint such as a PC.
* B. SW1 SW1 functions as the authenticator, controlling access to the network port and relaying EAP messages.
* C. RADIUS server The RADIUS server is the authentication server, not the supplicant.
* D. R1 R1 is part of the network path in the figure, but it is not the device requesting admission to the network.
ENCOR exam point:
For 802.1X / NAC questions, remember this trio:
* Supplicant = endpoint/client
* Authenticator = switch or AP controlling access
* Authentication server = RADIUS / Cisco ISE

**QUESTION NO: 35**
Cisco SD-Access コントロール プレーンはどのテクノロジーに基づいていますか?
**A.** LISP
**B.** CTS
**C.** SGT
**D.** VRF
***Answer:*** A