# Free Questions for 350-501 by go4braindumps

## Shared by Alvarado on 09-08-2024

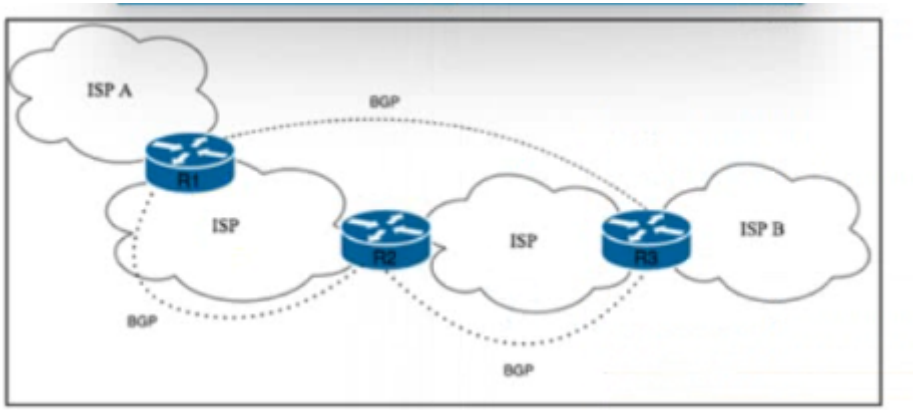
**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

Refer to the exihibit.




Refer to the exhibit. Tier 1 ISP A is connected to small Tier 3 ISP B. The EBGP routing protocol is used for route exchange. The networking team at ISP A noticed the flapping of BGP sessions with ISP B. The team decides to Improve stability on the network by suppressing the subnet for 30 minutes when a session begins to flap. Which action must the team perform to meet this goal?

## Options:

**A-** Implement a BGP route-penalty timer on ISP A router R1 with the bgp penalty-timer 30 250 750 15 command.

**B-** Implement BGP route dampening on ISP A router R1 with the bgp dampening 15 700 1500 30 command.

**C-** Implement BGP route suppression on ISP A router R2 with the bgp suppression 30 600 1200 30 command.

**D-** Implement a BGP route withdraw-delay timer on ISP B router R3 with the bgp withdraw-delay 30 15 90 30 command.

### Answer:

B

### Explanation:

To address the issue of BGP session flapping between ISP A and ISP B, the networking team at ISP A should implement BGP route dampening. This feature helps stabilize the network by suppressing the advertisement of flapping routes. The commandbgp dampening 15 700 1500 30will set the parameters for route dampening, where routes that flap will be suppressed for 30 minutes. This action will prevent the constant advertisement and withdrawal of unstable routes, thus improving the stability of the network.Reference:= For further details on BGP route dampening and its configuration, the Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) course materials and Cisco's official documentation provide comprehensive guidance.

## Question 2

**Question Type:** MultipleChoice

A customer site is being connected to a Frame Relay network via a T1 link. The customer has a contract for 512 kbps service with a Tc value of 125 ms. Under peak line conditions, customer traffic can reach four times the contracted speed. Which QoS configuration must the service provider implement to limit the customer to the contracted values?

```
policy-map policy_map
 class class_map
  police cir 512000 bc 64000 pir 20480000 be 192000
   conform-action transmit
   exceed-action drop
```

```
policy-map policy_map
 class class_map
  police cir 512kbps bc 256kbps pir 2Mbps be 9600 kbps
   conform-action transmit
   exceed-action set-de-bit transmit
   violate-action drop
```

```
policy-map policy_map
 class class_map
  police cir 512000 bc 128000 pir 256000 be 32000
   conform-action transmit
   exceed-action set-be-bit transmit
   exceed-action drop
```

```
policy-map policy_map
 class class_map
  police cir 512000 bc 32000 pir 64000 be 6400
   conform-action transmit
   violate-action set-dscp-transmit default
   exceed-action drop
```

## Options:

**A-** Option A

**B-** Option B

**C-** Option C

**D-** Option D

### Answer:

B

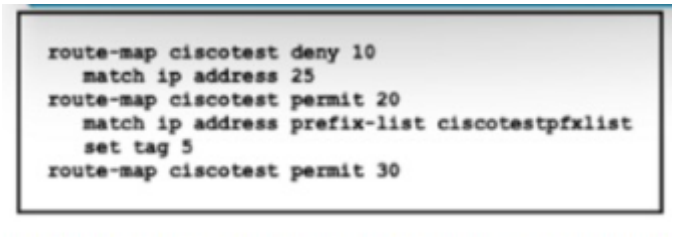
### Explanation:

The service provider must implement a QoS configuration that includes traffic policing to enforce the contracted bandwidth limits. Option B is the correct choice because it specifies a committed information rate (CIR) of 512 kbps, which matches the customer's contracted rate. The configuration also includes a burst size that accommodates the Tc value of 125 ms, allowing for brief periods of higher traffic without dropping packets.This setup ensures that under peak conditions, any traffic exceeding the contracted rate is either marked or dropped, thus preventing the customer from exceeding the agreed-upon bandwidth.Reference:= For more detailed information on QoS configurations for Frame Relay networks, refer to the Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) course materials, which cover the principles of traffic policing and shaping in service provider environments

## Question 3

**Question Type:** MultipleChoice

Refer to the exihibit.




Refer to the exhibit. A client wants to filter routes to a BGP peer to limit access to restricted areas within the network. The engineer configures the route map ciscotest to filter routes from the BGP neighbor. The engineer also sets a tag that will be used for QoS in the future. Which task must be performed to complete the Implementation?

## Options:

**A-** Attach the new route map to the BGP neighbor statement in the inbound direction.

**B-** Create a policy map named ciscotest and apply It to inbound traffic on the link that is directly connected to the BGP neighbor.

**C-** Create a route map, configure BGP with an IPv4 address family, and activate the neighbor.

**D-** Add a route map statement with sequence 40 that links a BGP community to the routing protocol

## Answer:

A

### Explanation:

To complete the implementation of the route map "ciscotest" for filtering routes to a BGP peer, the engineer must attach the route map to the BGP neighbor statement in the inbound direction.This will apply the specified filtering criteria to routes received from the BGP neighbor, thereby limiting access to restricted areas within the network as intended by the client.Reference:= The Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) course materials discuss the configuration of route maps and their application to BGP neighbors for route filtering purposes

## Question 4

**Question Type:** MultipleChoice

How is RSVP used with MPLS traffic engineering tunnels?

### Options:

**A-** It assigns a tag to a packet as it travels through the tunnel.

**B-** It removes and reassigns an MPLS label when the packet enters the tunnel.

**C-** It reduces the CPU burden when a packet travels through the tunnel.

**D-** It reserves bandwidth along the path of the tunnel.

### Answer:

D

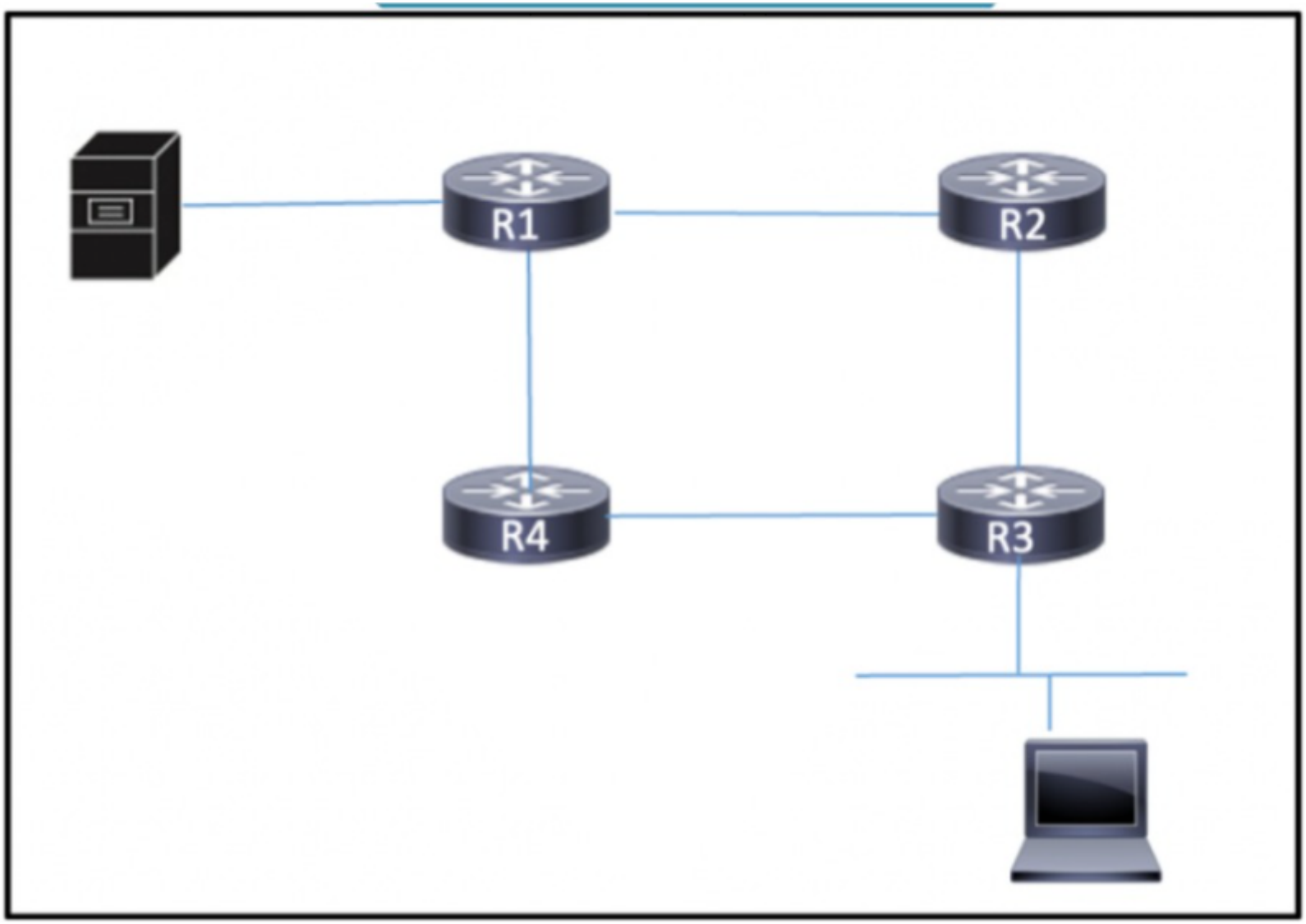
### Explanation:

RSVP (Resource Reservation Protocol) is used with MPLS (Multiprotocol Label Switching) traffic engineering tunnels primarily to reserve bandwidth along the path of the tunnel.This ensures that sufficient resources are allocated for the traffic to meet quality of service requirements, which is crucial for maintaining the performance of critical applications that traverse the network.Reference:= For more information on RSVP and MPLS traffic engineering, refer to the Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) course materials, which provide detailed explanations on how these technologies work together to optimize network traffic1.

## Question 5

**Question Type:** MultipleChoice

Refer to the exihibit.




Refer to the exhibit. A host connected to R3 must connect with a server on R1 that provides critical, time-sensitive dat

a. Traffic between the host and server must always be given bandwidth to traverse the links when they are congested, with other traffic being dropped. How must the network engineer implement a QoS strategy with classification to ensure that the traffic is given the appropriate bandwidth?

## Options:

**A-** Implement FIFO to guarantee that the server traffic is sent first while other traffic is queued.

**B-** Implement policing to rate-limit noncritical traffic that exceeds designated thresholds.

**C-** Implement traffic shaping to delay noncritical traffic when the link is congested.

**D-** Implement strict priority to guarantee bandwidth for the server traffic.

## Answer:

D

## Explanation:

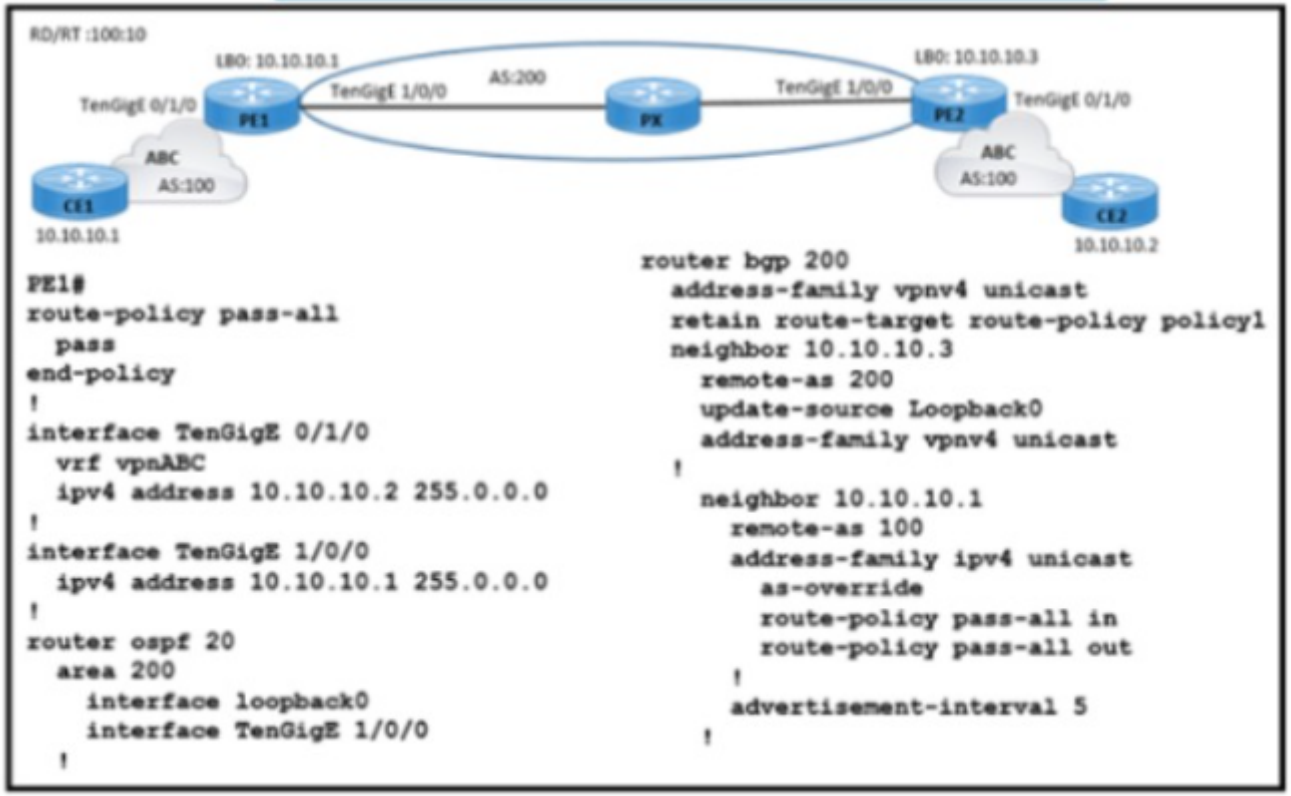
To ensure that critical, time-sensitive data from the server on R1 to the host on R3 is always prioritized, especially during congestion, the network engineer should implement a Quality of Service (QoS) strategy that uses strict priority queuing. This QoS mechanism ensures that traffic marked as high priority is transmitted first, while other traffic may be queued or dropped if necessary. Strict priority queuing is designed for scenarios exactly like this, where certain traffic must be guaranteed bandwidth to meet time-sensitive requirements.Reference:= For more detailed information on QoS strategies and classification, refer to the Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) course materials, specifically the sections discussing QoS mechanisms

and their implementation in service provider networks. Additionally, Cisco's official documentation on QoS provides comprehensive guidelines on configuring and applying strict priority queuing to ensure bandwidth for critical traffic.

# Question 6

**Question Type:** **MultipleChoice**

Refer to the exihibit.




Refer to the exhibit. A service provider engineer Is configuring the connection between CE1 and CE2. AS 200 of the service provider and AS 100 of enterprise ABC should connect using BGP. The engineer already completed the configuration of VRF RT 100:10 of enterprise ABC. Which configuration must the engineer apply on PE1 to meet the requirement?

```
vrf vpn1
rd 100:1
address-family vpnv4 unicast
redistribute connected
```

```
vrf vpn1
rd 100:1
address-family ipv4 unicast
redistribute connected
```

```
router bgp 200
neighbor 10.10.10.1
remote-as 100
address-family vpnv4 unicast
```

```
router bgp 200
address-family ipv4 unicast
neighbor 10.10.10.3
```

## Options:

**A-** Option A

**B-** Option B

**C-** Option C

**D-** Option D

### Answer:

C

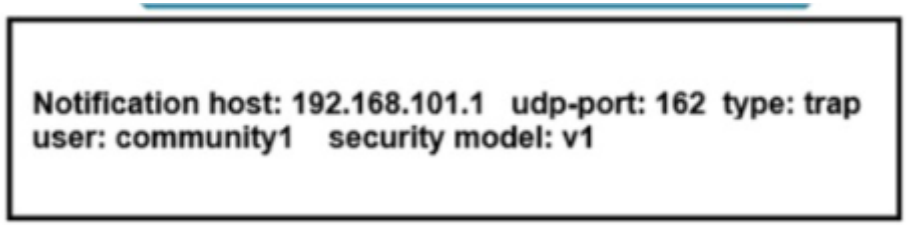
### Explanation:

The correct configuration for PE1 to connect AS 200 of the service provider with AS 100 of enterprise ABC using BGP, considering the VRF RT 100:10 is already configured, would involve setting up BGP with the correct neighbor and route distinguisher settings. Option C is likely the correct choice as it specifies the BGP neighbor to be within the enterprise ABC's AS 100 and includes the address family configuration necessary for VRF-aware BGP sessions.Reference:= The Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) course materials provide detailed instructions on configuring BGP in a service provider environment, including the use of VRFs and route distinguishers.For more information, please refer to the official Cisco documentation and course materials related to SPCOR1.

## Question 7

**Question Type:** MultipleChoice

Refer to the exihibit.




Refer to the exhibit. Over the last few months. ISP A has doubled Its user base. The IT Director asked the engineering team to monitor memory consumption and buffer statistics on all P and PE devices In the MPLS core. Most devices have CPU usage of 70% or more, so the solution must be targeted and secure. Which two commands must the engineering team implement on P and PE devices to meet these requirements? (Choose two.)

## Options:

**A-** snmp-server host 192.168.101.1 version 3 auth community1 memory

**B-** snmp-server enable traps memory bufferpeak

**C-** snmp-server host 192.168.101.1 version 2c community1 memory

**D-** snmp-server host 192.168.101.1 version 1 community1 auth memory

**E-** snmp-server enable snmp-traps community1 bufferpeak

## Answer:

A, B

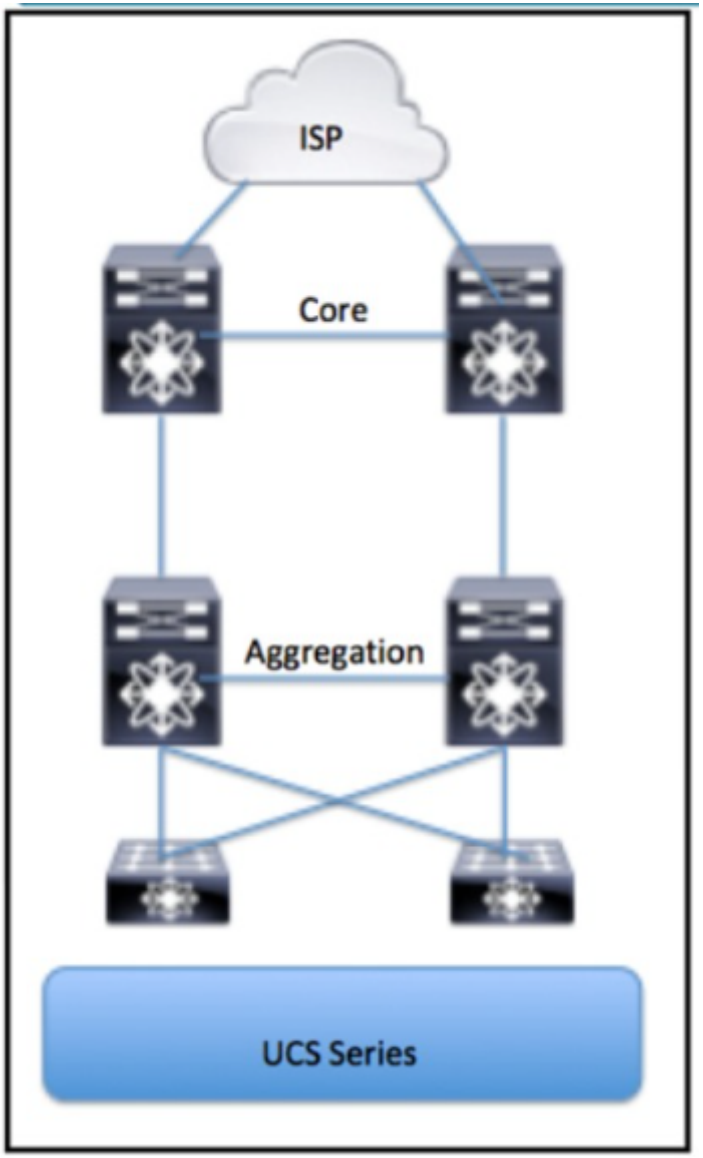
### Explanation:

To monitor memory consumption and buffer statistics securely on P and PE devices in an MPLS core, especially considering the high CPU usage, the engineering team should implement SNMP version 3 for its security features. Therefore, option A is correct as it specifies SNMP version 3 with authentication. Option B is also correct as it enables traps for memory buffer peak, which is essential for monitoring memory thresholds and ensuring quick response to potential issues.

## Question 8

**Question Type:** MultipleChoice

Refer to the exihibit.




Refer to the exhibit. Which part of the diagram will host OpenStack components?

## Options:

**A-** Aggregation

**B-** UCS Series

**C-** Access

**D-** Core

## Answer:

B

## Explanation:

In the context of Cisco's Implementing and Operating Service Provider Network Core Technologies, the UCS Series is typically where OpenStack components would be hosted. OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a data center, all managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface.

# Question 9

**Question Type:** MultipleChoice

Refer to the exihibit.

```
import  import
from requests. auth import HTTPBasicAuth
auth = HTTPBasicAuth('cisco_device', 'cisco_device')
headers = { 'Accept': 'application/yang-data+json', 'Content-Type': 'application/yang-data+json' }
url = "https://172.168.211.65/restconf/data/Cisco-IOS-XE-native:native/interface/GigabitEthernet=0/1
payload = """
{
  "Cisco-IOS-XE-native:GigabitEthernet": {
    "ip": {
      "address": {
        "primary": {
          "address": "10.1.131.112",
          "mask": "255.255.255.252"
        }
      }
    }
  }
}
"""
response = requests.patch(url, verify=False)
print ("Done" + response.status)
```

Refer for the exhibit. To optimize network operations, the senior architect created this Python 3.9 script for network automation tasks and to leverage Ansible 4.0 playbooks. Devices In the network support only RFC 2617-based authentication What does the script do?

## Options:

**A-** The script logs in via SSH and configures interface GigabitEthernetO/1 with IP address 10.1.131.112/30.

**B-** The script leverages REST API calls and configures Interface GlgabilEthemet0/1 with IP address 10.1.131.112/30.

**C-** The script performs a configuration sanity check on the device with IP address 172.168.211.65 via HTTP and returns an alert If the payload field falls to match.

**D-** The script parses the JSON response from the router at IP address 172 168.211.65 and checks If the interface GigaWtEthernet0/1 with IP address 10.1.131.112 exists on the router.

### Answer:

B

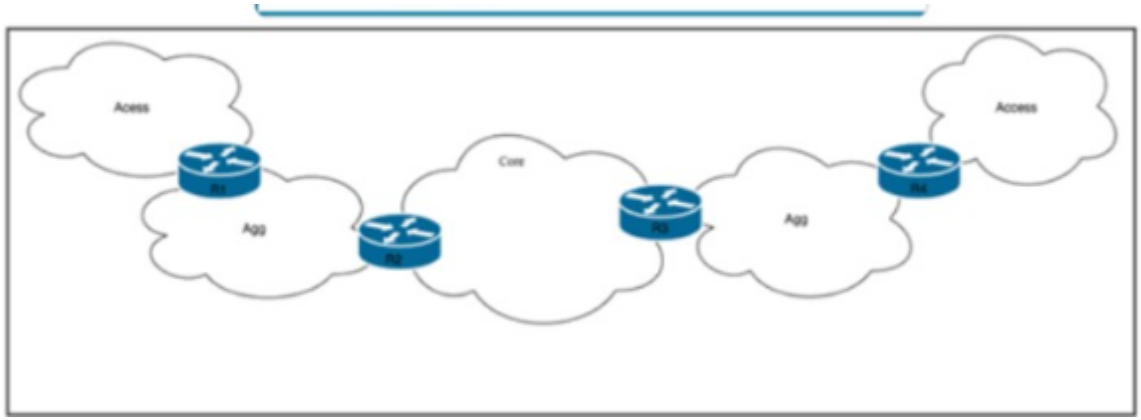
### Explanation:

The script is designed to leverage REST API calls for network configuration tasks. It uses therequestslibrary in Python to send a PATCH request to the device with IP address 172.168.211.65. The script includes RFC 2617-based authentication, which is used for HTTP, indicating that it's not using SSH for login. The payload of the REST API call specifies the configuration for the interface GigabitEthernet0/1 with the IP address 10.1.131.112/30. Therefore, the script is performing option B, configuring the interface via REST API calls.

## Question 10

**Question Type:** MultipleChoice

Refer to the exihibit.




Refer to the exhibit. Tier 1 ISP A purchased several Tier 2 ISPs to increase their customer base and provide more regional coverage. ISP A plans to implement MPLS services in the access layer, with scalability up to 100.000 devices In one packet network and service recovery up to 50 ms. The network architect decided to use different independent IGP and LDP domains and interconnect LSPs that are based on RFC 3107. Which two actions must the network engineer perform to meet the requirements? (Choose two.)

## Options:

**A-** Implement BGP PIC core functionality on routers R2 and R3.

**B-** Configure three OSPF areas, with Area 0 In the core domain, and Areas 2 and 3 in the aggregation domain.

**C-** Implement BGP connectivity between routers R1 and R4 with VPNv4 address family enabled.

**D-** Implement BGP inline RR functionality with next-hop-self capabilities on routers R2 and R3.

**E-** Implement the IS-IS routing protocol on the access domain.

## Answer:

A, C

## Explanation:

To meet the scalability and service recovery requirements, the network engineer should implement BGP PIC core functionality on routers R2 and R3 (Option A). This will enhance the convergence time during a failure. Additionally, establishing BGP connectivity between routers R1 and R4 with VPNv4 address family enabled (Option C) will facilitate MPLS services across multiple IGP domains.

Implementing and Operating Cisco Service Provider Network Core Technologies

On-Demand E-Learning for Implementing and Operating Cisco Service Provider Network Core Technologies