# Free Questions for 350-501

## Shared by Stuart on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

Question Type: MultipleChoice

Which fact must a network engineer consider when planning to deploy RSVP-TE FRR?

## Options:

A- The FRR backup tunnel reserves the total bandwidth of all protected tunnels
B- FRR protects MPLS LDP and RSVP-TE LSPs.
C- PLR prefers FRR NHOP backup tunnels over NNHOP tunnels.
D- PLR prefers FRR NNHOP backup tunnels over NHOP tunnels.

## Answer:

C

## Explanation:

RSVP-TE Fast Reroute (FRR) is a mechanism that provides protection switching for MPLS TE LSPs. The Point of Local Repair (PLR) will prefer to use a next-hop (NHOP) backup tunnel over a next-next-hop (NNHOP) backup tunnel when both are available. This preference is due to the fact that NHOP backup tunnels can provide faster rerouting around the failure point, minimizing traffic disruption and packet loss.

# Question 2

Question Type: MultipleChoice

Refer to the exihibit.

```
GET https://192.168.201.10/api/class/aaaUser.json?
      query-target-filter=eq(aaaUser.lastName,"CiscoTest")
```

Refer to the exhibit. An engineer configured several network devices to run REST APIs. After testing, the organization plans to use REST APIs throughout the network to manage the network more efficiently. What is the effect if this script?

## Options:

A- It returns an AAA users with the last name CiscoTest.
B- It creates a class map named aaauser with traffic tagged from AAA.
C- It queries the local database to find a user named aaaUser.Json
D- It adds the user CiscoTest to the AAA database located at 192.168.201.10.

## Answer:

D

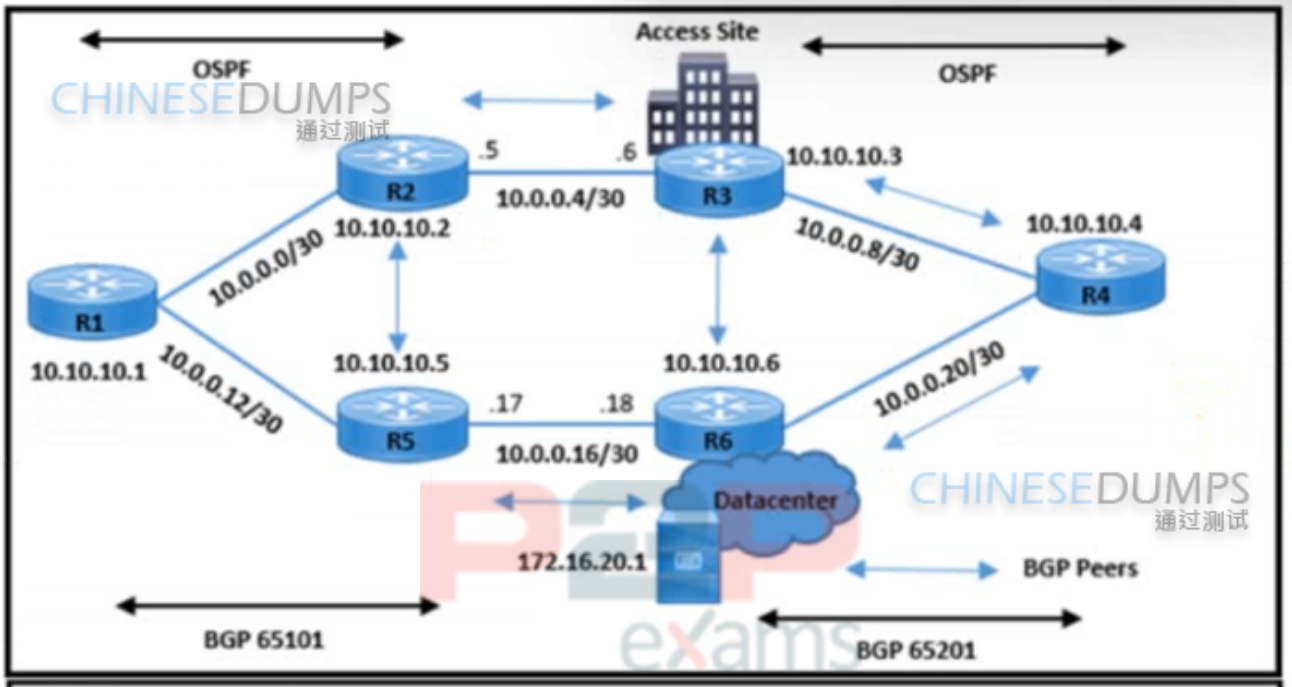
## Explanation:

The script shown in the exhibit is a REST API call that adds a user with the last name 'CiscoTest' to the AAA database on the server located at the IP address 192.168.201.10. This is achieved through a POST request, which is typically used to create or update resources on a server. The script specifies the user details in JSON format, which is a common data format used for API calls.

# Question 3

Question Type: MultipleChoice

Refer to the exihibit.




```
R3#show  ip route
     192.168.30.0/32 is subnetted, 1 subnets
B       192.168.30.1 [200/0] via 10.10.10.4, 00:39:23
     172.16.0.0/32 is subnetted, 2 subnets
O       172.16.20.1 [110/3] via 10.0.0.10, 00:05:39, GigabitEthernet2/0
B       172.16.10.10 [200/0] via 10.10.10.1, 00:39:23
     10.0.0.0/8 is variably subnetted, 15 subnets, 3 masks
C       10.0.0.8/30 is directly connected, GigabitEthernet2/0
O       10.0.0.12/30 [110/3] via 10.0.0.5, 00:41:16, FastEthernet0/0
S       10.10.10.2/32 [1/0] via 10.0.0.5
C       10.10.10.3/32 is directly connected, Loopback0
O       10.0.0.0/30 [110/2] via 10.0.0.5, 00:41:16, FastEthernet0/0

O       10.10.10.1/32 [110/3] via 10.0.0.5, 00:41:16, FastEthernet0/0
O       10.10.10.6/32 [110/2] via 10.0.0.29, 00:41:16, FastEthernet1/0
O       10.10.10.4/32 [110/2] via 10.0.0.10, 00:41:16, GigabitEthernet2/0
C       10.0.0.4/30 is directly connected, FastEthernet0/0
```

```
O       10.10.10.1/32 [110/3] via 10.0.0.5, 00:41:16, FastEthernet0/0
O       10.10.10.6/32 [110/2] via 10.0.0.29, 00:41:16, FastEthernet1/0
O       10.10.10.4/32 [110/2] via 10.0.0.10, 00:41:16, GigabitEthernet2/0
C       10.0.0.4/30 is directly connected, FastEthernet0/0
O       10.10.10.5/32 [110/12] via 10.0.0.5, 00:41:16, FastEthernet0/0
O       10.0.0.24/30 [110/11] via 10.0.0.5, 00:41:16, FastEthernet0/0
C       10.0.0.28/30 is directly connected, FastEthernet1/0
B       10.0.0.16/30 [200/0] via 10.10.10.5, 00:39:23
O       10.0.0.20/30 [110/2] via 10.0.0.10, 00:41:16, GigabitEthernet2/0
     192.168.1.0/32 is subnetted, 1 subnets

R4#show ip route 172.16.20.1
Routing entry for 172.16.20.1/32
  Known via "ospf 10", distance 110, metric 2, type intra area
  Last update from 10.0.0.21 on FastEthernet1/0, 00:06:51 ago
  Routing Descriptor Blocks:
  * 10.0.0.21, from 172.16.20.1, 00:06:51 ago, via FastEthernet1/0
      Route metric is 2, traffic share count is 1
```

Refer to the exhibit. The network operations team reported that the access site that is connected to R3 is not connecting to the application server in the data center and that all packets that are sent from the application server to the access site are dropped. The team verified that OSPF and BGP peerings are up in BGP AS 65101 and BGP AS 65201. R4 is expected to receive traffic from the application server route via OSPF. Which action resolves this issue?

## Options:

A- Remove the route-map on R4 when advertising 172.16.20.1 in BGP to R3.
B- Advertise application server 172.16.20.1 in the OSPF routing table on R6.
C- Allow 172.16.20.1 in the BGP advertisement on R3 in the route-map.
D- Add the next-hop-self command on R6 to enable R3 iBGP peering.

## Answer:

C

## Explanation:

The issue described involves packets being dropped when sent from the application server to the access site. Since OSPF and BGP peerings are confirmed to be operational, the problem likely lies within the route advertisement. Allowing 172.16.20.1 in the BGP advertisement on R3 by adjusting the route-map will likely resolve the issue, ensuring that traffic destined for 172.16.20.1 is not being inadvertently filtered or blocked.

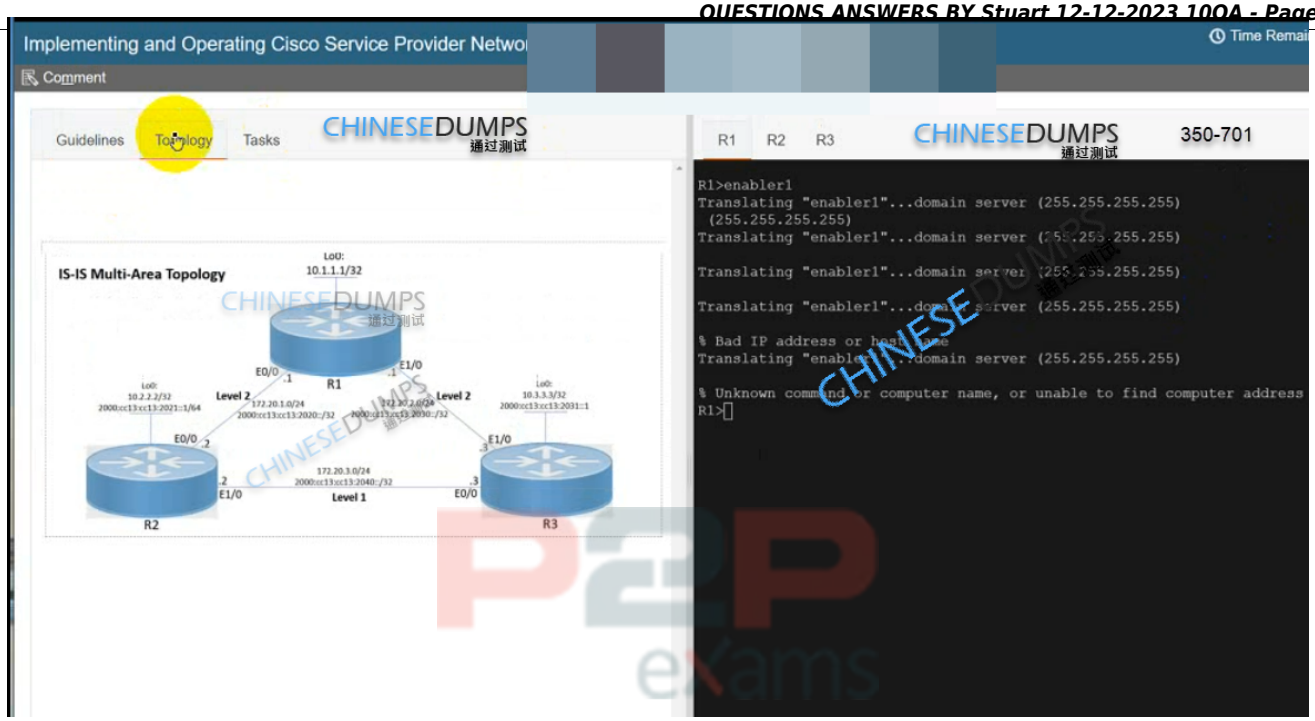
Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) course provides insights into configuring, verifying, troubleshooting, and optimizing Service Provider IP network infrastructures, which includes understanding and implementing BGP routing and route maps1.

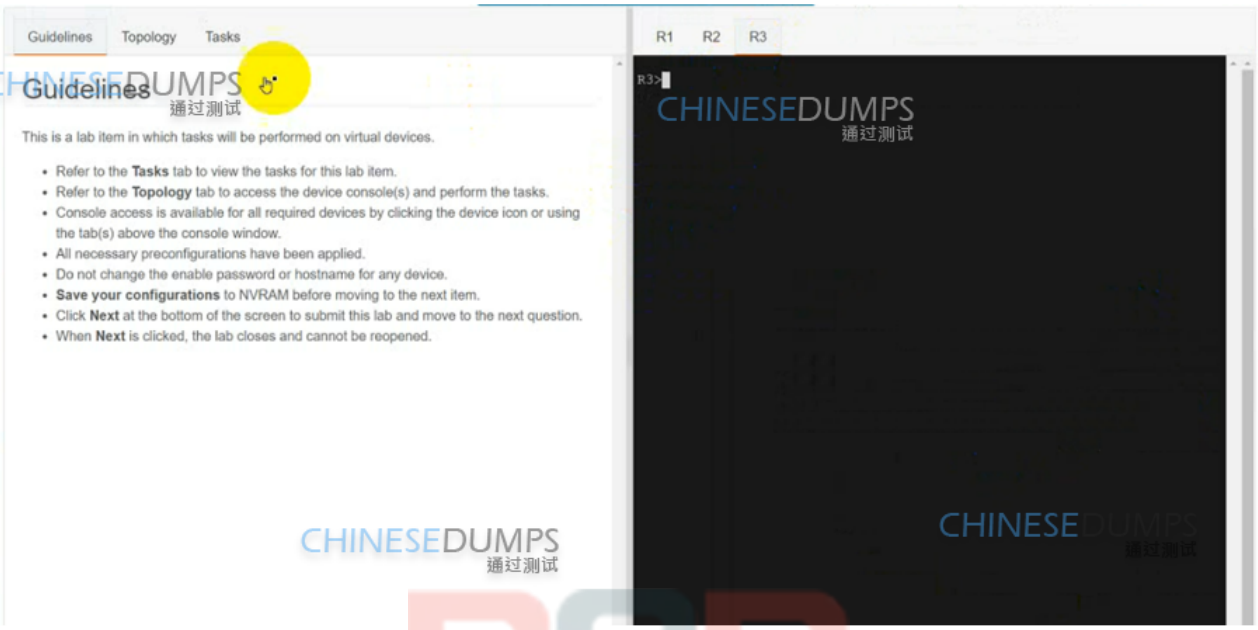
The official Cisco certification exam overview for SPCOR, which includes topics on BGP routing and route maps, can also serve as a reference

# Question 4

Question Type: MultipleChoice

Simulation1


Implementing and Operating Cisco Service Provider Netwo
Comment
Guidelines
Topology
Tasks
CHINESEDUMPS
通过测试
IS-IS Multi-Area Topology
Lo0:
10.1.1.1/32
R1
R2
R3
E0/0
E1/0
Level 2
Level 1
172.20.1.0/24
172.20.2.0/24
172.20.3.0/24
R1
R2
R3
350-701
R1>enable1
Translating "enable1"...domain server (255.255.255.255)
(255.255.255.255)
% Unknown command or computer name, or unable to find computer address
R1>


Guidelines
Topology
Tasks
Guidelines
This is a lab item in which tasks will be performed on virtual devices.
Refer to the Tasks tab to view the tasks for this lab item.
Refer to the Topology tab to access the device console(s) and perform the tasks.
Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
All necessary preconfigurations have been applied.
Do not change the enable password or hostname for any device.
Save your configurations to NVRAM before moving to the next item.
Click Next at the bottom of the screen to submit this lab and move to the next question.
When Next is clicked, the lab closes and cannot be reopened.
R1
R2
R3
R3>
CHINESEDUMPS
通过测试




## Options:

A- See the solution below

## Answer:

A

## Explanation:

SOLUTION:-

R1

Config t

router isis 1

net 49.0001.0010.0001.0101.00

area-password C1sc0!

int et0/0

ip router isis 1

isis authen mode text level-2

isis circuit-type level-2

isis tag 1

int et1/0

ip router isis 1

isis authen mode text level-2

isis circuit-type level-2

isis tag 1

R2

router isis 2

net 49.0001.0010.0002.0202.00

area-password C1sc0!

int et0/0

ip router isis 2

isis authen mode text level-2

isis circuit-type level-2

isis tag 2

int et1/0

ip router isis 2

isis authen mode text level-1

isis circuit-type level-1

isis tag 2

R3

router isis 3

net 49.0001.0010.0003.0303.00

area-password C1sc0!

int et0/0

ip router isis 3

isis authen mode text level-1

isis circuit-type level-1

isis tag 3

int et1/0

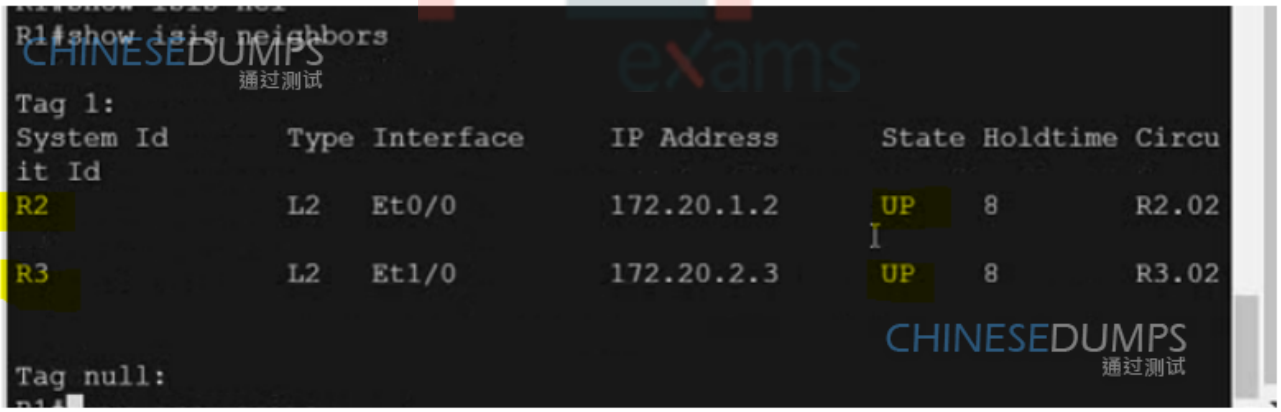
ip router isis 3

isis authen mode text level-2

isis circuit-type level-2

isis tag 3

R1 Verification: -




R1

Config t

Ipv6 unicast-routing

Router isis 1

Metric-style wide

Address-family ipv6 unicast

Multi-topology

Int loop0

Ip router isis 1

Ipv6 router isis 1

Isis tag 1

Int et0/0

Ipv6 router isis 1

Int et1/0

Ipv6 router isis 1

R2

Config t

Ipv6 unicast-routing

Router isis 2

Metric-style wide

Address-family ipv6 unicast

Multi-topology

Int loop0

Ip router isis 2

Ipv6 router isis 2

Isis tag 2

Int et0/0

Ipv6 router isis 2

Int et1/0

Ipv6 router isis 2

R3

Config t

Ipv6 unicast-routing

Router isis 3

Metric-style wide

Address-family ipv6 unicast

Multi-topology

Int loop0

Ip router isis 3

Ipv6 router isis 3

Isis tag 3

Int et0/0

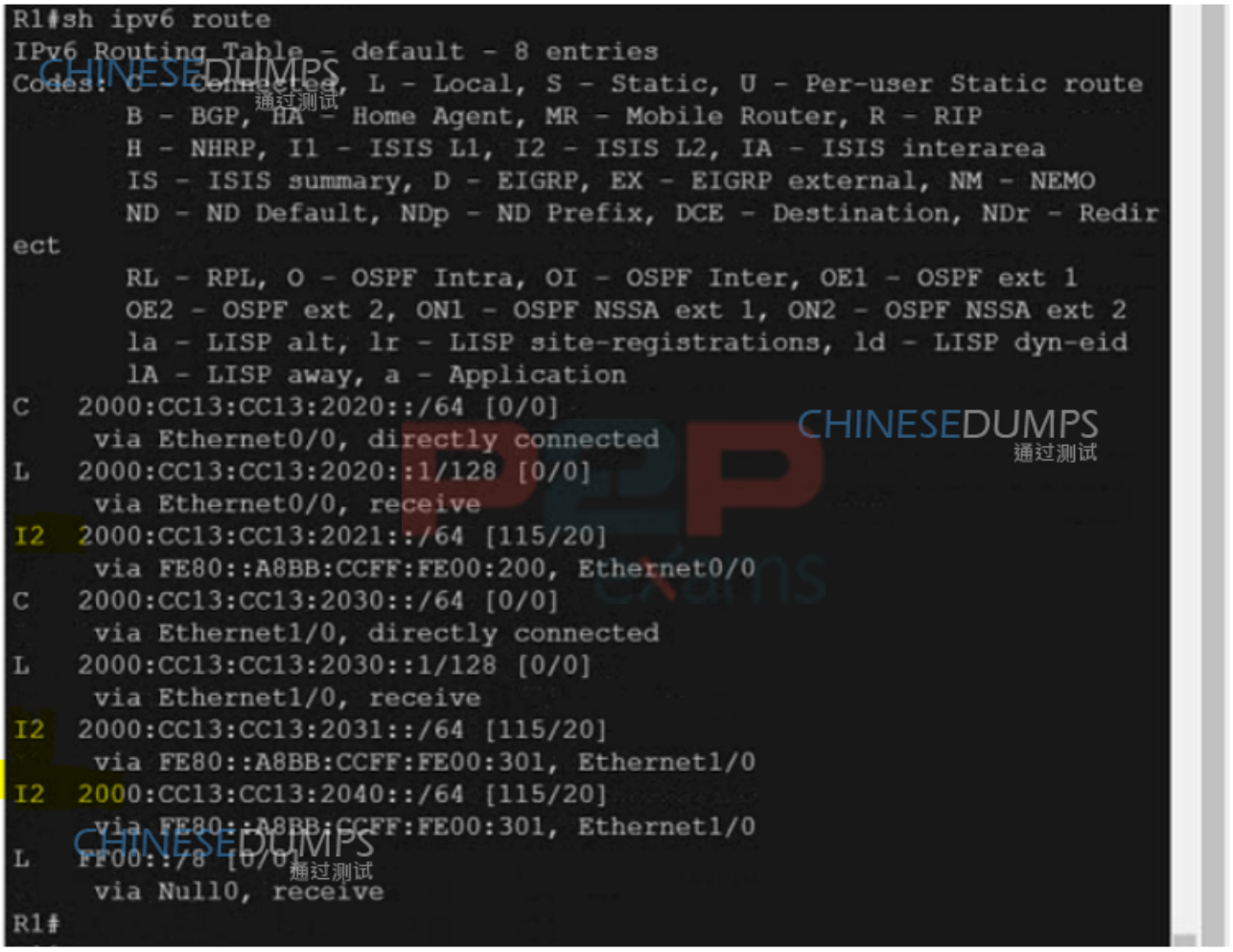
Ipv6 router isis 3

Int et1/0

Ipv6 router isis 3

R1 Ipv6 Verification: -




R1

Copy run start

R2

Copy run start

R3

Copy run start

# Question 5

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 6

Question Type: MultipleChoice

Why is the keyword none needed when implementing management plane security using TACACS?

### Options:

A- It altovSWMB6ter to query a RADIUS server when the TACACS+ server is unreachable.
B- It allows the local database to authenticate when the TACACS^ server is unreachable.
C- It allows authentication to succeed when the TACACS+ server is unreachable.
D- It prevents all users from accessing router 1 unless the TACACS+ server is reachable,

### Answer:

C

### Explanation:

The keyword 'none' is essential in management plane security using TACACS to ensure that authentication can still succeed when the TACACS+ server is unreachable. This fallback mechanism allows network resources to remain accessible even if the TACACS+ server fails or becomes unreachable.Reference: Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) - Management Plane Security section.

# Question 7

Question Type: MultipleChoice

According to RFC5305 on IS-IS extensions for traffic engineering, what is the 4-octet sub-TLV type 10 of extended IS-IS reachability TLV type 22?

## Options:

A- TE default metric
B- maximum reservable link bandwidth
C- administrative group (color)
D- IPv4 neighbor address

## Answer:

B

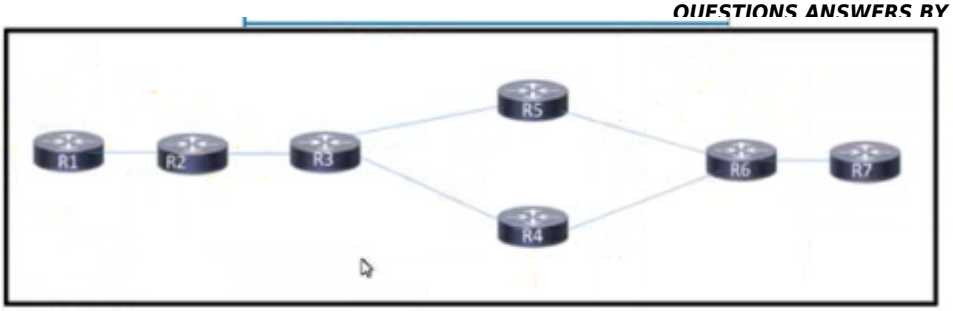
## Explanation:

RFC 5305 extends the IS-IS protocol for traffic engineering by specifying new information that an Intermediate System (router) can place in Link State Protocol Data Units (LSPs). Sub-TLV type 10 of the extended IS-IS reachability TLV type 22 is used to specify the maximum reservable link bandwidth.This is an important parameter for traffic engineering as it defines the amount of bandwidth that can be reserved by traffic engineering algorithms for use in constrained-path computations for MPLS traffic engineering Label Switched Paths (LSPs).Reference: RFC 53051.

# Question 8

Question Type: MultipleChoice

Refer to the exhibit. After a networking team configured this MPLS topology, the supervisor wants to view MPLS labels to verify the path that packets take from router R1 to router R7 The team already Issued an ICMP ping to verify connectivity between the devices. Which task must the team perform to allow the supervisor to view the label switch path?




## Options:

A- Configure MPLS TE to display the labels in the stack between the head and tail-end routers
B- Implement MPLS LDP to assign labels to all the routes in the transit path.
C- Configure MPLS LDP Sync to sync labels from the routing table to the MPLS forwarding table.
D- Implement MPLS OAM to display the labels for each hop along the path

## Answer:

D

# Question 9

Question Type: MultipleChoice

What is a characteristics of the Pipe model for MPLS QoS?

## Options:

A- The same QoS policy is applied to all customer traffic on the egress PE.
B- If the outer EXP is changed, it is copied to the DSCP value.
C- The MPLS EXP bits are set by the CE.
D- The DSCP value determines how the packet is forwarded

## Answer:

C

## Explanation:

In the Pipe model of MPLS QoS, the MPLS EXP bits are set by the Customer Edge (CE) device. This model allows the CE to mark the packets, and these markings are retained throughout the MPLS network until they reach the egress Provider Edge (PE) router. The PE router does not alter the

MPLS EXP value, ensuring that the QoS policy applied by the customer is preserved end-to-end.

# Question 10

Question Type: MultipleChoice

A network architect dcides to expand the scope of the multicast deployment within the company network the network is already using PIM-SM with a static RP that supports a high-bandwidth. video-based training application that s heavily used by the employees, but excessive bandwidth usage is a concern How must the engineer update the network to provide a more efficient multicast implementation'?

## Options:

A- Configure IGMP to manage the multicast hosts on each LAN
B- implement BSR to support dynamic RP notification.
C- Deploy ICMP to Improve multicast reachability across the network using static RP.
D- Implement STP to improve switching performance for multicast data.

## Answer:

B

To Get Premium Files for 350-501 Visit
https://www.p2pexams.com/products/350-501

For More Free Questions Visit
https://www.p2pexams.com/cisco/pdf/350-501

