



**Cisco**

**Exam Questions 300-410**

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Exam Topic 3)

A network administrator must optimize the segment size of the TCP packet on the DMVPN IPsec protected tunnel interface, which carries application traffic from the head office to a designated branch. The TCP segment size must not overwhelm the MTU of the outbound link. Which configuration must be applied to the router to improve the application performance?

- ☒ interface tunnel30  
ip mtu 1400  
ip tcp packet-size 1360  
!  
crypto ipsec fragmentation after-encryption
- ☐ interface tunnel30  
ip mtu 1400  
ip tcp payload-size 1360  
!  
crypto ipsec fragmentation before-encryption
- ☐ interface tunnel30  
ip mtu 1400  
ip tcp adjust-mss 1360  
!  
crypto ipsec fragmentation after-encryption
- ☐ interface tunnel30  
ip mtu 1400  
ip tcp max-segment 1360  
!  
crypto ipsec fragmentation before-encryption

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

### NEW QUESTION 2

- (Exam Topic 3)

Refer to the exhibit.

```
*Sep 26 19:50:43.504: SNMP: Packet received via UDP from
192.168.1.2 on GigabitEthernet0/1SrParseV3SnmpMessage: No
matching Engine ID.

SrParseV3SnmpMessage: Failed.
SrDoSnmp: authentication failure, Unknown Engine ID

*Sep 26 19:50:43.504: SNMP: Report, reqid 29548, errstat 0,
erridx 0
internet.6.3.15.1.1.4.0 = 3
*Sep 26 19:50:43.508: SNMP: Packet sent via UDP to 192.168.1.2
process_mgmt_req_int: UDP packet being de-queued
```

Which two commands provide the administrator with the information needed to resolve the issue? (Choose two.)

- A. snmp user
- B. debug snmp engine-id
- C. debug snmpv3 engine-id
- D. debug snmp packet
- E. showsnmpv3 user

**Answer: AE**

### NEW QUESTION 3

- (Exam Topic 3)

An engineer configures PBR on R5 and wants to create a policy that matches traffic destined toward 10.10.10.0/24 and forward 10.1.1.1. The traffic must also have its IP precedence set to 5. All other traffic should be forward toward 10.1.1.2 and have its IP precedence set to 0. Which configuration meets the requirements?

- A. access-list 1 permit 10.10.10.0 0.0.0.255 access-list 2 permit any route-map CCNP permit 10 match ip address 1 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 match ip address 2 set ip next-hop 10.1.1.2 set ip precedence 0 ! route-map CCNP permit 30
- B. access-list 100 permit ip any 10.10.10.0 0.0.0.255 route-map CCNP permit 10 match ip address 100 set ip next-hop 10.1.1.1 set ip precedence 0 ! route-map CCNP permit 20 set ip next-hop 10.1.1.2 set ip precedence 5 ! route-map CCNP permit 30
- C. access-list 1 permit 10.10.10.0 0.0.0.255 route-map CCNP permit 10 match ip address 1 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 set ip next-hop 10.1.1.2 set ip precedence 0
- D. access-list 100 permit ip any 10.10.10.0 0.0.0.255 route-map CCNP permit 10 match ip address 100 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 set ip next-hop 10.1.1.2 set ip precedence 0

Answer: D

#### NEW QUESTION 4

- (Exam Topic 3)

Which two components are required for MPLS Layer 3 VPN configuration? (Choose two)

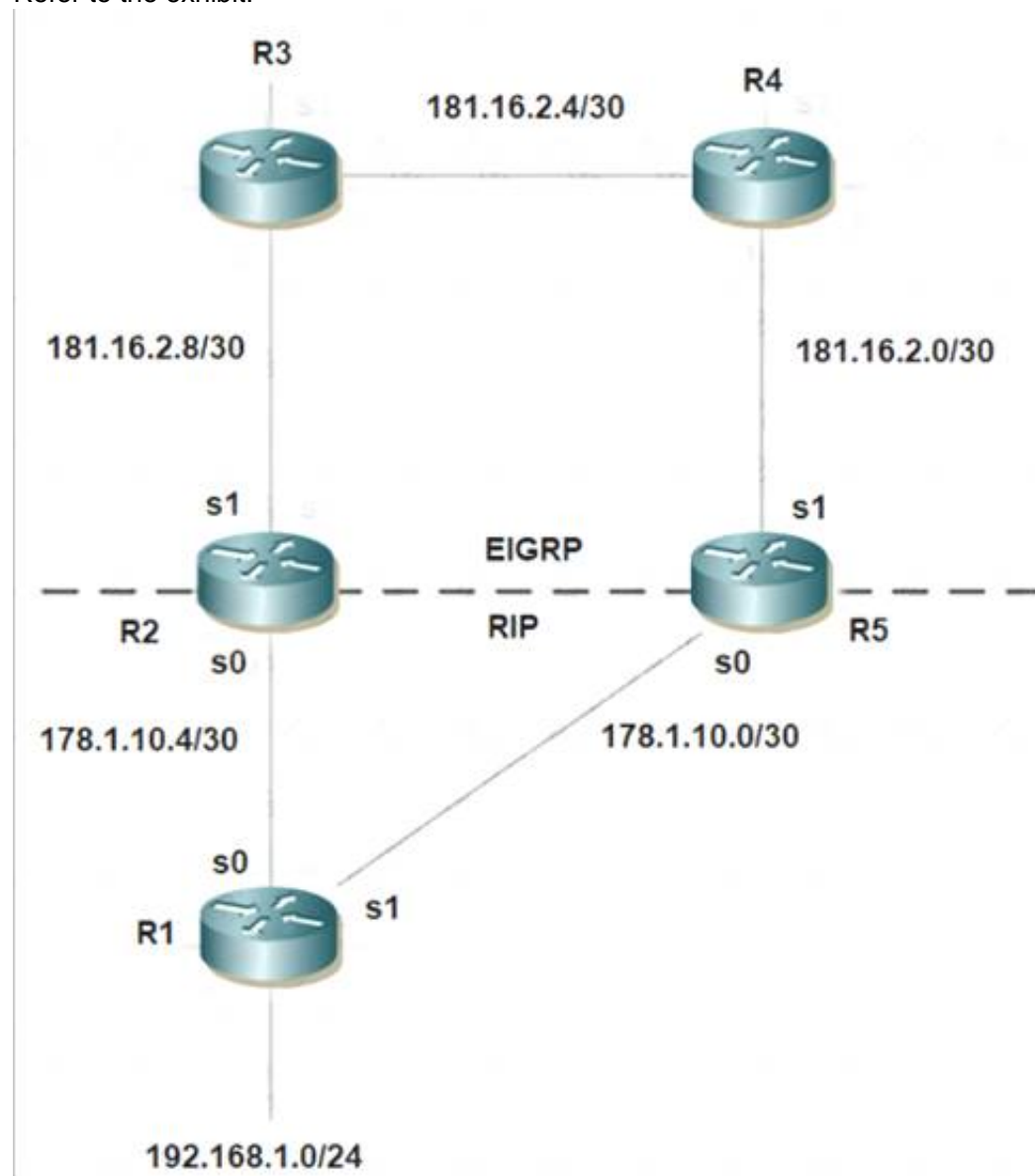
- A. Use pseudowire for Layer 2 routes
- B. Use MP-BGP for customer routes
- C. Use OSPF between PE and CE
- D. Use a unique RD per customer VRF
- E. Use LDP for customer routes

Answer: CD

#### NEW QUESTION 5

- (Exam Topic 3)

Refer to the exhibit.



Mutual redistribution is enabled between RIP and EIGRP on R2 and R5. Which configuration resolves the routing loop for the 192.168.1.0/24 network?

- A. R2:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit anyR5:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit any
- B. R2:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit anyR5:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit any
- C. R2:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit anyR5:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit any
- D. R2:router eigrp 7network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 7 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit anyR5:router eigrp 7network 181.16.0.0redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 7 metric 2!access-list 1 deny 192.168.1.0 access-list 1 permit any

Answer: D

#### Explanation:

<https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.ht>

#### NEW QUESTION 6

- (Exam Topic 3)

What is a characteristic of IPv6 RA Guard?

- A. RA messages are allowed from the host port to the switch
- B. It is unable to protect tunneled traffic
- C. It filters rogue RA broadcasts from connected hosts
- D. It is supported on the egress direction of the switch

Answer: C

### NEW QUESTION 7

- (Exam Topic 3)

An engineer configured a router with this configuration

```
ip access-hst DENY TELNET
```

```
10 deny tcp any any eq 23 log-input
```

The router console starts receiving log message :%SEC-6-IPACCESSLOGP: list DENY\_TELNET denied tcp 192.168.1.10(1022)(FastEthernet1/0 D508.89gb.003f) ->192.168.2.20(23), 1 packet"

Which action stops messages on the console while still denying Telnet?

- A. Configure a 20 permit ip any any command
- B. Remove log-Input keyword from the access list.
- C. Replace log-input keyword with the log keyword in the access list.
- D. Configure a 20 permit ip any any log-input command.

Answer: B

### NEW QUESTION 8

- (Exam Topic 3)

Refer to the exhibit.

```
R1#sh ip route
      10.0.0.0/8 is variably subnetted, 3 subnets, 1 masks
D       10.1.2.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
D       10.1.1.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
```

An engineer configures the router 10.1.100.10 for EIGRP autosummarization so that R1 should receive the summary route of 10.0.0.0/8. However, R1 receives more specific /24 routes.

Which action resolves this issue?

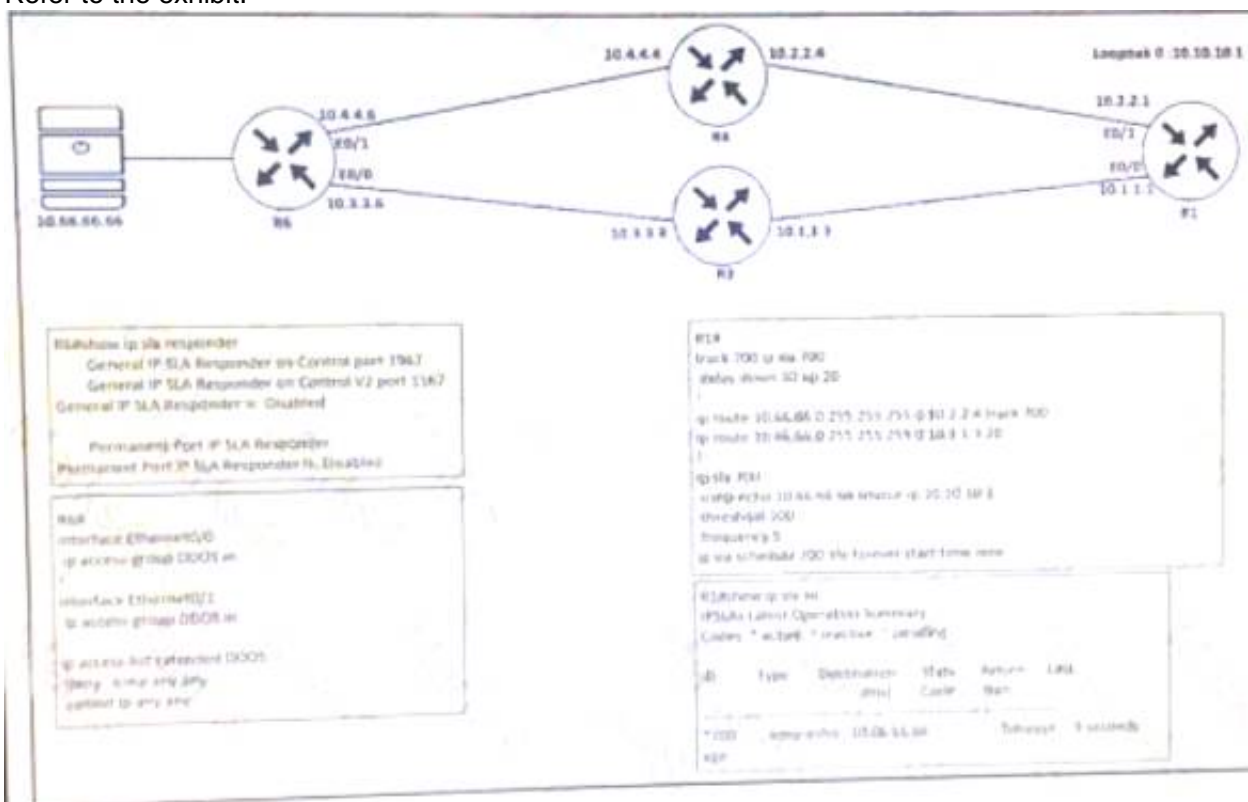
- A. Router R1 should configure ip summary address eigrp (AS number) 10.0.0.0 255.0.0.0 for the R1 Fast Ethernet 0/0 connected interface.
- B. Router R1 should configure ip route 10.0.0.0 255.0.0.0 null 0 for the routes that are received on R1.
- C. Router 10.1.100.10 should configure ip route 10.0.0.0 255.0.0.0 null 0 for the routes that are summarized toward R1.
- D. Router 10.1.100.10 should configure ip summary address eigrp (AS number) 10.0.0.0 255.0.0.0 for the R1 Fast Ethernet 0/0 connected interface.

Answer: D

### NEW QUESTION 9

- (Exam Topic 3)

Refer to the exhibit.



A network administrator is trying to switch to the privileged EXEC level on R1 but failed. Which configuration resolves the issue?

- A. Enable password Cisco@123
- B. tacass server enable-password Cisco@123
- C. tacacs-server enable-password Cisco@123
- D. enable-password Cisco@123

Answer: D



## NEW QUESTION 10

- (Exam Topic 3)

The network administrator configured CoPP so that all HTTP and HTTPS traffic from the administrator device located at 172.16.1.99 toward the router CPU is limited to 500 kbps. Any traffic that exceeds this limit must be dropped.

```
access-list 100 permit ip host 172.16.1.99 any
```

```
!
```

```
class-map CM-ADMIN match access-group 100
```

```
!
```

```
policy-map PM-COPP class CM-ADMIN
```

```
police 500000 conform-action transmit
```

```
!
```

```
interface E0/0
```

```
service-policy input PM-COPP
```

CoPP failed to capture the desired traffic and the CPU load is getting higher. Which two configurations resolve the issue? (Choose two.)

A. interface E0/0no service-policy input PM-COPP!control-planeservice-policy input PM-COPP

B. policy-map PM-COPP class CM-ADMINno police 500000 conform-action transmit police 500 conform-action transmit!control-planeservice-policy input PM-COPP

C. no access-list 100access-list 100 permit tcp host 172.16.1.99 any eq 80

D. no access-list 100access-list 100 permit tcp host 172.16.1.99 any eq 80access-list 100 permit tcp host 172.16.1.99 any eq 443

E. policy-map PM-COPP class CM-ADMINno police 500000 conform-action transmit police 500 conform-action transmit

**Answer: A**

## NEW QUESTION 10

- (Exam Topic 3)

Which router translates the customer routing information into VPNv4 routes to exchange VPNv4 routes with other devices through MP-BGP?

A. PE

B. CE

C. P

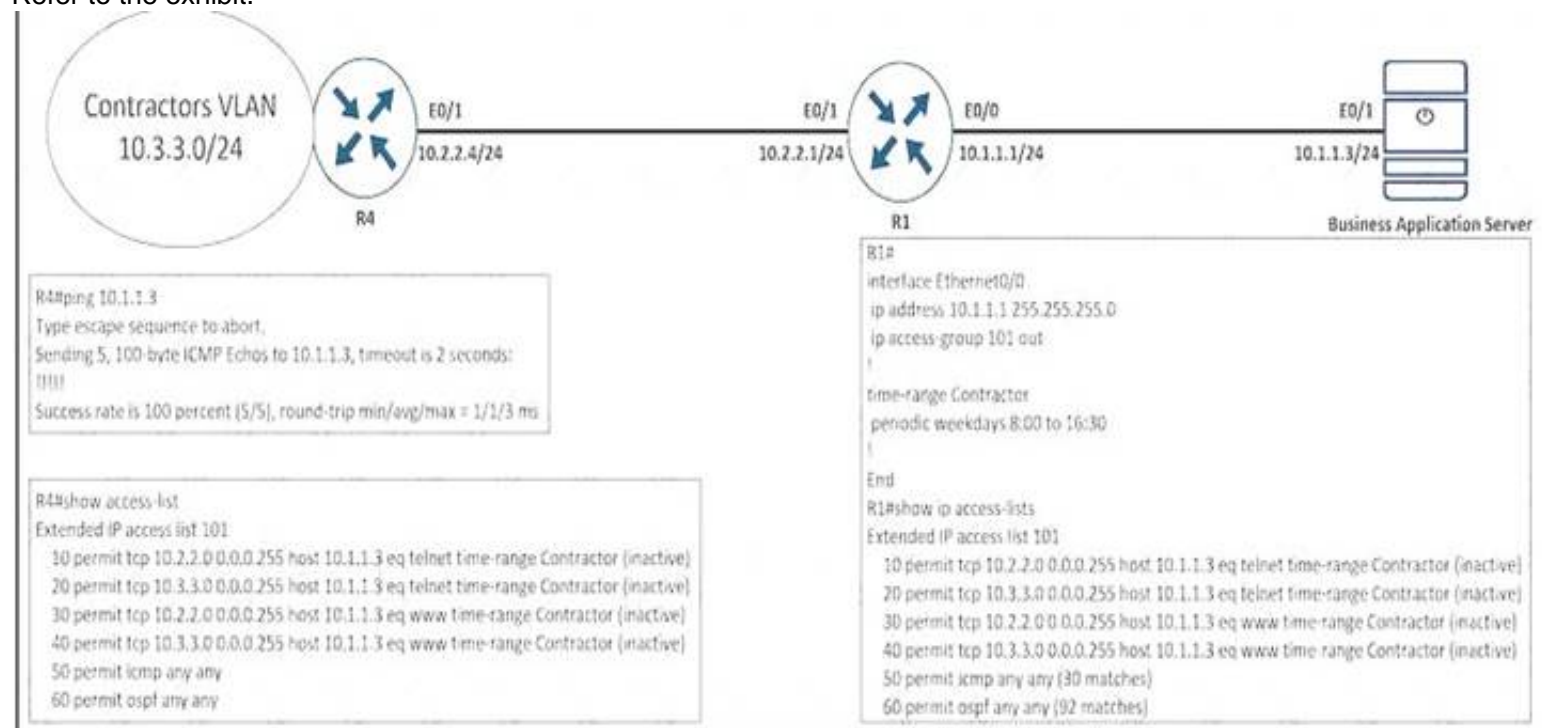
D. VPNv4 RR

**Answer: A**

## NEW QUESTION 12

- (Exam Topic 3)

Refer to the exhibit.



An engineer is troubleshooting failed access by contractors to the business application server via Telnet or HTTP during the weekend. Which configuration resolves the issue?

A)

**R1**

**time-range Contractor**

**no periodic weekdays 8:00 to 16:30**

**periodic daily 8:00 to 16:30**

B)

**R4**

**time-range Contractor**

**no periodic weekdays 17:00 to 23:59**

**periodic daily 8:00 to 16:30**

C)

**R4**

**no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor**

D)

**R1**

**no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor**

- A. Option
- B. Option
- C. Option
- D. Option

Answer: A

NEW QUESTION 16  
- (Exam Topic 3)

Customer ABC BGP Peering

BGP AS 100  
OSPFv3 IPv6

BGP AS 300  
OSPFv3 IPv6

```
SW100#sh ip bgp ipv6 uni summ
BGP router identifier 100.0.0.1, local AS number 100
BGP table version is 1, main routing table version 1

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:ABC:AABB:1100:1122:1111:2222:AAA1
              4      100      6      5        1    0    0 00:00:58      0

SW100#sh ip bgp ipv6 unicast
SW100#

R1#sh ip bgp ipv6 uni
BGP table version is 4, local router ID is 1.1.1.1
   Network        Next Hop        Metric LocPrf Weight Path
* i  2001::4/128    2001::4          0     100      0 300 i
*>i  2002::2/128    2001::2          0     100      0 i
R1#
R1#sh ipv6 route
O   2001::2/128 [110/1]
    via FE80::5200:C3FF:FE01:E600, GigabitEthernet0/0
B   2002::2/128 [200/0]
    via 2001::2
```

Refer to the exhibit SW100 cannot receive routes from R1 Which configuration resolves the issue?

☐ R1  
 router bgp 100  
 address-family ipv6  
 neighbor 2001::2 route-reflector-client  
 neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client

R2  
 router bgp 100  
 address-family ipv6  
 neighbor 2001::2  
 neighbor 2001::1 next-hop-self

☐ R1  
 router bgp 100  
 address-family ipv6  
 neighbor 2001::2 route-reflector-client  
 neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client

R2  
 router bgp 100  
 address-family ipv6  
 neighbor 2001::2  
 neighbor 2001::1 as-override

☐ R1  
 router bgp 100  
 address-family ipv6  
 no synchronization

R2  
 router bgp 100  
 address-family ipv6  
 no synchronization  
 SW100  
 router bgp 100  
 address-family ipv6  
 no synchronization

☐ R1  
 router bgp 100  
 address-family ipv6  
 redistribute connected

R2  
 router bgp 100  
 address-family ipv6  
 redistribute connected

- A. Option A
- B. Option B
- C. Option C
- D. Option C

**Answer: A**

#### NEW QUESTION 17

- (Exam Topic 3)

Refer to the exhibit.

```
R1(config)#ip access-list standard EIGRP-FILTER
R1(config-std-nacl)#permit 10.10.10.0 0.0.0.255
R1(config)#router eigrp 10
R1(config-router)#distribute-list route-map EIGRP in
!
R1(config)#route-map EIGRP permit 10
R1(config-route-map)#match ip address EIGRP-FILTER
!
R1#show ip route eigrp
D      10.10.10.0/24
```

An engineer must filter incoming EIGRP updates to allow only a set of specific prefixes. The distribute list is tested, and it filters out all routes except network 10.10.10.0/24. How should the engineer temporarily allow all prefixes to be learned by the routers again without adjusting the existing access list?

- A. A permit 20 statement should be added before completing the ACL with the required prefixes, and then the permit 20 statement can be removed.
- B. A permit any statement should be added before completing the ACL with the required prefixes and then the permit any statement can be removed.
- C. A continue statement should be added within the permit 10 statement before completing the ACL with the required prefixes, and then the continue statement



can be removed.

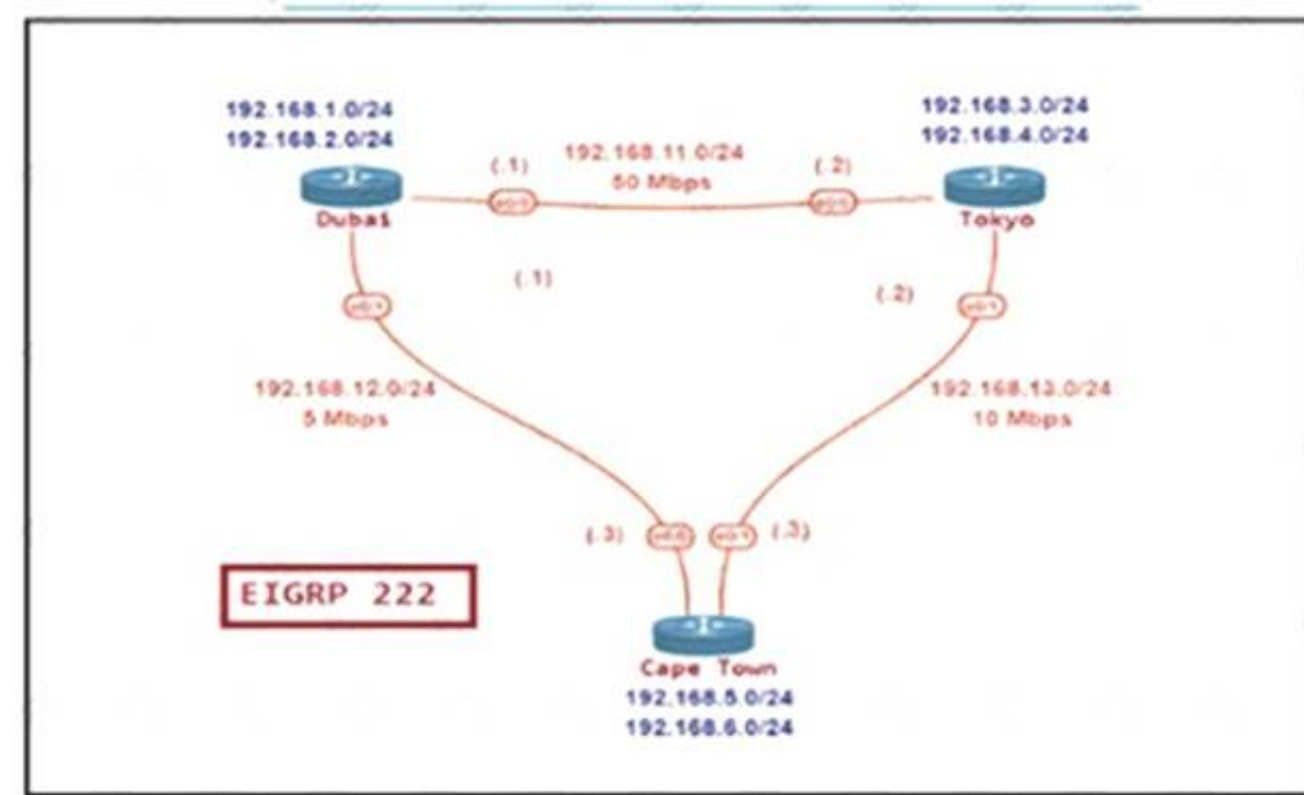
D. An extended access list must be used instead of a standard access list to accomplish the task

**Answer: C**

### NEW QUESTION 18

- (Exam Topic 3)

Refer to the exhibit.



- D 192.168.2.0/24 [90/409600] via 192.168.12.1, 00:09:11, Ethernet0/0
- D 192.168.3.0/24 [90/409600] via 192.168.13.2, 00:17:23, Ethernet0/1
- D 192.168.4.0/24 [90/409600] via 192.168.13.2, 00:17:23, Ethernet0/1
- 192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.5.0/24 is directly connected, Loopback0
- L 192.168.5.1/32 is directly connected, Loopback0
- 192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.6.0/24 is directly connected, Loopback1
- L 192.168.6.1/32 is directly connected, Loopback1
- D 192.168.11.0/24 [90/307200] via 192.168.13.2, 00:17:40, Ethernet0/1
- [90/307200] via 192.168.12.1, 00:17:40, Ethernet0/0
- 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.12.0/24 is directly connected, Ethernet0/0
- L 192.168.12.3/32 is directly connected, Ethernet0/0
- 192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.13.0/24 is directly connected, Ethernet0/1
- L 192.168.13.3/32 is directly connected, Ethernet0/1

The network administrator must configure Cape Town to reach Dubai via Tokyo based on the speeds provided by the service provider. It was noticed that Cape Town is reaching Dubai directly and failed to meet the requirement. Which configuration fixes the issue?

A)

Dubai

```
router eigrp 100
 variance 2
```

B)

CapeTown

```
router eigrp 100
 variance 2
```

C)

CapeTown

```
interface E 0/0
 bandwidth 5000
interface E 0/1
 bandwidth 10000
```

D)

### Cape Town

```
interface E 0/0
bandwidth 5000
interface E 0/1
bandwidth 10000
```

### Dubai

```
interface E 0/0
bandwidth 50000
interface E 0/1
bandwidth 5000
```

### Tokyo

```
interface E 0/0
bandwidth 50000
interface E 0/1
bandwidth 10000
```

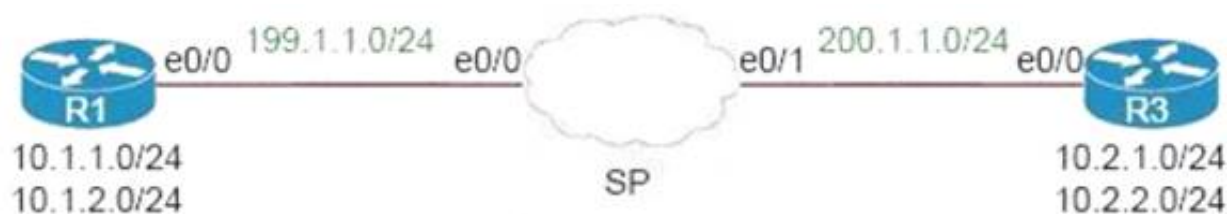
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

### NEW QUESTION 22

- (Exam Topic 3)

Refer to the exhibit.



An engineer must configure a LAN-to-LAN IPsec VPN between R1 and the remote router. Which IPsec Phase 1 configuration must the engineer use for the local router?

- A. crypto isakmp policy 5 authentication pre-share encryption 3des hash sha group 2!crypto isakmp key cisco123 address 200.1.1.3
- B. crypto isakmp policy 5 authentication pre-share encryption 3des hash md5 group 2!crypto isakmp key cisco123 address 200.1.1.3
- C. crypto isakmp policy 5 authentication pre-share encryption 3des hash md5 group 2!crypto isakmp key cisco123 address 199.1.1.1
- D. crypto isakmp policy 5 authentication pre-share encryption 3des hash md5 group 2!crypto isakmp key cisco123! address 199.1.1.1

**Answer: A**

### Explanation:

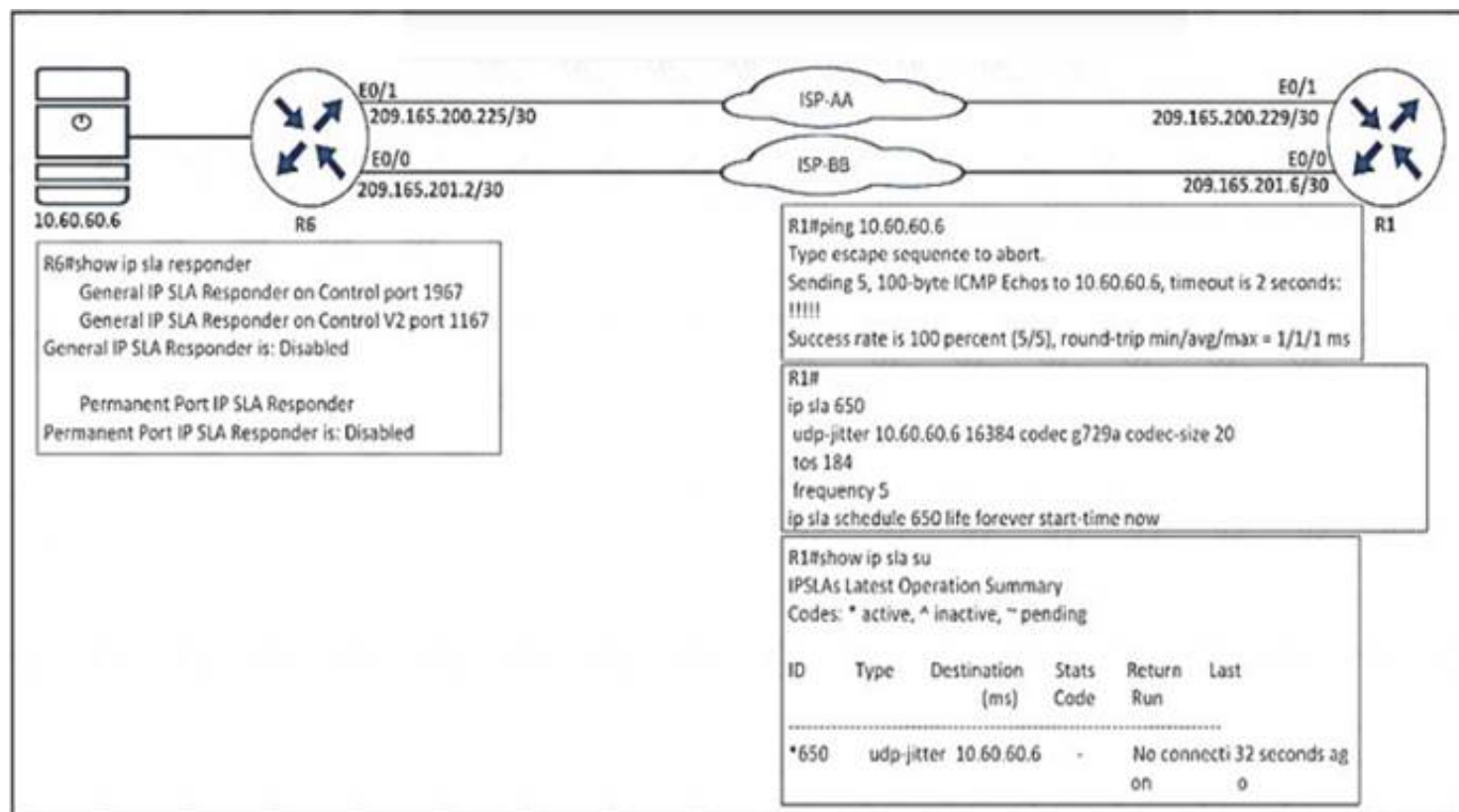
In the “crypto isakmp key ... address” command, the address must be of the IP address of the other end (which is 200.1.1.3 in this case) so Option A and Option B are correct. The difference between these two options are in the hash SHA or MD5 method but both of them can be used although SHA is better than MD5 so we choose Option A the best answer.

Note: Cisco no longer recommends using 3DES, MD5 and DH groups 1, 2 and 5.

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_imgmt/configuration/xr-16-5/sec-ipsec-management-xr-16-5-book/sec-ipsec-usability-enhance.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_imgmt/configuration/xr-16-5/sec-ipsec-management-xr-16-5-book/sec-ipsec-usability-enhance.html)

### NEW QUESTION 26

- (Exam Topic 3)



Refer to the exhibit. Which configuration resolves the IP SLA issue from R1 to the server?

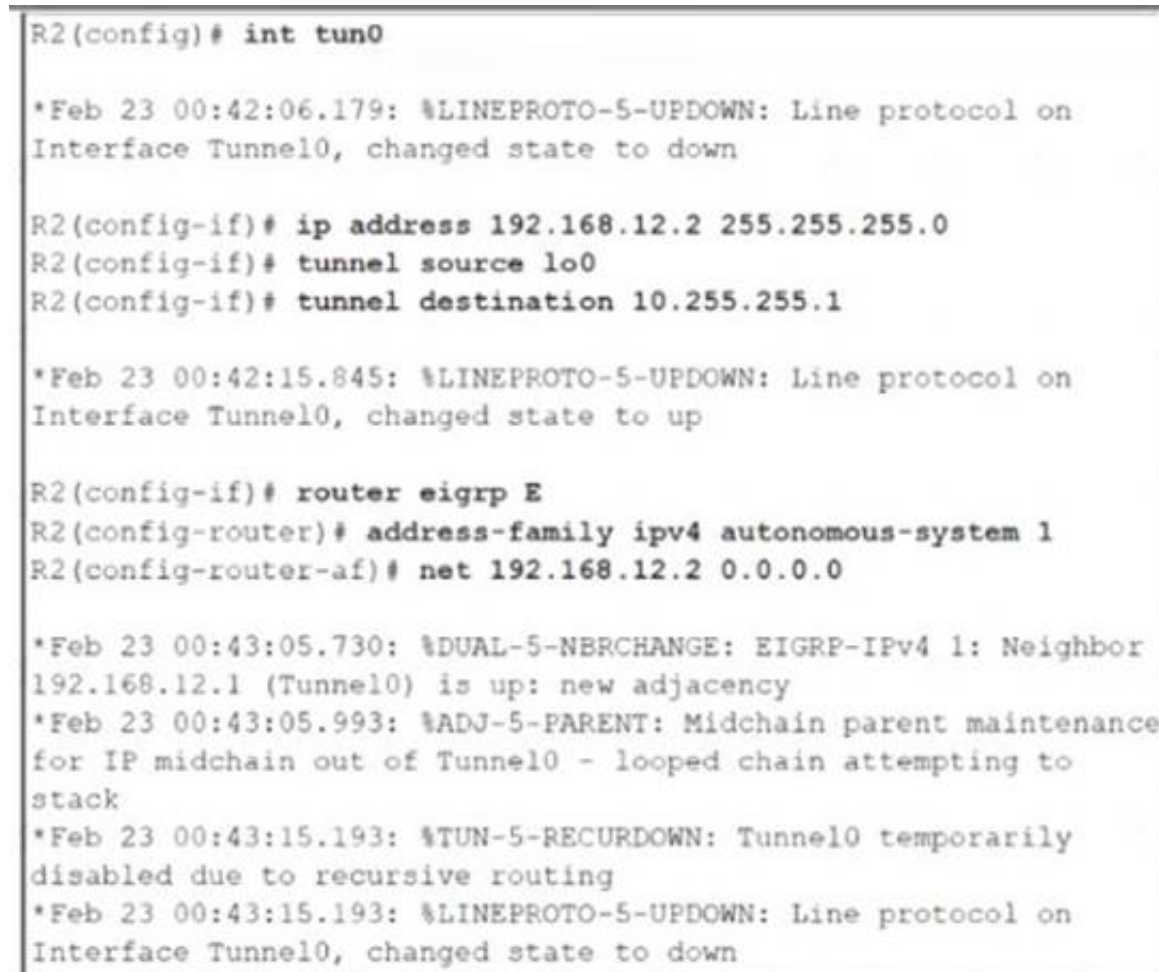
- A. R6(config)#ip sla responder
- B. R6(config)#ip sla responder udp-echo ipaddress 10.60.60.6 po 5000
- C. R6(config)#ip sla 650 R6(config-ip-sla)ff udp-jitter 10.60.60.6
- D. R6(config)#ip sla schedule 10 life forever start-time now

**Answer: A**

#### NEW QUESTION 27

- (Exam Topic 3)

Refer to the exhibit.



An administrator is configuring a GRE tunnel to establish an EIGRP neighbor to a remote router. The other tunnel endpoint is already configured. After applying the configuration as shown, the tunnel started flapping. Which action resolves the issue?

- A. Stop sending a route matching the tunnel destination across the tunnel.
- B. Modify the network command to use the Tunnel0 Interface netmask.
- C. Advertise the Loopback0 interface from R2 across the tunnel.
- D. Readdress the IP network on the Tunnel0 on both routers using the /31 netmask.

**Answer: A**

#### NEW QUESTION 32

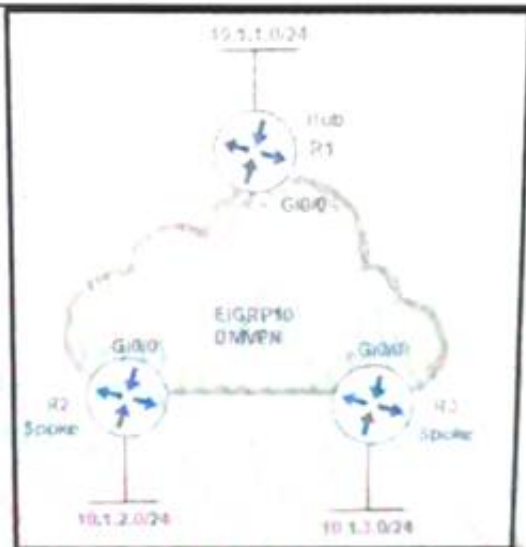
- (Exam Topic 3)

Refer to the exhibit.



```
R2#show ip route eigrp | include 10.1.
D    10.1.1.0/24

R3#show ip route eigrp | include 10.1.
D    10.1.1.0/24
```



An engineer configures DMVPN and receives the hub location prefix of 10.1.1.0/24 on R2 and R3. The R3 prefix of 10.1.3.0/24 is not received on R2, and the R2 prefix 10.1.2.0/24 is not received on R3. Which action resolves the issue?

- A. Split horizon prevents the routes from being advertised between spoke routers; it should be disabled with the command `no ip split-horizon eigrp 10` on the tunnel interface of R1.
- B. There is no spoke-to-spoke connection; DMVPN configuration should be modified to enable a tunnel connection between R2 and R3 and neighbor relationship confirmed by use of the `show ip eigrp neighbor` command.
- C. Split horizon prevents the routes from being advertised between spoke routers; it should be disabled with the `no ip split-horizon eigrp 10` command on the Gi0/0 interface of R1.
- D. There is no spoke-to-spoke connection; DMVPN configuration should be modified with a manual neighbor relationship configured between R2 and R3 and confirmed by use of the `show ip eigrp neighbor` command.

**Answer:** A

#### Explanation:

In this topology, the Hub router will receive advertisements from R2 Spoke router on its tunnel interface. The problem here is that it also has a connection with R3 Spoke on that same tunnel interface. If we don't disable split-horizon, then the Hub will not relay routes from R2 to R3 and the other way around. That is because it received those routes on the same interface (tunnel) and therefore it cannot advertise back out that same interface (split-horizon rule). Therefore, we must disable split-horizon on the Hub router to make sure the Spokes know about each other.

#### NEW QUESTION 36

- (Exam Topic 3)

What is a function of BFD?

- A. peer recovery after a Layer 3 protocol adjacency failure
- B. peer recovery after a Layer 2 adjacency failure
- C. failure detection independent of routing protocols and media types
- D. failure detection dependent on routing protocols and media types

**Answer:** D

#### NEW QUESTION 40

- (Exam Topic 3)

Refer to the exhibit.

A network administrator is troubleshooting OSPF adjacency issue by going through the console logs in the router, but due to an overwhelming log message stream, it is impossible to capture the problem. Which two commands reduce console log messages to relevant OSPF neighbor problem details so that the issue can be resolved? (Choose two)

- A. `debug condition interface`
- B. `debug condition ip`
- C. `debug condition ospf neighbor`
- D. `debug condition session-id ADJCHG`
- E. `debug condition all`

**Answer:** AD

#### NEW QUESTION 44

- (Exam Topic 3)

What is considered the primary advantage of running BFD?

- A. reduction in time needed to detect Layer 2 switched neighbor failures
- B. reduction in time needed to detect Layer 3 routing neighbor failures
- C. reduction in CPU needed to detect Layer 2 switch neighbor failures
- D. reduction in CPU needed to detect Layer 3 routing neighbor failures

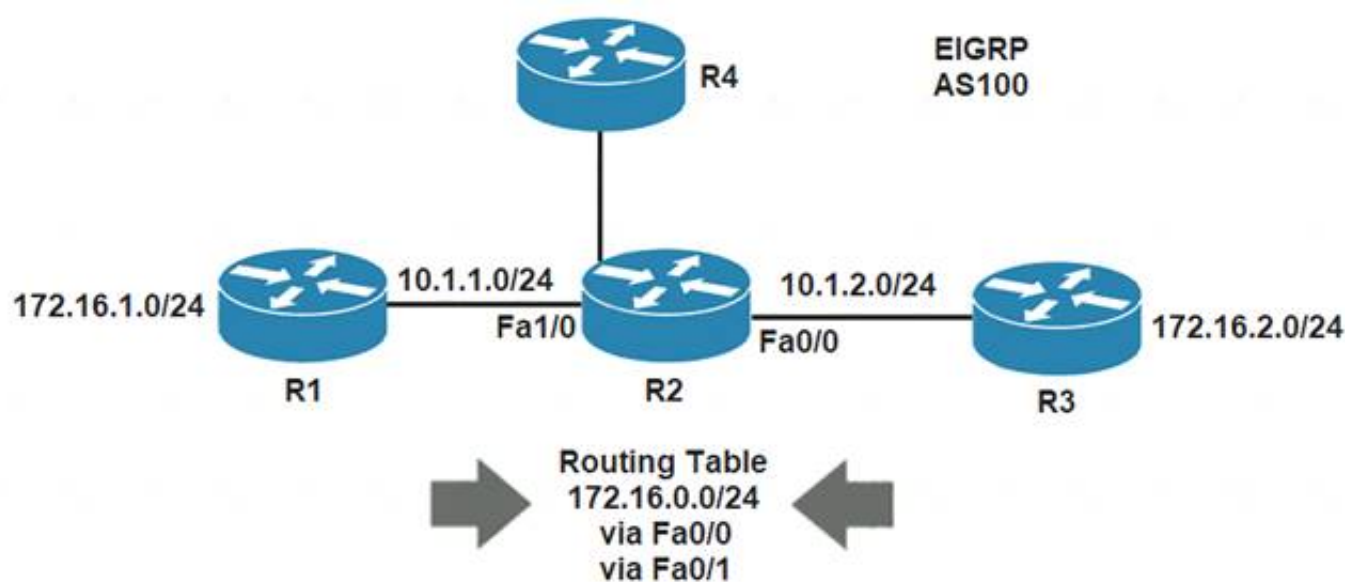


Answer: B

#### NEW QUESTION 49

- (Exam Topic 3)

Refer to the exhibit.



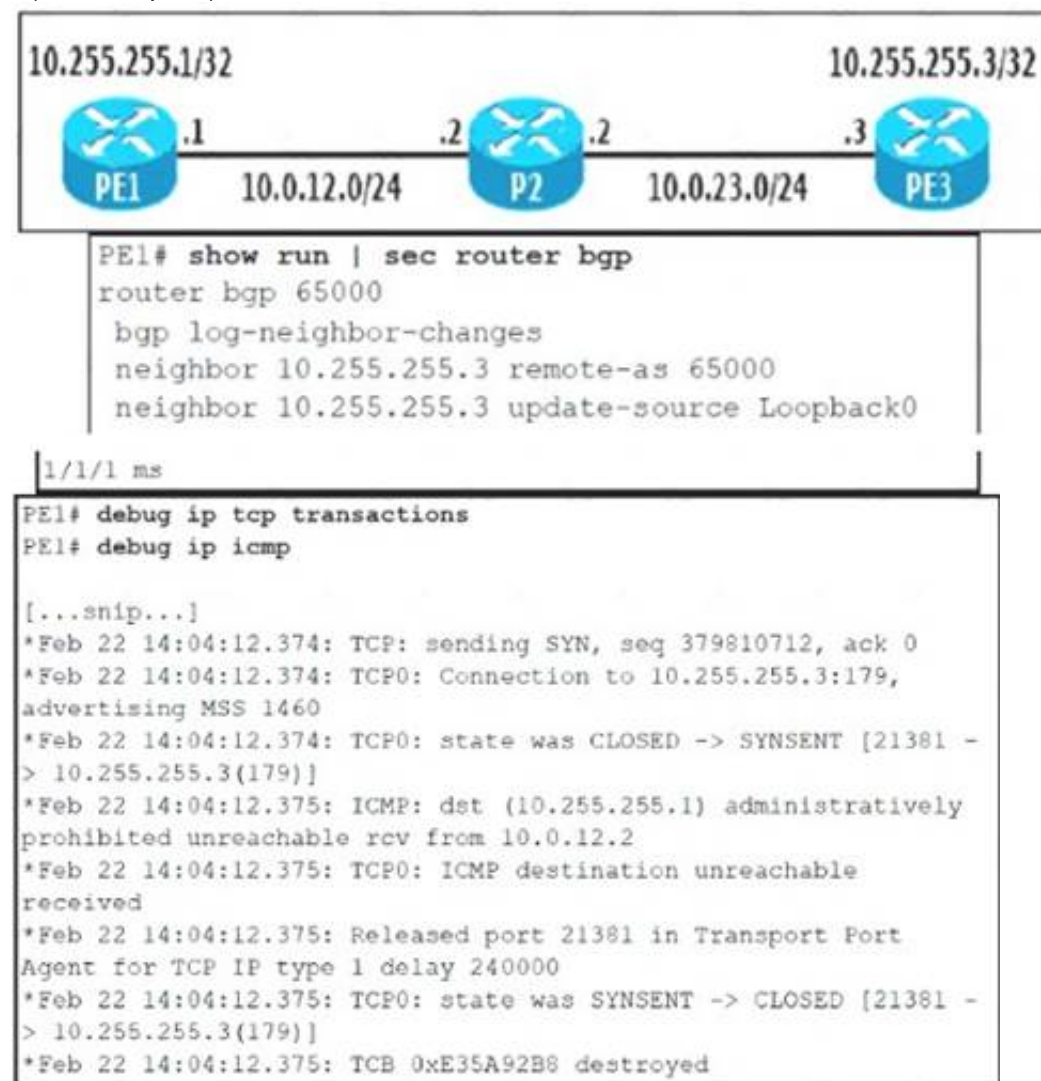
R4 is experiencing packet drop when trying to reach 172.16.2.7 behind R2. Which action resolves the issue?

- A. Insert a /16 floating static route on R2 toward R3 with metric 254
- B. Insert a /24 floating static route on R2 toward R3 with metric 254
- C. Enable auto summarization on all three routers R1, R2, and R3
- D. Disable auto summarization on R2

Answer: D

#### NEW QUESTION 54

- (Exam Topic 3)



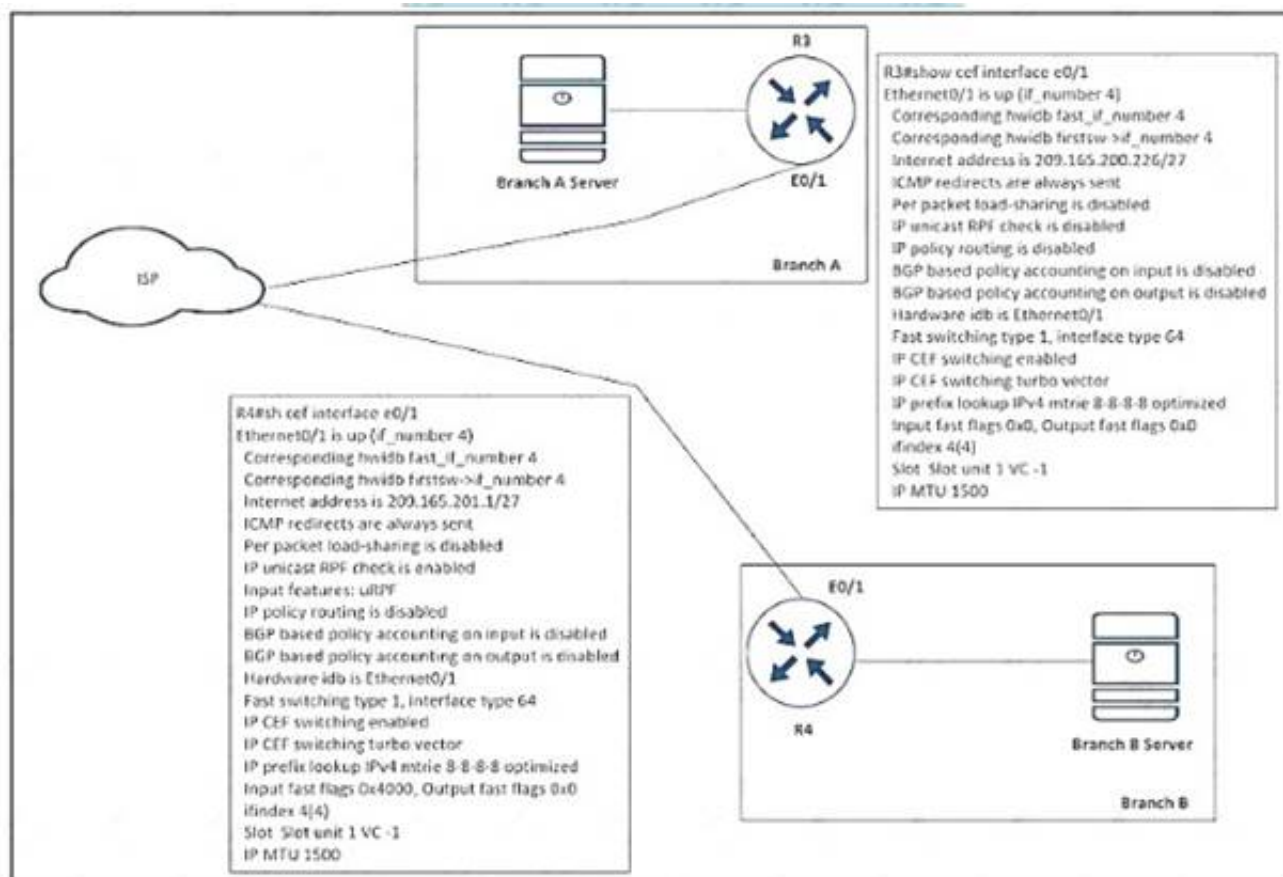
Refer to the exhibit. The administrator is troubleshooting a BGP peering between PE1 and PE3 that is unable to establish Which action resolves the issue?

- A. P2 must have a route to PE3 to establish a BGP session to PE1
- B. Disable sending ICMP unreachables on P2 to allow PE1 to establish a session with PE3
- C. Ensure that the PE3 loopback address is used as a source for BGP peering to PE1
- D. Remove the traffic filtering rules on P2 blocking the BGP communication between PE1 and PE3

Answer: C

#### NEW QUESTION 58

- (Exam Topic 3)



Refer to the exhibit.

A shoe retail company implemented the uRPF solution for an antispoofing attack. A network engineer received the call that the branch A server is under an IP spoofing attack. Which configuration must be implemented to resolve the attack?

A)

**R4**  
**interface ethernet0/1**  
**ip unicast RPF check reachable-via any allow-default allow-self-ping**

B)

**R4**  
**interface ethernet0/1**  
**ip verify unicast source reachable-via any allow-default allow-self-ping**

C)

**R3**  
**interface ethernet0/1**  
**ip verify unicast source reachable-via any allow-default allow-self-ping**

D)

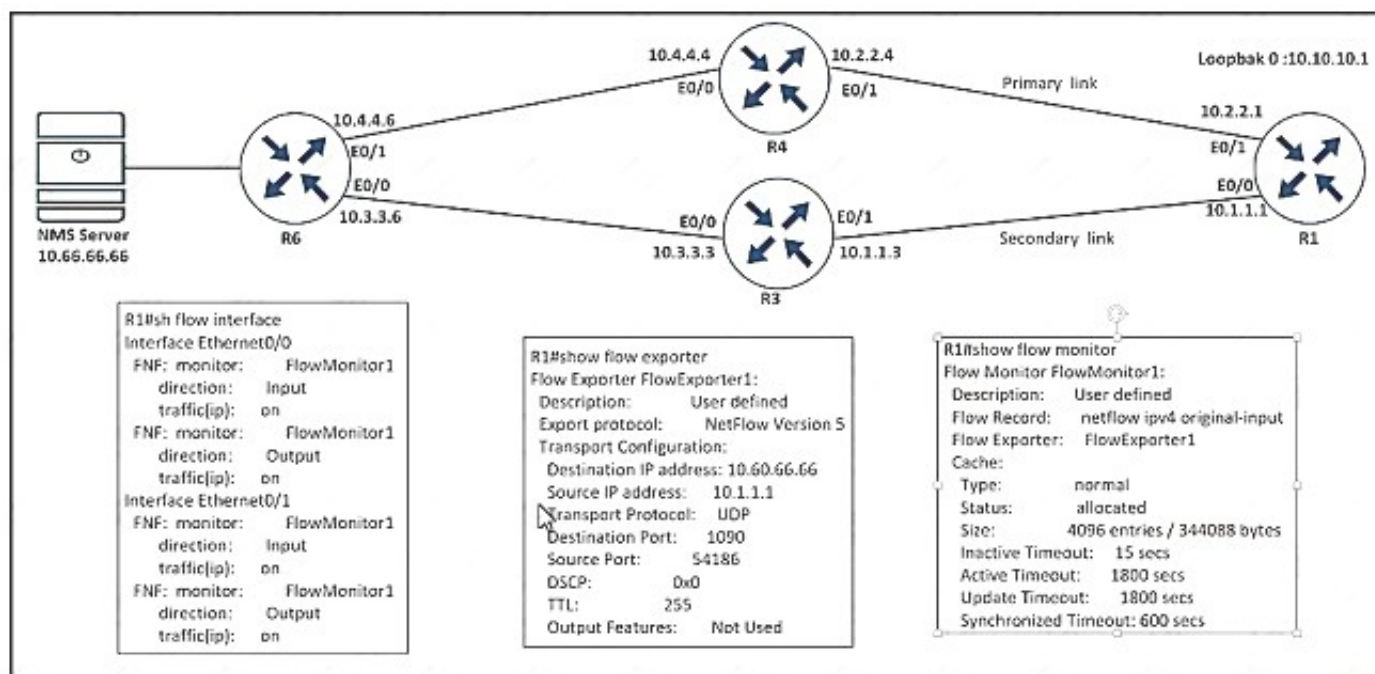
**R3**  
**interface ethernet0/1**  
**ip unicast RPF check reachable-via any allow-default allow-self-ping**

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

**NEW QUESTION 59**

- (Exam Topic 3)



Refer to the exhibit. An engineer configured NetFlow on R1, but the flows do not reach the NMS server from R1. Which configuration resolves this Issue?

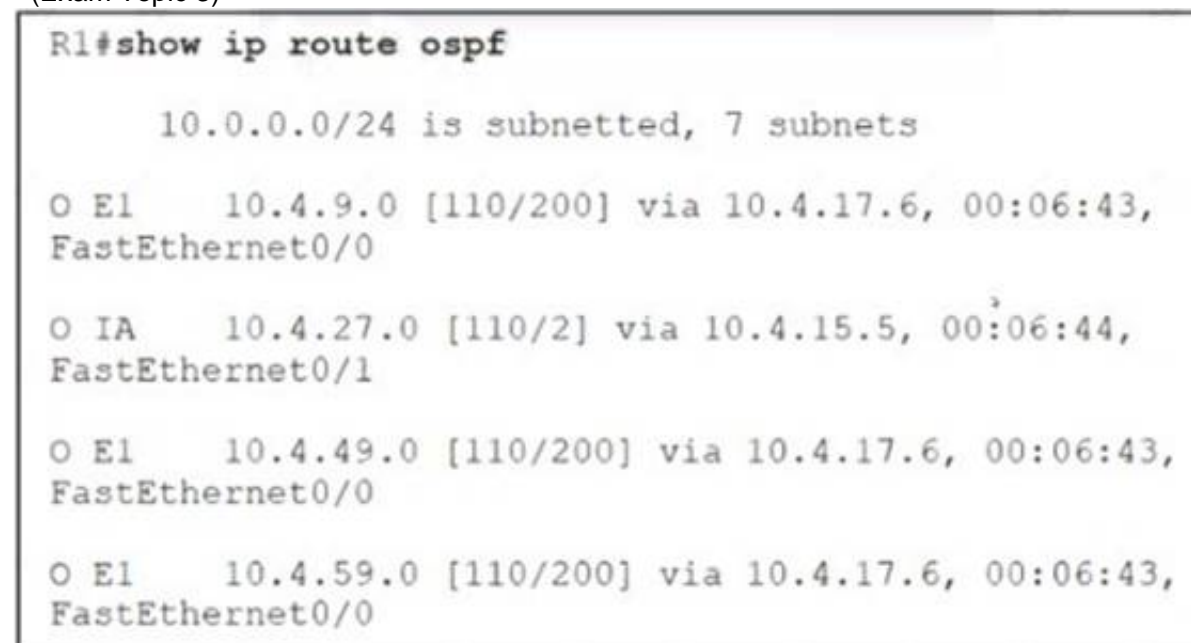
- ☐ R1(config)#flow monitor FlowMonitor1  
R1(config-flow-monitor)#destination 10.66.66.66
- ☐ R1(config)#flow exporter FlowExporter1  
R1(config-flow-exporter)#destination 10.66.66.66
- ☒ R1(config)#interface Ethernet0/0  
R1(config-if)#ip flow monitor Flowmonitor1 input  
R1(config-if)#ip flow monitor Flowmonitor1 output
- ☐ R1(config)#interface Ethernet0/1  
R1(config-if)#ip flow monitor Flowmonitor1 input  
R1(config-if)#ip flow monitor Flowmonitor1 output

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

#### NEW QUESTION 62

- (Exam Topic 3)



Refer to the exhibit. An engineer configured two ASBRs, 10.4.17.6 and 10.4.15.5, in an OSPF network to redistribute identical routes from BGR However, only prefixes from 10.4.17.6 are installed into the routing table on R1. Which action must the engineer take to achieve load sharing for the BGP-originated prefixes?

- A. The ASBRs are advertising the redistributed prefixes with the iBGP metric and must be modified to Type 1 on ASBR 10.4.17.6.
- B. The ASBRs are advertising the redistributed prefixes with a different admin distance and must be changed to 110 on ASBR 10.4.15.5.
- C. The admin distance of the prefixes must be adjusted to 20 on ASBR 10.4.15.5 to advertise prefixes to R1 identically from both ASBRs.
- D. The ASBRs are advertising the redistributed prefixes as Type 1 and must be modified to Type 2

**Answer: D**

#### NEW QUESTION 66

- (Exam Topic 3)

Refer to the exhibit.



```
snmp-server community Public RO 90
snmp-server community Private RW 90
R1#show access-list 90
Standard IP access list 90
  permit 10.11.110.11
  permit 10.11.111.12
```

```
Nov 6 06:45:11: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
10.11.110.12
Nov 6 06:45:12: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
10.11.110.12
```

A network administrator notices these console messages from host 10.11.110.12 originating from interface E1/0. The administrator considers this an unauthorized attempt to access SNMP on R1. Which action prevents the attempts to reach R1 E1/0?

- A. Configure IOS control plane protection using ACL 90 on interface E1/0
- B. Configure IOS management plane protection using ACL 90 on interface E1/0
- C. Create an inbound ACL on interface E1/0 to deny SNMP from host 10.11.110.12
- D. Add a permit statement including the host 10.11.110.12 into ACL 90

**Answer: C**

#### NEW QUESTION 68

- (Exam Topic 3)

```
ip access-list extended CoPP-ICMP
  permit icmp any any echo
!
ip access-list extended CoPP-BGP
  permit tcp any eq bgp any established
!
ip access-list extended CoPP-EIGRP
  permit eigrp any host 224.0.0.10
!
Class-map match-all CoPP-CLASS
  match access-group name CoPP-ICMP
  match access-group name CoPP-BGP
  match access-group name CoPP-EIGRP
!
```

Refer to the exhibit A CoPP policy is implemented to allow specific control traffic, but the traffic is not matching as expected and is getting unexpected behavior of control traffic. Which action resolves the issue?

- A. Use match-any instruction in class-map
- B. Create a separate class map against each ACL.
- C. Create a separate class map for ICMP traffic.
- D. Use default-class to match ICMP traffic

**Answer: A**

#### NEW QUESTION 71

- (Exam Topic 3)

Refer to the exhibit.

```
R1#sh ip route
      10.0.0.0/8 is variably subnetted, 3 subnets, 1 masks
D       10.1.2.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
D       10.1.1.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
```

Although summarization is configured for R1 to receive 10.0.0.0/8, more specific routes are received by R1. How should the 10.0.0.0/8 summary route be received from the neighbor, attached to R1 via Fast Ethernet0/0 interface?

- A. R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0.255.0.0.0 command under the Fast Ethernet 0/0 interface.
- B. The summarization condition is not met Router 10 1 100.10 requires a route for 10 0.0.0/8 that points to null 0
- C. The summarization condition is not met
- D. The network 10.1.100.0/24 should be changed to 172.16.0.0/24.
- E. R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0 0.0.0.255 command under the Fast Ethernet 0/0 interface.



Answer: D

#### NEW QUESTION 74

- (Exam Topic 3)

A company is expanding business by opening 35 branches over the Internet. A network engineer must configure DMVPN at the branch routers to connect with the hub router and allow NHRP to add spoke routers securely to the multicast NHRP mappings automatically Which configuration meets this requirement at the hub router?

A)

```
interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1
ip nhrp nhs dynamic
ip nhrp network-id 10
tunnel mode mgre auto
```

B)

```
interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1
ip nhrp registration no-unique
ip nhrp network-id 10
tunnel mode gre nmba
```

C)

```
interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1
ip nhrp map multicast dynamic
ip nhrp network-id 10
tunnel mode gre multipoint
```

D)

```
interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1
ip nhrp map multicast 224.0.0.0
ip nhrp network-id 10
tunnel mode gre ipv4
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

#### Explanation:

The command “ip nhrp map multicast dynamic” allows NHRP to automatically add spoke routers to the multicast NHRP mappings.

#### NEW QUESTION 76

- (Exam Topic 3)

```
*Sep 3 23:18:21.264: EIGRP: Neighbor (10.1.2.192) not yet found
*Sep 3 23:19:18.675: Going down: Peer 10.1.2.1 total=2 stub 0, iib-stub=0 iid-all=0
*Sep 3 23:19:18.675: EIGRP: Handle deallocation failure [1]
*Sep 3 23:19:18.675: EIGRP: Neighbor 10.1.2.1 went down on Tunnel1.
*Sep 3 23:19:22.943: EIGRP: New peer 10.1.2.1.
*Sep 3 23:19:22.943: %DUAL-5-NBRCHANGE: EIGRP-IPv4 3111: Neighbor 10.1.2.1 (Tunnel1) is up: new adjacency
```

Refer to the exhibit. Which configuration command establishes an EIGRP neighbor adjacency between the hub and spoke?

- A. connected 10.1.2.192 command on spoke router
- B. network 10.1.2.192 command on spoke router
- C. eigrp-peer 10.1.2.192 command on the hub router
- D. neighbor 10.1.2.192 command on hub router

Answer: D

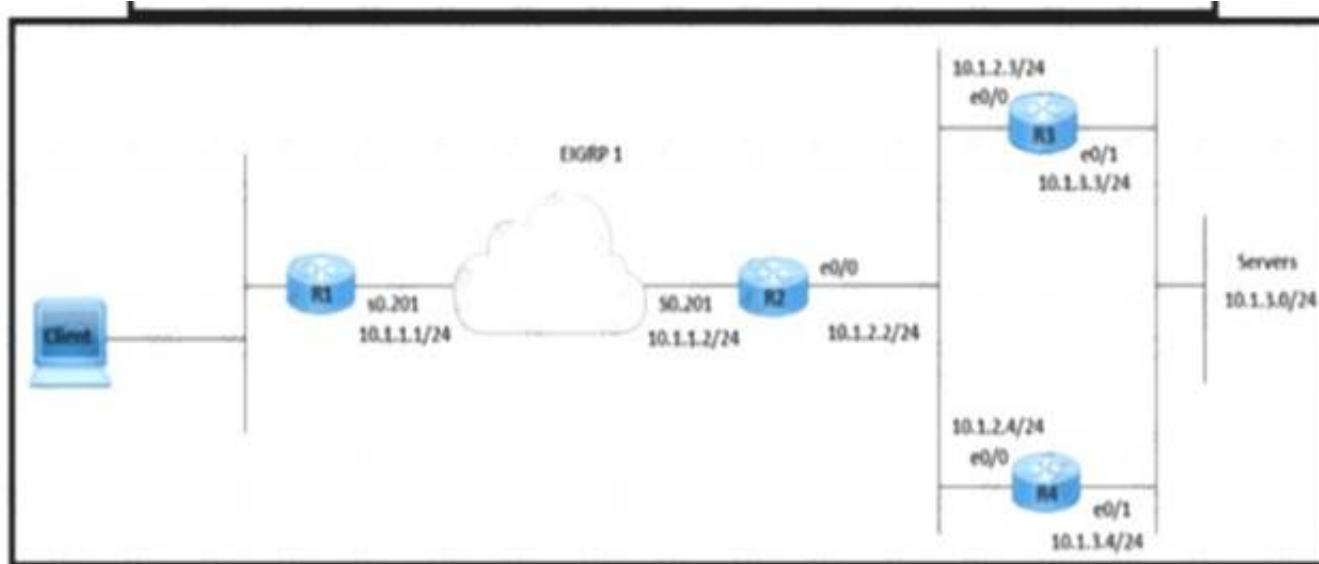
#### NEW QUESTION 79

- (Exam Topic 3)

Exhibit.

```
R2# show ip eigrp topology 10.1.3.0 255.255.255.0

IP-EIGRP (AS 1): topology entry for 10.1.3.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 307200
Routing Descriptor Blocks:
 10.1.2.3 (Ethernet0), from 10.1.2.3, Send flag is 0x0
    Composite metric is (307200/281600), Route is Internal
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 2000 microseconds
      Reliability is 255/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 1
 10.1.2.4 (Ethernet0), from 10.1.2.4, Send flag is 0x0
    Composite metric is (312320/286720), Route is Internal
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 2200 microseconds
      Reliability is 255/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 1
```



Refer to the exhibit. A network is configured for EIGRP equal-cost load balancing, but the traffic destined to the servers is not load balanced. Link metrics from router R2 to R3 and R4 are the same. Which delay value must be configured to resolve the issue?

- A. 208 on R3 E0/0
- B. 120 on R4 E0/1
- C. 120 on R3 E0/1
- D. 2200 on R4 E0/1

**Answer: C**

## NEW QUESTION 82

- (Exam Topic 3)

What are two characteristics of IPv6 Source Guard? (Choose two.)

- A. requires IPv6 snooping on Layer 2 access or trunk ports
- B. used in service provider deployments to protect DDoS attacks
- C. requires the user to configure a static binding
- D. requires that validate prefix be enabled
- E. recovers missing binding table entries

**Answer: DE**

## Explanation:

IPv6 Source Guard uses the IPv6 First-Hop Security Binding Table to drop traffic from unknown sources or bogus IPv6 addresses not in the binding table. The switch also tries to recover from lost address information, querying DHCPv6 server or using IPv6 neighbor discovery to verify the source IPv6 address after dropping the offending packet(s).

Reference: <https://blog.ipspace.net/2013/07/first-hop-ipv6-security-features-in.html>

## NEW QUESTION 85

- (Exam Topic 3)

An engineer received a ticket about a router that has reloaded. The monitoring system graphs show different traffic patterns between logical and physical interfaces when the router is rebooted. Which action resolves the issue?

- A. Configure the snmp ifindex persist command globally.
- B. Clear the logical interfaces with snmp ifindex clear command
- C. Configure the snmp ifindex persist command on the physical interfaces.
- D. Trigger a new snmpwalk from the monitoring system to synchronize interface OIDs

**Answer: A**

### NEW QUESTION 88

- (Exam Topic 3)

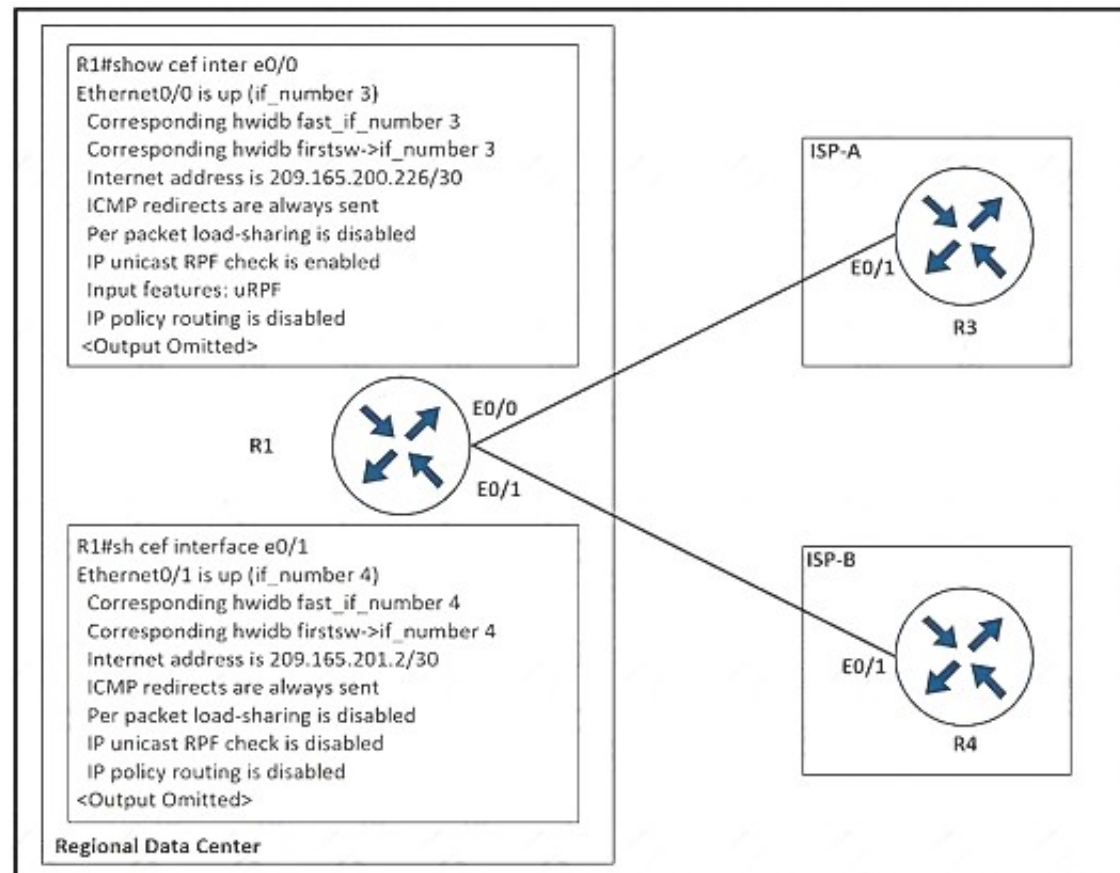
An engineer notices that R1 does not hold enough log messages to identify the root cause during troubleshooting. Which command resolves this issue?

- A. #logging buffered 4096 critical
- B. (config)#logging buffered 16000 informational
- C. #logging buffered 16000 critical
- D. (config)#logging buffered 4096 informational

**Answer: B**

### NEW QUESTION 90

- (Exam Topic 3)



Refer to the exhibit. The company implemented uRPF to address an antispoofing attack. A network engineer received a call from the IT security department that the regional data center is under an IP attack. Which configuration must be implemented on R1 to resolve this issue?

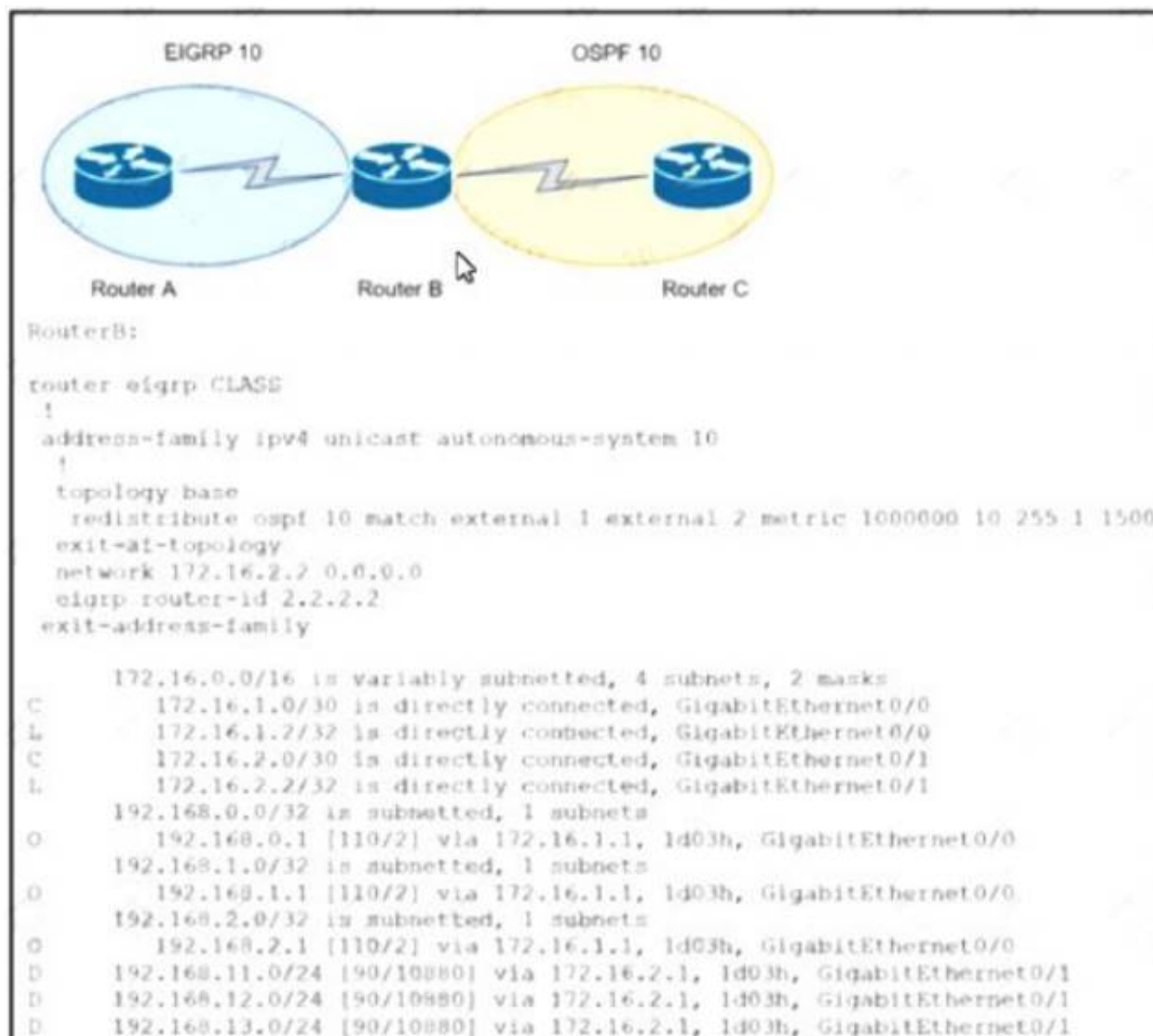
- ☐ interface ethernet0/0  
ip verify unicast reverse-path
- ☐ interface ethernet0/1  
ip verify unicast reverse-path
- ☒ interface ethernet0/1  
ip unicast RPF check reachable-via any allow-default allow-self-ping
- ☐ interface ethernet0/0  
ip unicast RPF check reachable-via any allow-default allow-self-ping

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

### NEW QUESTION 95

- (Exam Topic 3)



Refer to the exhibit. An engineer configured route exchange between two different companies for a migration project EIGRP routes were learned in router C but no OSPF routes were learned in router A. Which configuration allows router A to receive OSPF routes?

- A. (config-router-af)#redistribute ospf 10 1000000 10 255 1 1500
- B. (config-router-af-topology)#redistribute ospf 10 metric 1000000 10 255 1 1500
- C. (config-router-af-topology)#redistribute connected
- D. (config-router-af-topology)#no redistribute ospf 10 match external 1 external 2 metric 1000000 10 255 1 1500

**Answer: B**

#### NEW QUESTION 99

- (Exam Topic 3)

Which feature minimizes DoS attacks on an IPv6 network?

- A. IPv6 Binding Security Table
- B. IPv6 Router Advertisement Guard
- C. IPv6 Prefix Guard
- D. IPv6 Destination Guard

**Answer: D**

#### Explanation:

The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs address resolutions only for those addresses that are active on the link, and requires the FHS binding table to be populated with the help of the IPv6 snooping feature. The feature enables the filtering of IPv6 traffic based on the destination address, and blocks the NDP resolution for destination addresses that are not found in the binding table. By default, the policy drops traffic coming for an unknown destination.

Reference: [https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600\\_1\\_5\\_0s\\_book/IPv6\\_Security.pdf](https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_1_5_0s_book/IPv6_Security.pdf)

#### NEW QUESTION 102

- (Exam Topic 3)



```
R4#
interface FastEthernet1/0
ip address 10.1.1.14 255.255.255.252
ip access-group VENDOR in
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 EIGRPKEY
speed 100
full-duplex
!
interface loopback 100
ip address 10.199.100.1 255.255.255.255
!
router eigrp 100
network 10.1.1.8 0.0.0.3
network 10.1.1.12 0.0.0.3
no auto-summary
eigrp router-id 100.4.4.4
neighbor 10.1.1.13 FastEthernet1/0
redistribute connected
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 100.4.4.4 mask 255.255.255.255
neighbor 10.1.1.13 remote-as 65001
no auto-summary
!
ip access-list extended VENDOR
permit tcp 192.168.32.0 0.0.7.255 host 10.199.100.1 eq 22 time-range VENDOR_ACCESS
!
time-range VENDOR_ACCESS
periodic weekend 22:00 to 23:00
```

Refer to the exhibit A network engineer received a call from the vendor for a failed attempt to remotely log in to their managed router loopback interface from 192.168.40.15 Which action must the network engineer take to resolve the issue?

- A. The IP access list VENDOR must be applied to interface loopback 100
- B. The time-range configuration must be changed to use absolute instead of periodic
- C. The EIGRP configuration must be updated to include a network statement for loopback 100
- D. The source IP summarization must be updated to include the vendor source IP address

**Answer: C**

#### NEW QUESTION 106

- (Exam Topic 3)

Which two technologies optimize MPLS infrastructure using bandwidth protection services when experiencing slow response? (Choose two.)

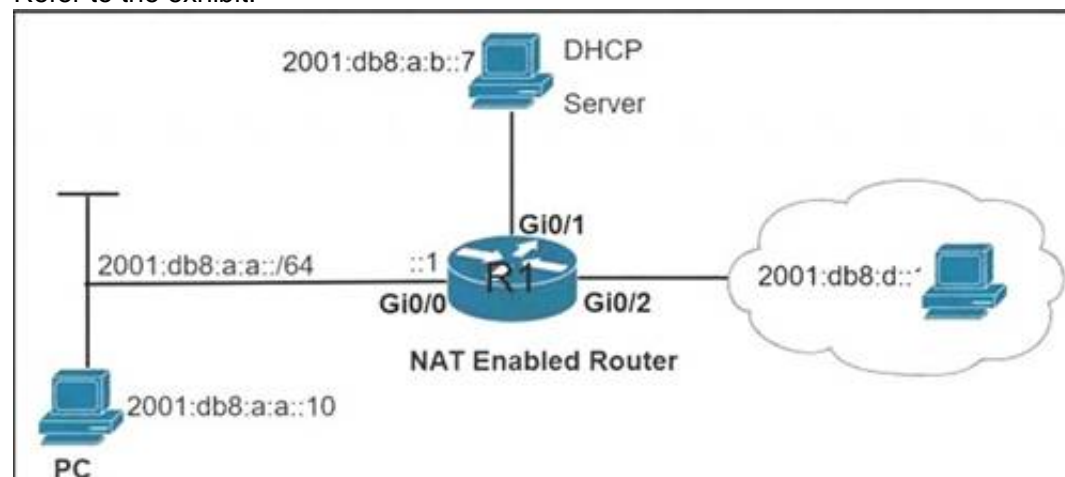
- A. IPLFA
- B. MPLS OAM
- C. VPLS
- D. SO-MPLS
- E. Fast-Rwroute

**Answer: AE**

#### NEW QUESTION 109

- (Exam Topic 3)

Refer to the exhibit.



```
C:\PC> ping 2001:db8:a:b::7
Pinging 2001:db8:a:b::7 with 32 bytes of data:
Reply from 2001:db8:a:b::7: time=46ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Ping statistics for 2001:db8:a:b::7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 40ms, Maximum = 46ms, Average = 41ms

R1# telnet 2001:db8:a:b::7
Trying 2001:DB8:A:B::7 ... Open
User Access Verification
Password:

R1# show ipv6 access-list TSHOOT
IPv6 access list TSHOOT
deny tcp any host 2001:DB8:A:B::7 eq telnet (6 matches) sequence 10
permit tcp host 2001:DB8:A:A::10 host 2001:DB8:A:B::7 eq telnet sequence 20
permit tcp host 2001:DB8:A:A::10 host 2001:DB8:D::1 eq www sequence 30
permit ipv6 2001:DB8:A:A::/64 any (67 matches) sequence 40
```

An engineer is troubleshooting a failed Telnet session from PC to the DHCP server. Which action resolves the issue?

- A. Remove sequence 30 and add it back to the IPv6 traffic filter as sequence 5.
- B. Remove sequence 20 and add it back to the IPv6 traffic filter as sequence 5.
- C. Remove sequence 10 to add the PC source IP address and add it back as sequence 10.
- D. Remove sequence 20 for sequence 40 in the access list to allow Telnet.

**Answer: B**

#### NEW QUESTION 112

- (Exam Topic 3)

What are two characteristics of a VRF instance? (Choose two)

- A. It is defined by the VPN membership of a customer site attached to a P device.
- B. Each VRF has a different set of routing and CEF tables.
- C. All VRFS share customers routing and CEF tables.
- D. An interface must be associated to one VRF
- E. A customer site can be associated to different VRFs.

**Answer: BD**

#### NEW QUESTION 115

- (Exam Topic 3)

Which IPv6 first hop security feature controls the traffic necessary for proper discovery of neighbor device operation and performance?

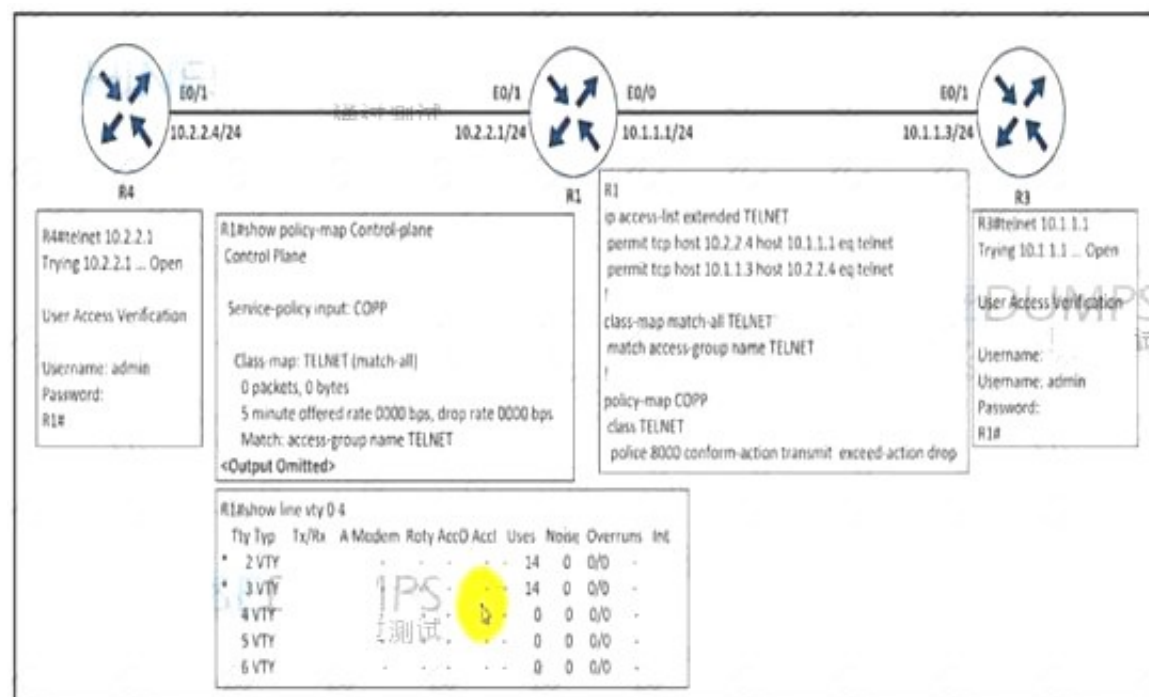
- A. RA Throttling
- B. Source or Destination Guard
- C. ND Multicast Suppression
- D. IPv6 Snooping

**Answer: D**

#### NEW QUESTION 117

- (Exam Topic 3)

Refer to the exhibit.



An engineer implemented CoPP to limit Telnet traffic to protect the router CPU. It was noticed that the Telnet traffic did not pass through CoPP Which configuration resolves the issue?

- ☐ policy-map COPP
  - class TELNET
  - police 8000 conform-action transmit exceed-action transmit
- ☐ policy-map COPP
  - class TELNET
  - police 8000 conform-action transmit exceed-action transmit violate-action drop
- ☐ ip access-list extended TELNET
  - permit tcp host 10.2.2.1 host 10.2.2.4 eq telnet
  - permit tcp host 10.1.1.1 host 10.1.1.3 eq telnet
- ☐ ip access-list extended TELNET
  - permit tcp host 10.2.2.4 host 10.2.2.1 eq telnet
  - permit tcp host 10.1.1.3 host 10.1.1.1 eq telnet

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

### NEW QUESTION 121

- (Exam Topic 3)

Refer to the exhibit.

```
crypto isakmp policy 1
 authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication donttell
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface FastEthernet0/0/0
 ip address 172.17.0.1 255.255.255.0
!
interface FastEthernet0/0/1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
!
```

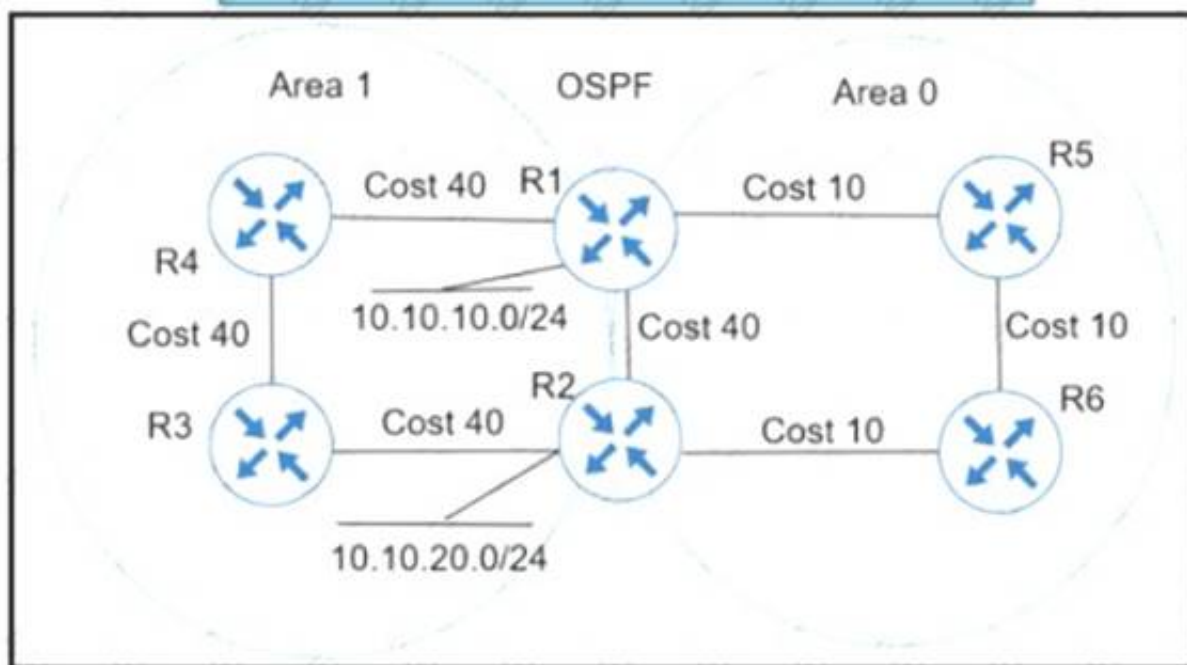
A network administrator must configure DMVPN tunnels between the hub and spoke with dynamic spoke-to-spoke tunnel capabilities using EIGRP. Which tunnel interface command must the network administrator configure to establish an EIGRP peer?

- A. no ip next-hop-self eigrp 1
- B. ip next-hop-self eigrp 1
- C. no ip nhrp next-hop-self
- D. ip nhrp next-hop-self

**Answer: C**

### NEW QUESTION 125

- (Exam Topic 3)



Refer to the exhibit Which action ensures that 10 10 10 0/24 reaches 10 10 20 0/24 through the direct link between R1 and R2?

- A. Configure R1 and R2 LAN links as nonpassive.
- B. Configure R1 and R2 links under area 1
- C. Configure OSPF link cost to 1 between R1 and R2
- D. Configure OSPF path cost to 3 between R1 and R2

**Answer: B**

#### NEW QUESTION 130

- (Exam Topic 3)

Which IPv6 feature enables a device to reject traffic when it is originated from an address that is not stored in the device binding table?

- A. IPv6 Snooping
- B. IPv6 Source Guard
- C. IPv6 DAD Proxy
- D. IPv6 RA Guard

**Answer: B**

#### Explanation:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6\\_fhsec/configuration/xs-3s/ip6f-xe-3s-book/ip6-src-guar](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xs-3s/ip6f-xe-3s-book/ip6-src-guar)

#### NEW QUESTION 134

- (Exam Topic 3)

Refer to the exhibit.

```
access-list 1 permit 209.165.200.215
access-list 2 permit 209.165.200.216
!
interface ethernet 1
ip policy route-map Texas
!
route-map Texas permit 10
match ip address 1
set ip precedence priority
set ip next-hop 209.165.200.217
!
route-map Texas permit 20
match ip address 2
set ip next-hop 209.165.200.218
```

Packets arriving from source 209.165.200.215 must be sent with the precedence bit set to 1, and packets arriving from source 209.165.200.216 must be sent with the precedence bit set to 5. Which action resolves the issue?

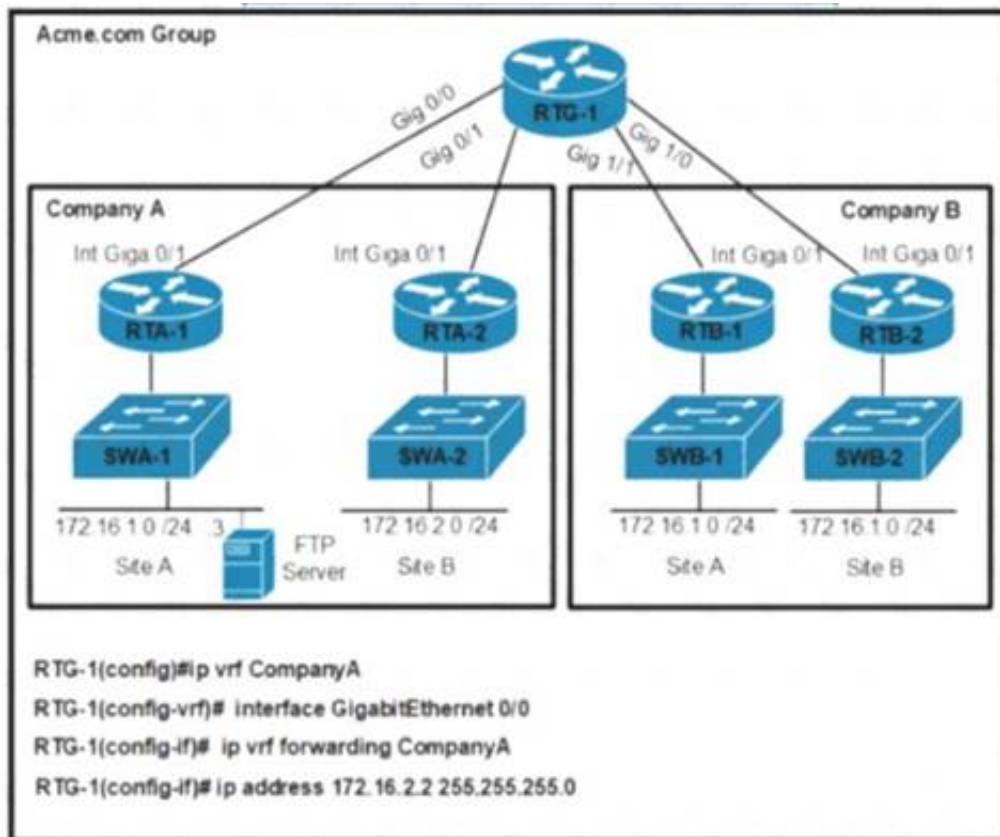
- A. set ip precedence critical in route-map Texas permit 10
- B. set ip precedence critical in route-map Texas permit 20
- C. set ip precedence immediate in route-map Texas permit 10
- D. set ip precedence priority in route-map Texas permit 20

**Answer: B**

#### NEW QUESTION 135

- (Exam Topic 3)





Refer to the exhibit. An engineer must configure a per VRF for TACACS+ for company A. Which configuration on RTG-1 accomplishes the task?

- ☐ aaa new-model  
 aaa group server tacacs+ Tacacscluster  
 server-private 172.16.1.1 port 49 key routing  
 ip tacacs source-interface GigabitEthernet 0/0  
 ip vrf forwarding CompanyA
- ☐ aaa new-model  
 aaa group server tacacs+ Tacacscluster  
 server-private 172.16.1.3 port 49 key routing  
 ip tacacs source-interface GigabitEthernet 0/1  
 ip vrf forwarding CompanyA
- ☐ aaa new-model  
 aaa group server tacacs+ Tacacscluster  
 server-private 172.16.1.1 port 49 key routing  
 ip tacacs source-interface GigabitEthernet 0/1  
 ip vrf CompanyA
- ☐ aaa new-model  
 aaa group server tacacs+ Tacacscluster  
 server-private 172.16.1.3 port 49 key routing  
 ip tacacs source-interface GigabitEthernet 0/0  
 ip vrf CompanyA

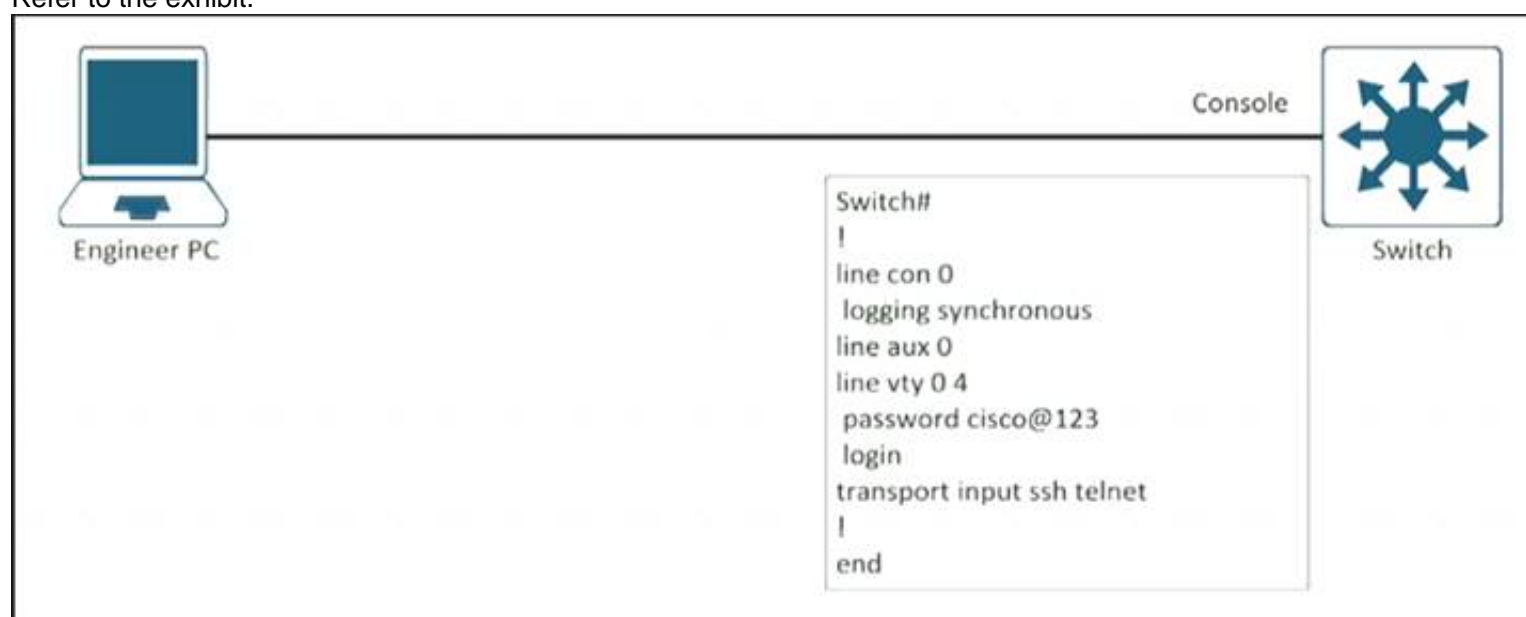
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

#### NEW QUESTION 139

- (Exam Topic 3)

Refer to the exhibit.



An engineer must block access to the console ports for all corporate remote Cisco devices based on the recent corporate security policy but the security team still can connect through the console port. Which configuration on the console port resolves the issue?

- A. transport input telnet
- B. login and password
- C. no exec
- D. exec 0.0

**Answer: C**

**Explanation:**

“no exec” will disable access to a line. It is used if we want to allow only outgoing session (and disable incoming session) so this command will block all console port access.

There is no “exec 0 0” command. We can only find the “exec prompt” command in IOS Version 15.4(2)T4.

```
Router(config-line)#exec ?
  prompt EXEC prompt
  <cr>

Router(config-line)#exec pro
Router(config-line)#exec prompt ?
  timestamp Print timestamps for show commands

Router(config-line)#exec prompt █
```

The most similar command is “exec-timeout 0 0” command, which is used to prevent Telnet/SSH sessions from timing out.

**NEW QUESTION 141**

- (Exam Topic 3)

Which control plane process allows the MPLS forwarding state to recover when a secondary RP takes over from a failed primary RP?

- A. MP-BGP uses control plane services for label prefix bindings in the MPLS forwarding table
- B. LSP uses NSF to recover from disruption \*i control plane service
- C. FEC uses a control plane service to distribute information between primary and secondary processors
- D. LDP uses SSO to recover from disruption in control plane service

**Answer: C**

**NEW QUESTION 146**

- (Exam Topic 3)

An engineer configured VRF-Lite on a router for VRF blue and VRF red. OSPF must be enabled on each VRF to peer to a directly connected router in each VRF. Which configuration forms OSPF neighbors over the network 10.10.10.0/28 for VRF blue and 192.168.0.0/30 for VRF red?

- ☐ router ospf 1 vrf blue  
network 10.10.10.0 0.0.0.15 area 0  
router ospf 2 vrf red  
network 192.168.0.0 0.0.0.3 area 0
- ☐ router ospf 1 vrf blue  
network 10.10.10.0 0.0.0.240 area 0  
router ospf 2 vrf red  
network 192.168.0.0 0.0.0.252 area 0
- ☐ router ospf 1 vrf blue  
network 10.10.10.0 0.0.0.252 area 0  
router ospf 2 vrf red  
network 192.168.0.0 0.0.0.240 area 0
- ☐ router ospf 1 vrf blue  
network 10.10.10.0 0.0.0.3 area 0  
router ospf 2 vrf red  
network 192.168.0.0 0.0.0.15 area 0

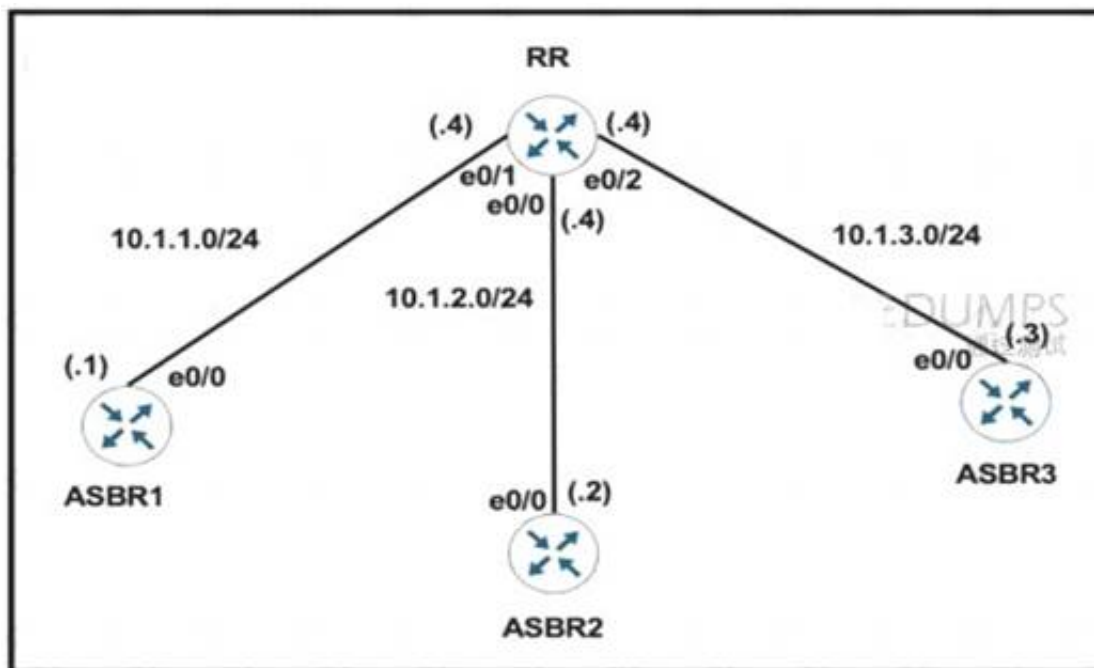
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

# NEW QUESTION 150

- (Exam Topic 3)

Refer to the exhibit.



RR Configuration:

```
router bgp 100
neighbor IBGP peer-group
neighbor IBGP route-reflector-client
neighbor 10.1.1.1 remote-as 100
neighbor 10.1.2.2 remote-as 100
neighbor 10.1.3.3 remote-as 100
```

The network administrator configured the network to establish connectivity between all devices and notices that the ASBRs do not have routes for each other. Which set of configurations resolves this issue?

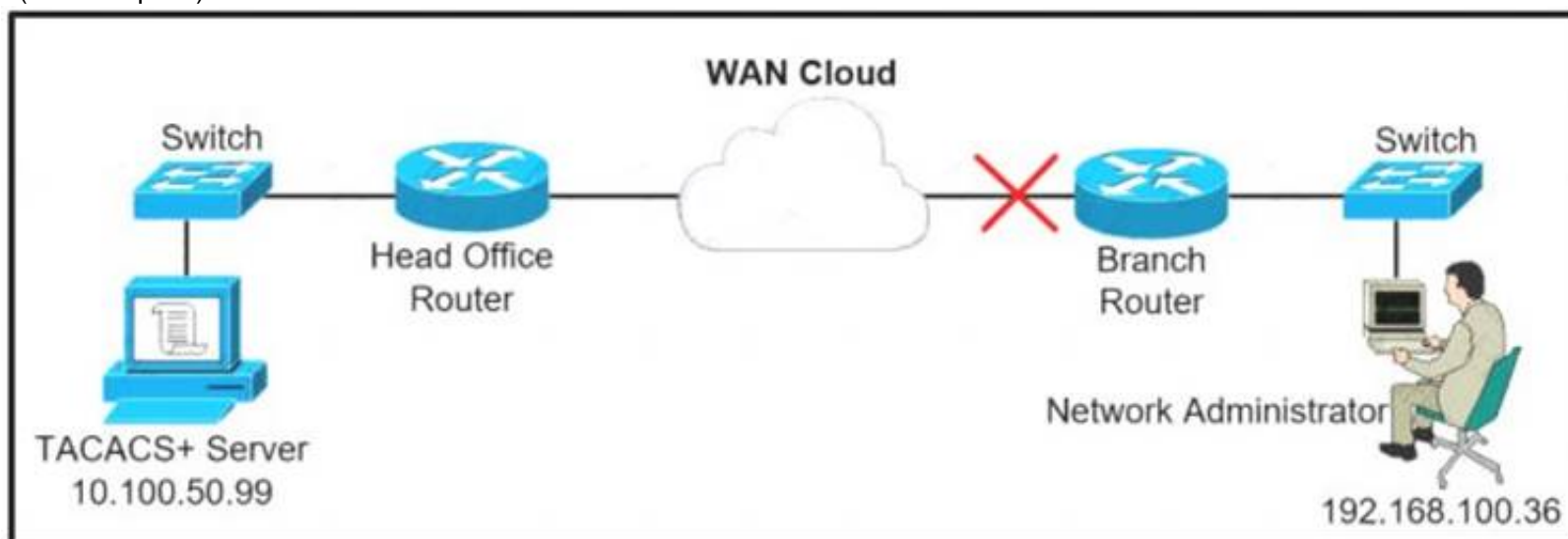
- ☒ router bgp 100
  - neighbor 10.1.1.1 next-hop-self
  - neighbor 10.1.2.2 next-hop-self
  - neighbor 10.1.3.3 next-hop-self
- ☐ router bgp 100
  - neighbor IBGP update-source Loopback0
- ☐ router bgp 100
  - neighbor IBGP next-hop-self
- ☐ router bgp 100
  - neighbor 10.1.1.1 peer-group IBGP
  - neighbor 10.1.2.2 peer-group IBGP
  - neighbor 10.1.3.3 peer-group IBGP

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

# NEW QUESTION 152

- (Exam Topic 3)



A network administrator is trying to access a branch router using TACACS+ username and password credentials, but the administrator cannot log in to the router because the WAN connectivity is down. The branch router has following AAA configuration:

```
aaa new-model
aaa authorization commands 15 default group tacacs+
aaa accounting commands 1 default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
tacacs-server host 10.100.50.99
tacacs-server key Ci$co123
```



Which command will resolve this problem when WAN connectivity is down?

- A. aaa authentication login default group tacacs+ local
- B. aaa authentication login default group tacacs+ enable
- C. aaa authentication login default group tacacs+ console
- D. aaa authentication login console group tacacs+ enable

**Answer: A**

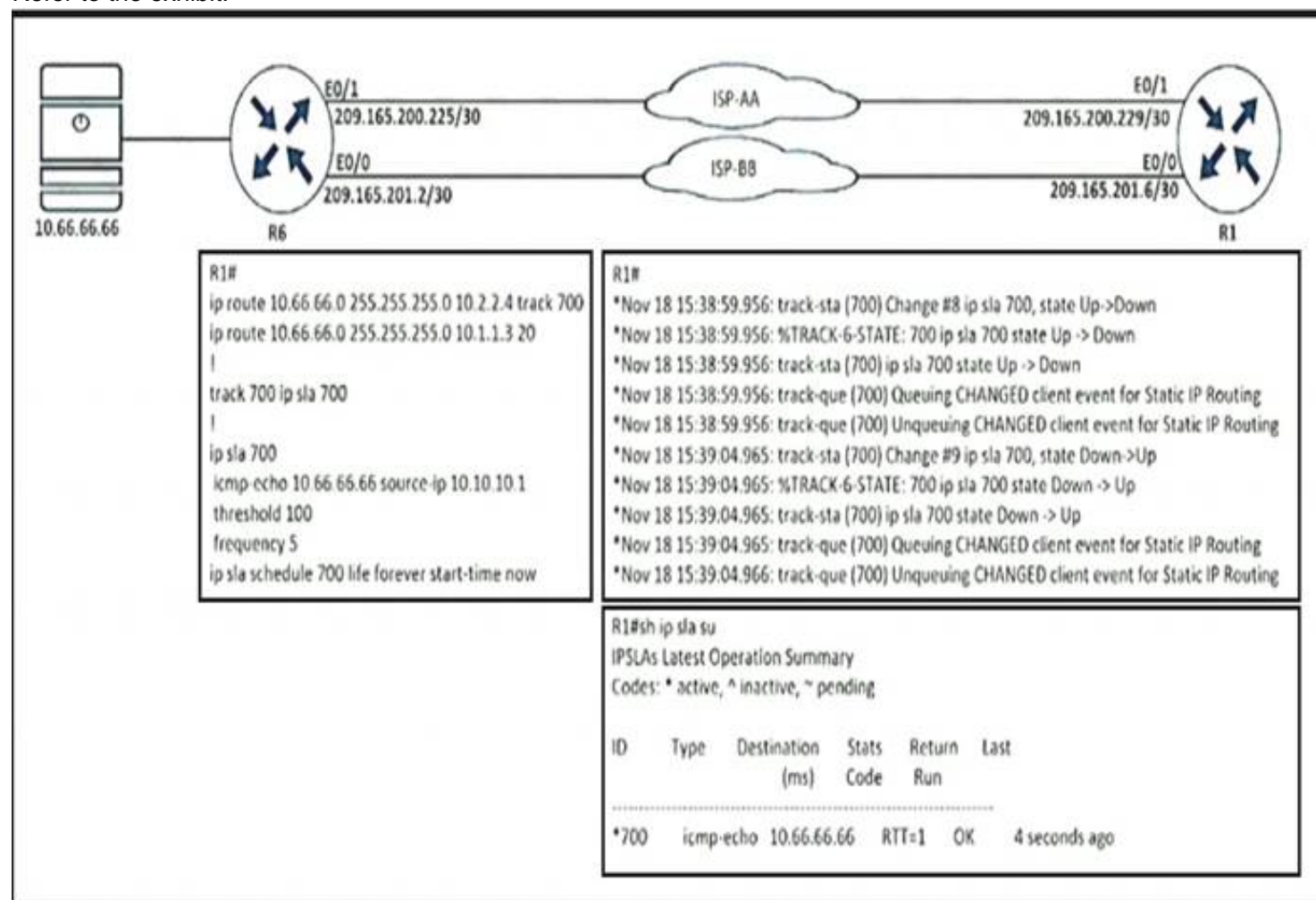
**Explanation:**

With the “aaa authentication login default group tacacs+ local ” command configured, when logging in, the password supplied will be attempted to be verified by the TACACS+ server before access is granted. If the server is unavailable/unreachable, then the switch will fall back to using the local authentication database.

**NEW QUESTION 156**

- (Exam Topic 3)

Refer to the exhibit.



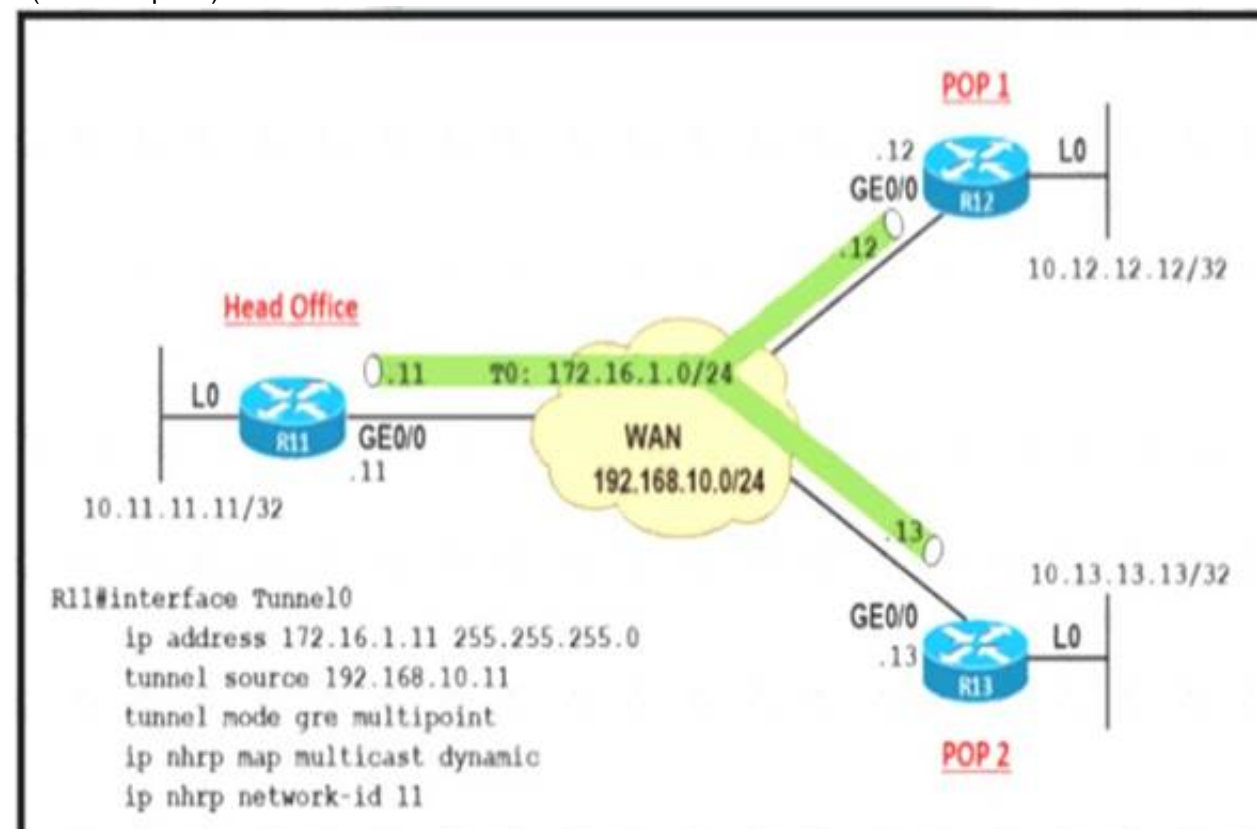
R1 is configured with IP SLA to check the availability of the server behind R6 but it kept failing. Which configuration resolves the issue?

- A. R1(config)# ip sla 700R1(config-track)# delay down 30 up 20
- B. R1(config)# ip sla 700R1(config-track)# delay down 20 up 30
- C. R1(config)# track 700 ip sla 700 R1(config-track)# delay down 30 up 20
- D. R1(config)# track 700 ip sla 700 R1(config-track)# delay down 20 up 30

**Answer: C**

**NEW QUESTION 158**

- (Exam Topic 3)





Refer to the exhibit A company builds WAN infrastructure between the head office and POPs using DMVPN hub-and-spoke topology to provide end-to-end communication All POPs must maintain point-to-point connectivity with the head office Which configuration meets the requirement at routers R12 and R13?

☐ R12#  
interface Tunnel0  
ip nhrp map multicast 192.168.10.11  
ip nhrp map 172.16.1.11 192.168.10.11  
ip nhrp network-id 12  
ip nhrp nhs 172.16.1.11

R13#  
interface Tunnel0  
ip nhrp map multicast 192.168.10.11  
ip nhrp map 172.16.1.11 192.168.10.11  
ip nhrp network-id 13  
ip nhrp nhs 172.16.1.11

☐ R12#  
interface Tunnel0  
ip nhrp map multicast 172.16.1.11  
ip nhrp map 172.16.1.11 192.168.10.11  
ip nhrp network-id 12  
ip nhrp nhs 192.168.10.11

R13#  
interface Tunnel0  
ip nhrp map multicast 172.16.1.11  
ip nhrp map 172.16.1.11 192.168.10.11  
ip nhrp network-id 13  
ip nhrp nhs 192.168.10.11

☐ Configure routers R12 and R13 as:

interface Tunnel0  
ip nhrp map multicast 172.16.1.11  
ip nhrp map 172.16.1.11 192.168.10.11  
ip nhrp network-id 11  
ip nhrp nhs 192.168.10.11

☐ Configure routers R12 and R13 as:

interface Tunnel0  
ip nhrp map multicast 192.168.10.11  
ip nhrp map 172.16.1.11 192.168.10.11  
ip nhrp network-id 11  
ip nhrp nhs 172.16.1.11

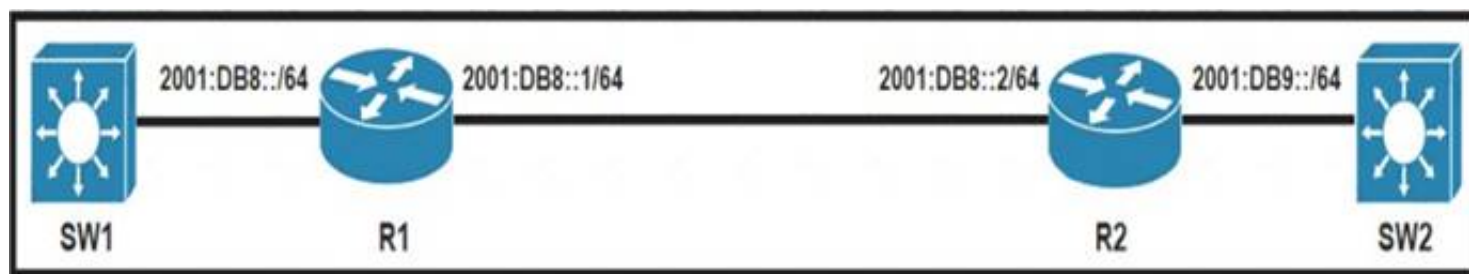
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

#### NEW QUESTION 159

- (Exam Topic 3)

Refer to the exhibit.



An engineer must advertise routes into IPv6 MP-BGP and failed. Which configuration resolves the issue on R1?

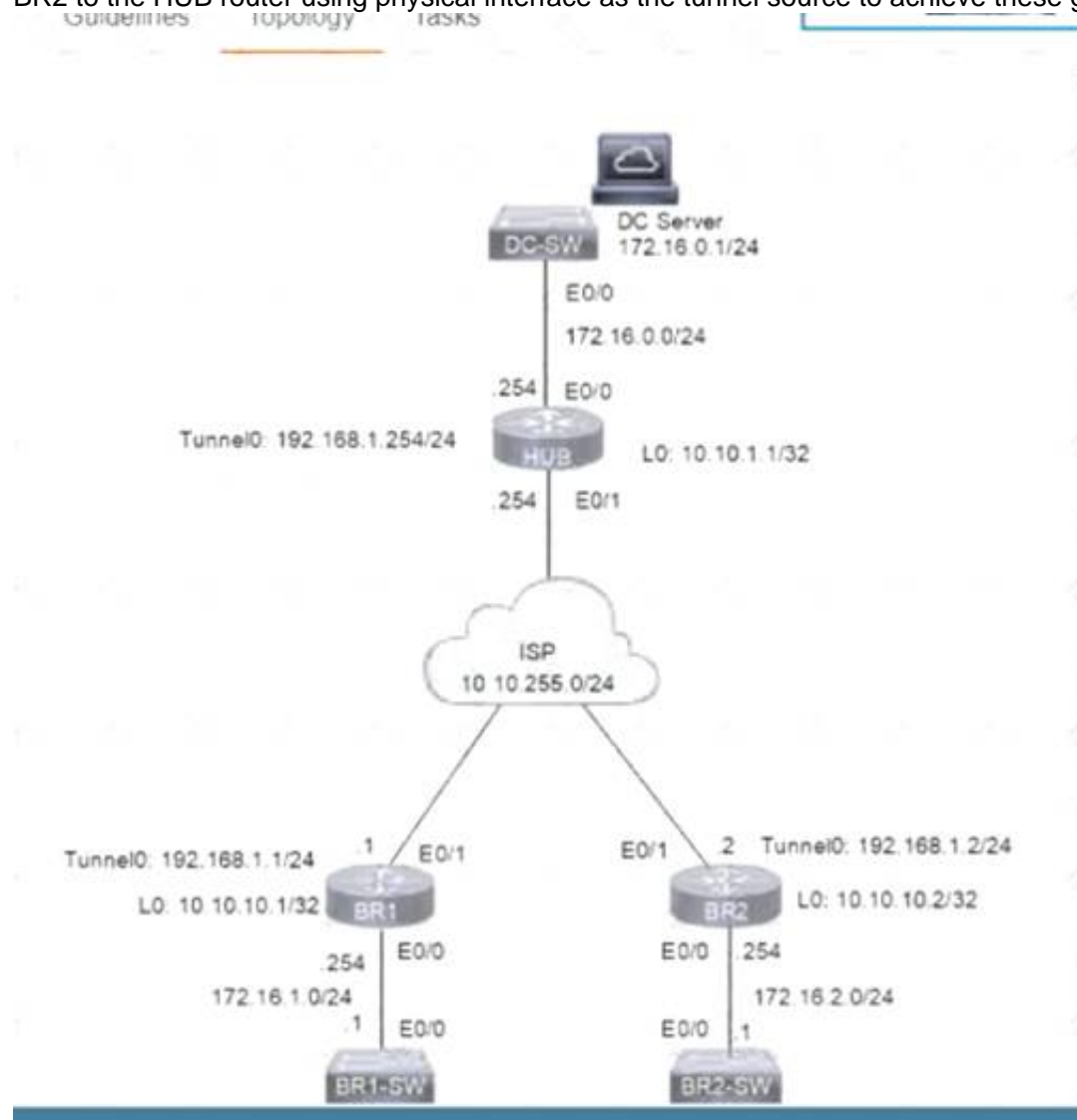
- A. router bgp 65000no bgp default ipv4-unicast address-family ipv6 multicast network 2001:DB8::/64
- B. router bgp 65000no bgp default ipv4-unicast address-family ipv6 unicast network 2001:DB8::/64
- C. router bgp 64900no bgp default ipv4-unicast address-family ipv6 unicast network 2001:DB8::/64
- D. router bgp 64900no bgp default ipv4-unicast address-family ipv6 multicastneighbor 2001:DB8:7000::2 translate-update ipv6 multicast

**Answer: B**

#### NEW QUESTION 164

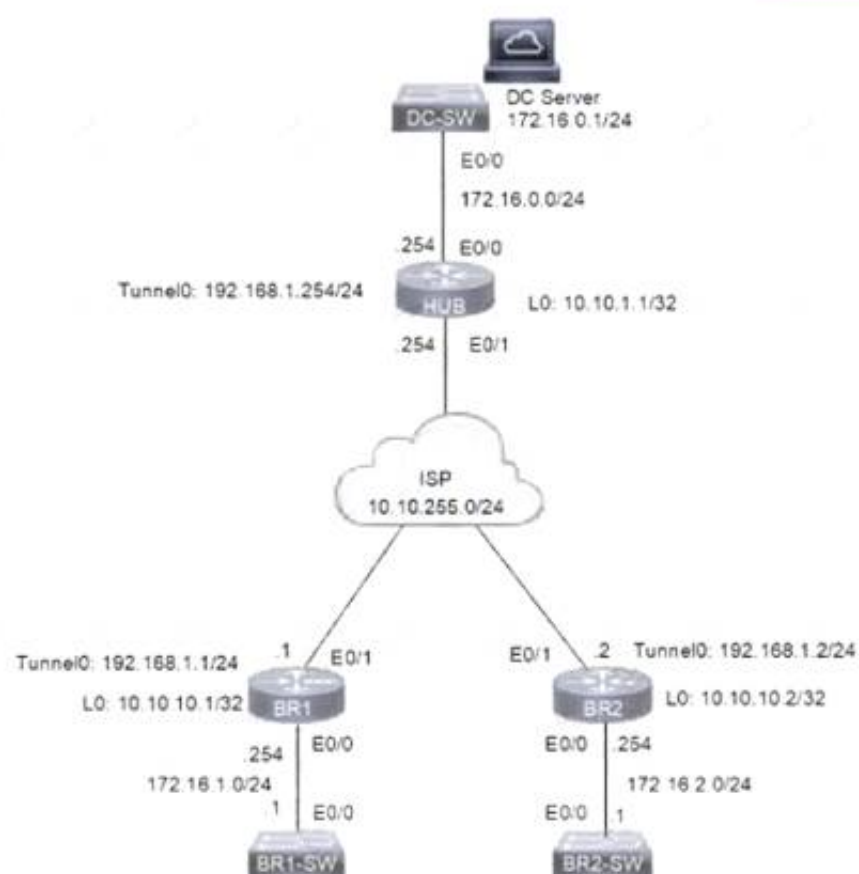
- (Exam Topic 3)

A DMVPN network is preconfigured with tunnel 0 IP address 192.168.1.254 on the HUB, IP connectivity, crypto policies, profiles, and EIGRP AS 100. The NHRP password is ccnp123, and the network ID and tunnel key is EIGRP ASN Do not introduce a static route. Configure DMVPN connectivity between routers BR1 and BR2 to the HUB router using physical interface as the tunnel source to achieve these goals:



A DMVPN network is preconfigured with tunnel 0 IP address 192.168.1.254 on the HUB, IP connectivity, crypto policies, profiles, and EIGRP AS 100. The NHRP password is **ccnp123**, and the network ID and tunnel key is **EIGRP ASN**. Do not introduce a static route. Configure DMVPN connectivity between routers BR1 and BR2 to the HUB router using physical interface as the tunnel source to achieve these goals:

1. Configure NHRP authentication, static IP-to-NBMA address maps, hold time 5 minutes, network ID, and server on branch router BR1.
2. Configure NHRP authentication, static IP-to-NBMA address maps, hold time 5 minutes, network ID, and server on branch router BR2.
3. Ensure that packet fragmentation is done before encryption to account for GRE and IPsec header and allow a maximum TCP segment size of 1360 on an IP MTU of 1400 on the tunnel interfaces of both branch routers.
4. Apply an IPsec profile to the tunnel. Verify that direct spoke-to-spoke tunnel is functional between branch routers BR1



Topology Diagram



A DMVPN network is preconfigured with tunnel 0 IP address 192.168.1.254 on the HUB, IP connectivity, crypto policies, profiles, and EIGRP AS 100. The NHRP password is **ccnp123**, and the network ID and tunnel key is **EIGRP ASN**. Do not introduce a static route. Configure DMVPN connectivity between routers BR1 and BR2 to the HUB router using physical interface as the tunnel source to achieve these goals:

1. Configure NHRP authentication, static IP-to-NBMA address maps, hold time 5 minutes, network ID, and server on branch router BR1.
2. Configure NHRP authentication, static IP-to-NBMA address maps, hold time 5 minutes, network ID, and server on branch router BR2.
3. Ensure that packet fragmentation is done before encryption to account for GRE and IPsec header and allow a maximum TCP segment size of 1360 on an IP MTU of 1400 on the tunnel interfaces of both branch routers.
4. Apply an IPsec profile to the tunnel. Verify that direct spoke-to-spoke tunnel is functional between branch routers BR1 and BR2 by using traceroute to Ethernet 0/0 IP address to get a full score.

Submit feedback about this item.

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

ON BR1

```
Current configuration : 405 bytes
!
interface Tunnel0
ip address 192.168.1.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication ccnp123
ip nhrp map 192.168.1.254 10.10.255.254
ip nhrp map multicast 10.10.255.254
ip nhrp network-id 100
ip nhrp holdtime 5
ip nhrp nhs 192.168.1.254
ip nhrp shortcut
ip tcp adjust-mss 1360
delay 1000
tunnel source 10.10.255.1
tunnel destination 10.10.255.254
tunnel key 100
end

BR1(config)#
BR1(config)#
```

ON BR2



```

DC-SW  HUB  BR1  BR1-SW  BR2  BR2-SW

UpDn Time --> Up or Down Time for a Tunnel

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
-----
1 10.10.255.254 192.168.1.254 NHRP 00:17:20 S

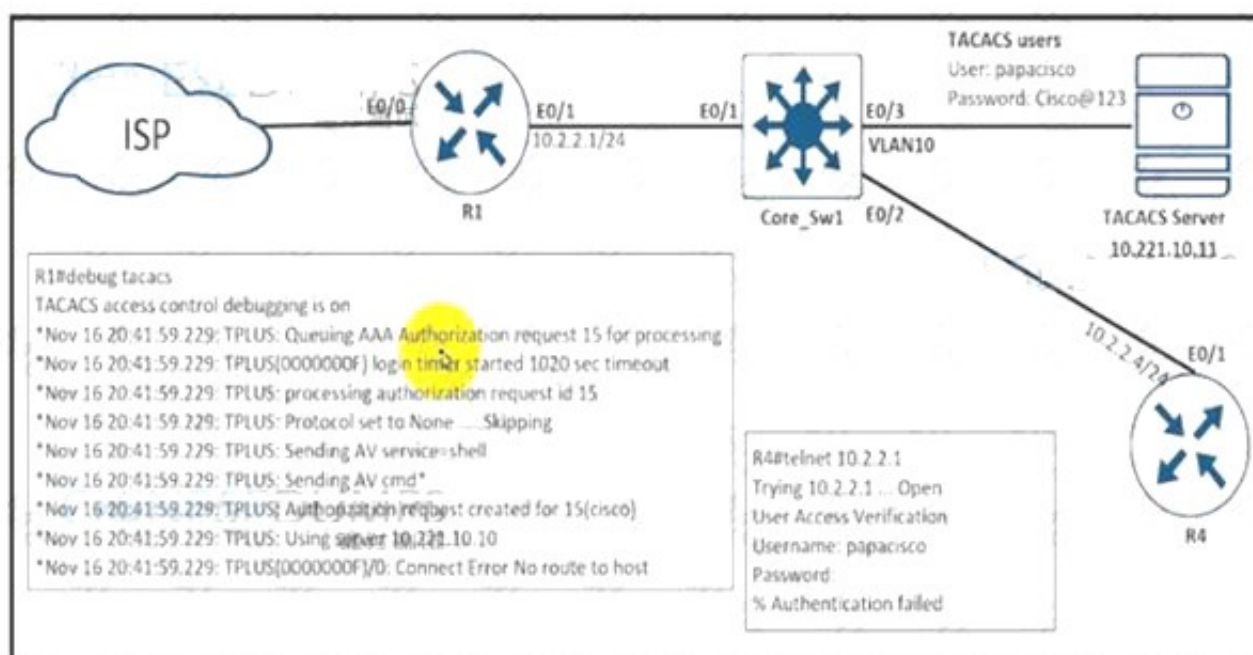
BR2(config)#do show run int tu 0
Building configuration...

Current configuration : 404 bytes
!
interface Tunnel0
 ip address 192.168.1.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication ccnpl23
 ip nhrp map 192.168.1.254 10.10.255.254
 ip nhrp map multicast 10.10.255.254
 ip nhrp network-id 100
 ip nhrp holdtime 5
 ip nhrp nhs 192.168.1.254
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source 10.10.10.2
 tunnel destination 10.10.255.254
 tunnel key 100
end
  
```

#### NEW QUESTION 169

- (Exam Topic 3)

Refer to the exhibit.



An engineer is trying to connect to R1 via Telnet with no success. Which configuration resolves the issue?

- ☐ tacacs server prod  
address ipv4 10.221.10.10  
exit
- ☒ ip route 10.221.10.10 255.255.255.255 ethernet 0/1
- ☐ tacacs server prod  
address ipv4 10.221.10.11  
exit
- ☐ ip route 10.221.0.11 255.255.255.255 ethernet 0/1

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

## NEW QUESTION 171

- (Exam Topic 3)

CPE# show snmp mib ifmib ifindex detail						
Description	ifIndex	Active	Persistent	Saved	TrapStatus	
Loopback1	8	yes	disabled	no	enabled	
GigabitEthernet1	1	yes	disabled	no	enabled	
GigabitEthernet3	3	yes	disabled	no	enabled	
GigabitEthernet3.123	10	yes	disabled	no	disabled	
VoIP-Null0	5	yes	disabled	no	enabled	
Loopback0	7	yes	disabled	no	enabled	
Null0	6	yes	disabled	no	enabled	
Loopback2	9	yes	disabled	no	enabled	
GigabitEthernet4	4	yes	disabled	no	enabled	
GigabitEthernet2	2	yes	disabled	no	enabled	

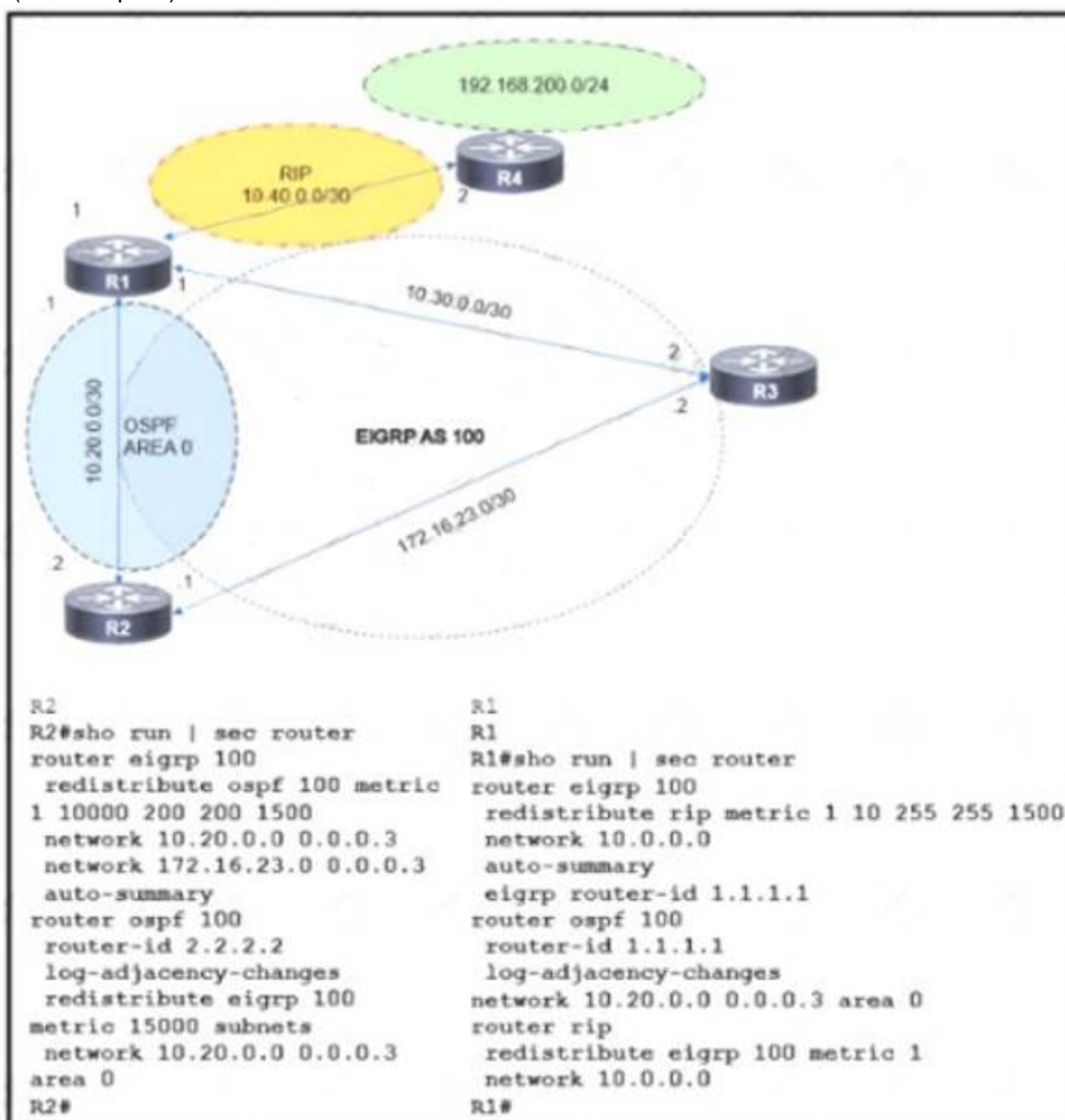
Refer to the exhibit. After reloading the router an administrator discovered that the interface utilization graphs displayed inconsistencies with their previous history in the NMS. Which action prevents this issue from occurring after another router reload in the future?

- A. Rediscover all the router interfaces through SNMP after the router is reloaded
- B. Save the router configuration to startup-config before reloading the router
- C. Configure SNMP to use static OIDs referring to individual router interfaces
- D. Configure SNMP interface index persistence on the router

**Answer: D**

## NEW QUESTION 173

- (Exam Topic 3)



Refer to the exhibit The route to 192 168 200 0 is flapping between R1 and R2 Which set of configuration changes resolves the flapping route?

- ☐ R2(config)#router ospf 100  
R2(config-router)#no redistribute eigrp 100  
R2(config-router)#redistribute eigrp 100 metric 1 subnets
- ☐ R1(config)#no router rip  
R1(config)#ip route 192.168.200.0 255.255.255.0 10.40.0.2
- ☐ R2(config)#router eigrp 100  
R2(config-router)#no redistribute ospf 100  
R2(config-router)#redistribute rip
- ☒ R1(config)#router ospf 100  
R1(config-router)#redistribute rip metric 1 metric-type 1 subnets

- A. Option A
- B. Option B

- C. Option C
- D. Option D

**Answer:** D

#### NEW QUESTION 178

- (Exam Topic 3)

The network administrator is tasked to configure R1 to authenticate telnet connections based on Cisco ISE using RADIUS. ISE has been configured with an IP address of 192.168.1.5 and with a network device pointing towards R1 (192.168.1.1) with a shared secret password of Cisco123. If ISE is down, the administrator should be able to connect using the local database with a username and password combination of admin/cisco123.

The administrator has configured the following on R1:

```
aaa new-model
!
username admin password cisco123
!
radius server ISE1
address ipv4 192.168.1.5
key Cisco123
!
aaa group server tacacs+ RAD-SERV
server name ISE1
!
aaa authentication login RAD-LOCAL group RAD-SERV
```

ISE has gone down. The Network Administrator is not able to Telnet to R1 when ISE went down. Which two configuration changes will fix the issue? (Choose two.)

- ☐ line vty 0 4  
login authentication RAD-LOCAL
- ☐ line vty 0 4  
login authentication default
- ☐ line vty 0 4  
login authentication RAD-SERV
- ☐ aaa authentication login RAD-SERV group RAD-LOCAL local
- ☐ aaa authentication login RAD-LOCAL group RAD-SERV local

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

**Answer:** CE

#### NEW QUESTION 182

- (Exam Topic 3)

A network administrator is troubleshooting a failed AAA login issue on a Cisco Catalyst c3560 switch. When the network administrator tries to log in with SSH using TACACS+ username and password credentials, the switch is no longer authenticating and is failing back to the local account. Which action resolves this issue?

- A. Configure ip tacacs source-interface GigabitEthernet 1/1
- B. Configure ip tacacs source-ip 192.168.100.55
- C. Configure ip tacacs-server source-ip 192.168.100.55
- D. Configure ip tacacs-server source-interface GigabitEthernet 1/1

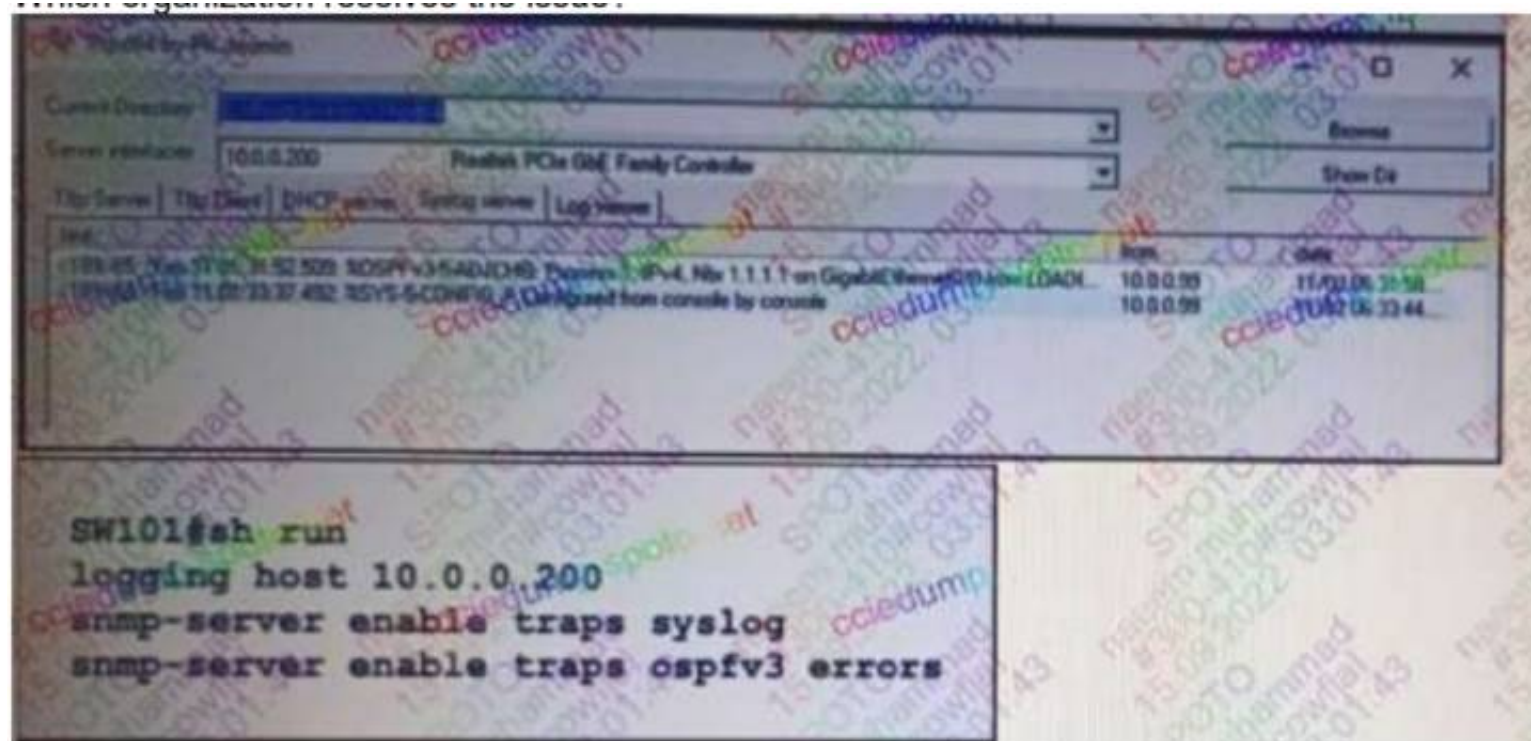
**Answer:** A

#### NEW QUESTION 183

- (Exam Topic 3)

Refer to the exhibit.





An engineer configures SW101 to send OSPFv3 interfaces state change messages to the server. However, only some OSPFv3 errors are being recorded. which organization resolves the ..?

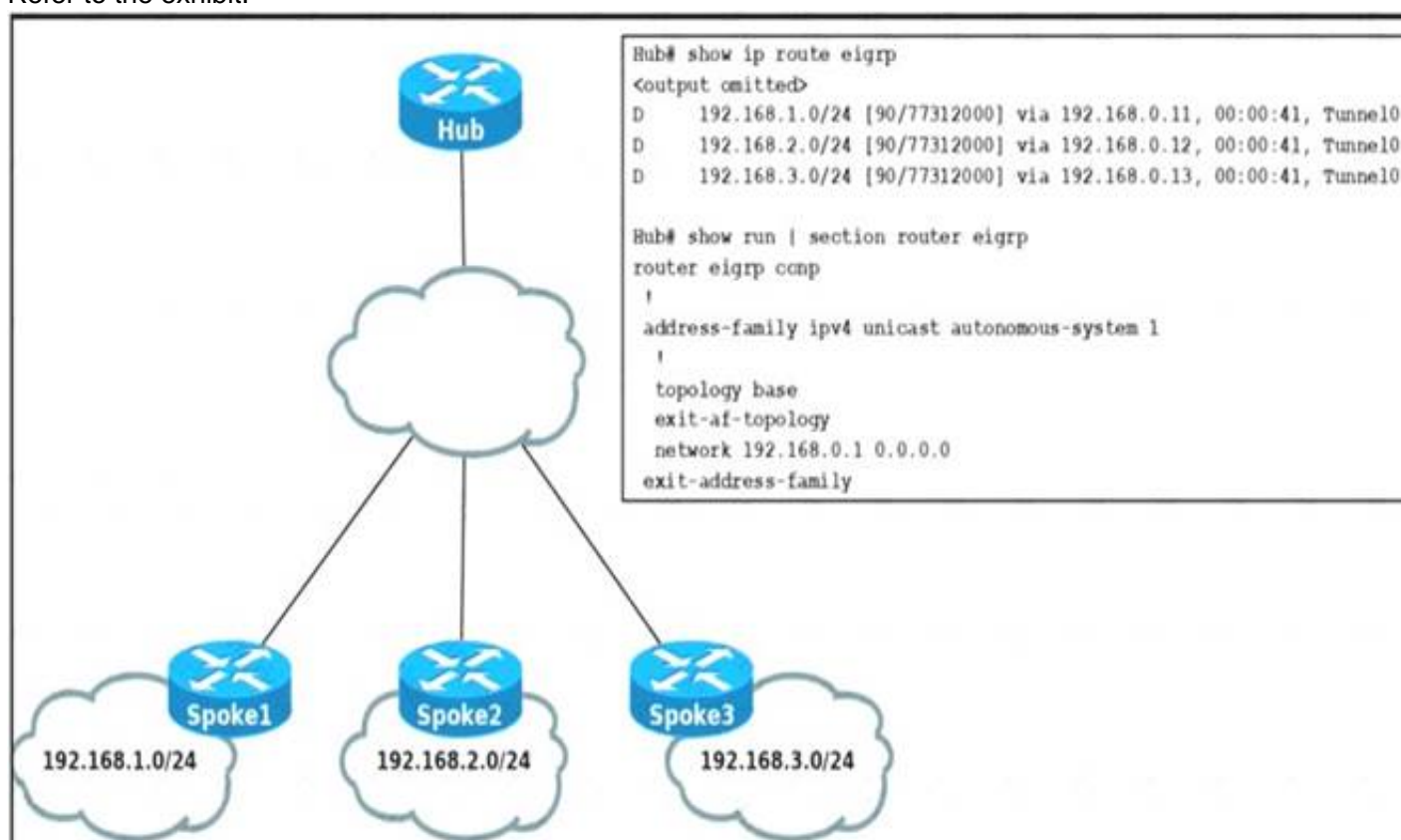
- A. snmp-server enable traps ospfv3 state-change if-state-change
- B. snmp-server enable traps ospfv3 state-change restart-status-change
- C. snmp-server enable traps ospfv3 state-change neighbor-state-change.
- D. snmp-server enable traps ospfv3 state-change if-state-change neighbor-state-change

**Answer: D**

#### NEW QUESTION 188

- (Exam Topic 3)

Refer to the exhibit.



Spoke routers do not learn about each other's routes in the DMVPN Phase2 network. Which action resolves the issue?

- A. Remove default route from spoke routers to establish a spoke-to-spoke tunnel.
- B. Configure a static route in each spoke to establish a spoke-to-spoke tunnel.
- C. Rectify incorrect wildcard mask configured on the hub router network command.
- D. Disable EIGRP split horizon on the Tunnel0 interface of the hub router.

**Answer: D**

#### NEW QUESTION 192

- (Exam Topic 3)

Refer to the exhibit.



```
ip sla 1
icmp-echo 8.8.8.8
threshold 1000
timeout 2000
frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 name ISP2 track 1
```

An administrator configures a router to stop using a particular default route if the DNS server 8.8.8.8 is not reachable through that route. However, this configuration did not work as desired and the default route still works even if the DNS server 8.8.8.8 is unreachable. Which two configuration changes resolve the issue? (Choose two.)

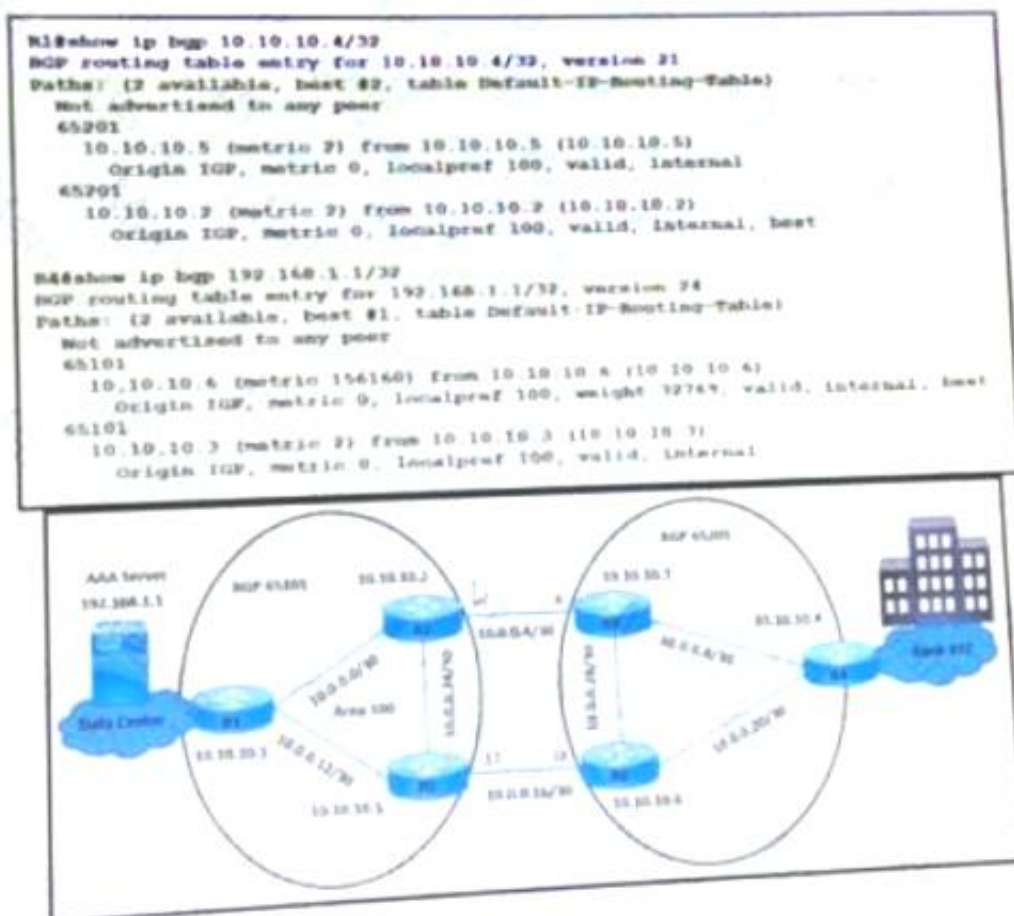
- A. Configure two static routes for the 8.8.8.8/32 destination to match the IP SLA probe for each ISP.
- B. Associate every IP SLA probe with the proper WAN address of the router.
- C. Reference the proper exit interfaces along with the next hops in both static default routes.
- D. Use a separate track object to reference the existing IP SLA 1 probe for every static route.
- E. Use a separate IP SLA probe and track object for every static route

**Answer:** AE

### NEW QUESTION 193

- (Exam Topic 3)

Refer to the exhibit.



A customer reports that user traffic of bank XYZ to the AAA server is not using the primary path via the R3-R2 link. The network team observes: No fiber is cut on links R2 and R3.

As101 and AS 201 routers established BGP peering. Which configuration resolves the issue?

A)

```
R2(config)#route-map BGP-Path permit 10
R2(config-route-map)# set metric 200
R2(config)#router bgp 65101
R2(config-router)# neighbor 10.10.10.3 route-map BGP-Path out
```

B)

```
R6(config)#router bgp 65201
R6(config-router)#no neighbor 10.10.10.5 weight 32769
```

C)

```
R4(config)#router bgp 65201
R4(config-router)#no neighbor 10.10.10.6 weight 32769
```

D)

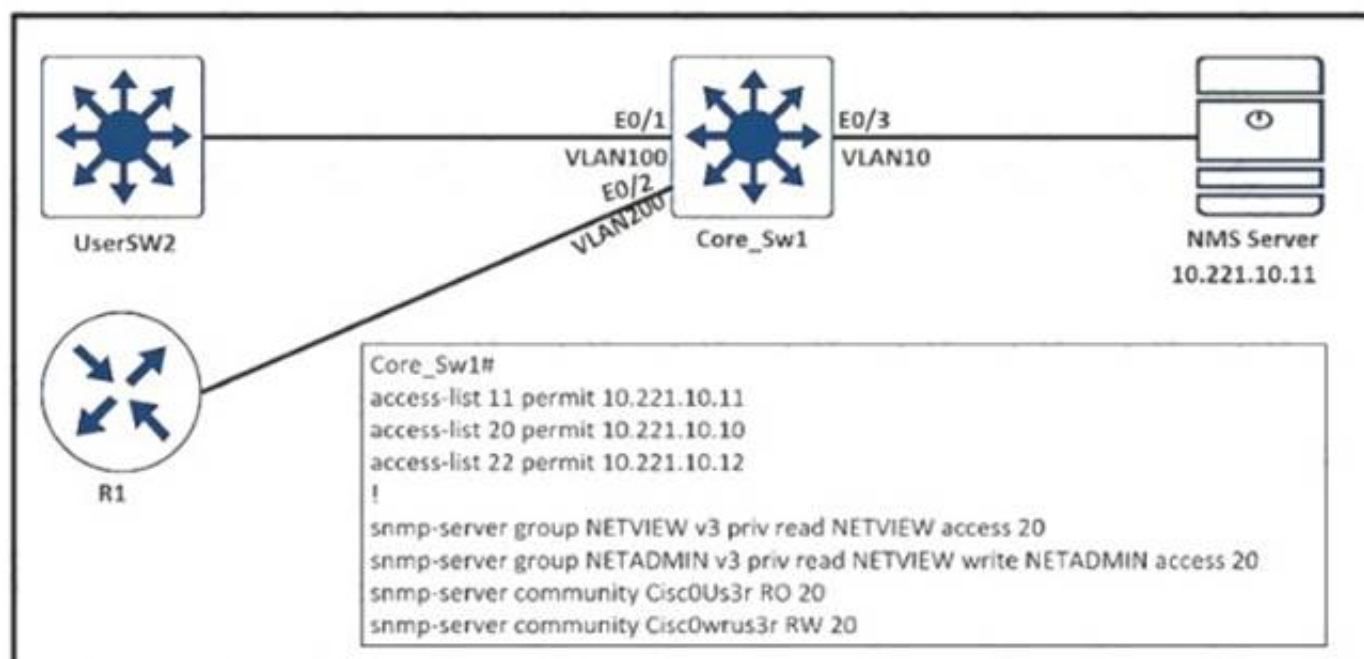
```
R1(config)#route-map BGP-Path permit 10
R1(config-route-map)# set local-preference 200
R1(config)#router bgp 65101
R1(config-router)# neighbor 10.10.10.2 route-map BGP-Path out
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

#### NEW QUESTION 194

- (Exam Topic 3)  
Refer to the exhibit.



An engineer configured SNMP communities on the Core\_SW1, but the SNMP server cannot obtain information from Core\_SW1. Which configuration resolves this issue?

- A. snmp-server group NETVIEW v2c priv read NETVIEW access 20
- B. access-list 20 permit 10.221.10.11
- C. access-list 20 permit 10.221.10.12
- D. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22

**Answer: B**

#### NEW QUESTION 196

- (Exam Topic 3)  
What are the two reasons for RD and VPNv4 addresses in an MPLS Layer 3 VPN? (Choose two.)

- A. RD is prepended to each prefix to make routes unique.
- B. VPN RT communities are used to identify customer unique routes.
- C. When the PE redistributes customer routes into MP-BGP, they must be unique.
- D. They are on a CE device to use for static configuration.

E. They are used for a BGP session with the CE device.

**Answer:** AC

#### NEW QUESTION 201

- (Exam Topic 3)

Refer to the exhibit.

```
Dallas_Router:

interface GigabitEthernet0/0/0.364
description Guest_Wifi_10.66.46.0/23
encapsulation dot1Q 364
ip address 10.66.46.1 255.255.254.0
ip helper-address 10.192.104.212
ip helper-address 10.191.103.140
ip access-group GUEST-ACCESS in
ip access-group GUEST-ACCESS-OUT out
no ip redirects
no ip unreachable
no ip proxy-arp

ip access-list extended GUEST-ACCESS
remark Internet Access Only
permit udp any any eq bootpc
permit udp any any eq bootps
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip any 224.0.0.0 31.255.255.255
deny ip any 169.254.0.0 0.0.255.255
deny ip any 127.0.0.0 0.255.255.255
deny ip any 192.0.2.0 0.0.0.255
deny ip any host 0.0.0.0
permit ip 10.66.42.0 0.0.0.255 any
permit ip 10.66.46.0 0.0.0.255 any

ip access-list extended GUEST-ACCESS-OUT
remark Used to block inbound traffic to Guest Networks
permit udp any any eq bootps
permit udp any any eq bootpc
permit udp any any eq domain
permit udp any any
permit icmp any any
permit tcp host 10.192.103.124 eq 15871 any
permit tcp any any established
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip any 224.0.0.0 31.255.255.255
deny ip any 169.254.0.0 0.0.255.255
deny ip any 127.0.0.0 0.255.255.255
deny ip any 192.0.2.0 0.0.0.255
deny ip any host 0.0.0.0
```

After a new regional office is set up, not all guests can access the internet via guest WiFi. Clients are getting the correct IP address from guest Wi-Fi VLAN 364. which action resolves the issue ?

- A. Allow 10.66.46.0/23 in the outbound ACL
- B. Allow DNS traffic through the outbound ACL
- C. Allow DNS traffic through the inbound ACL
- D. Allow 10.66.46.0/23 in the inbound ACL

**Answer:** C

#### NEW QUESTION 206

- (Exam Topic 3)

Refer to the exhibit.

```
R2# show ip ospf neighbor
R2#
R2# debug ip ospf hello

*Feb 22 23:46:58.699: OSPF-1 HELLO Et1/1: Rcv hello from
10.255.255.1 area 0 10.0.23.1
*Feb 22 23:46:58.703: OSPF-1 HELLO Et1/1: Mismatched hello
parameters from 10.0.23.1
*Feb 22 23:46:58.703: OSPF-1 HELLO Et1/1: Dead R 30 C 20, Hello
R 10 C 10 Mask R 255.255.255.0 C 255.255.255.0
```

The connected routers do not show up as OSPF neighbors. Which action resolves the issue?

- A. Change the R1 dead timer to 20.
- B. Change the R2 dead timer to 20.



- C. Change the R2 hello timer to 20.
- D. Change the R1 hello timer to 20.

**Answer:** A

#### NEW QUESTION 209

- (Exam Topic 3)

An engineer is implementing a coordinated change with a server team. As part of the change, the engineer must configure interface GigabitEthernet2 in an existing VRF "RED" then move the interface to an existing VRF "BLUE" when the server team is ready. The engineer configured interface GigabitEthernet2 in VRF "RED"

```
interface GigabitEthernet2
description Migration ID: B410A60D0806G06
vrf forwarding RED
ip address 10.0.0.0 255.255.255.254
negotiation auto
```

Which configuration completes the change?

- A. interface GigabitEthernet2 no ip addressvrf forwarding BLUE
- B. interface GigabitEthernet2 no vrf forwarding RED vrf forwarding BLUEip address 10.0.0.0 255.255.255.254
- C. interface GigabitEthernet2 no vrf forwarding RED vrf forwarding BLUE
- D. interface GigabitEthernet2 no ip addressip address 10.0.0.0 255.255.255.254vrf forwarding BLUE

**Answer:** B

#### Explanation:

When assigning an interface to a VRF, the IP address will be removed so we have to reassign the IP address to that interface.

#### NEW QUESTION 212

- (Exam Topic 3)

What action is performed for untagged outgoing labels in an MPLS router?

- A. Convert the incoming MPLS packet to an untagged packet and then do a FIB lookup
- B. Convert the incoming MPLS packet to an untagged packet and then do a RIB lookup.
- C. Convert the untagged packet to a labeled packet and forward it to the next router
- D. Convert the incoming MPLS packet to an IP packet and forward it to the next router.

**Answer:** C

#### NEW QUESTION 214

- (Exam Topic 3)

A network administrator opens a telnet connection to the router and gets the message:

R1#telnet 10.1.1.2

Trying 10.1.1.2 Open

(Connection to 10.1.1.2 closed by foreign host)

Router R2 is configured with enable secret and password commands. Which action resolves the issue?

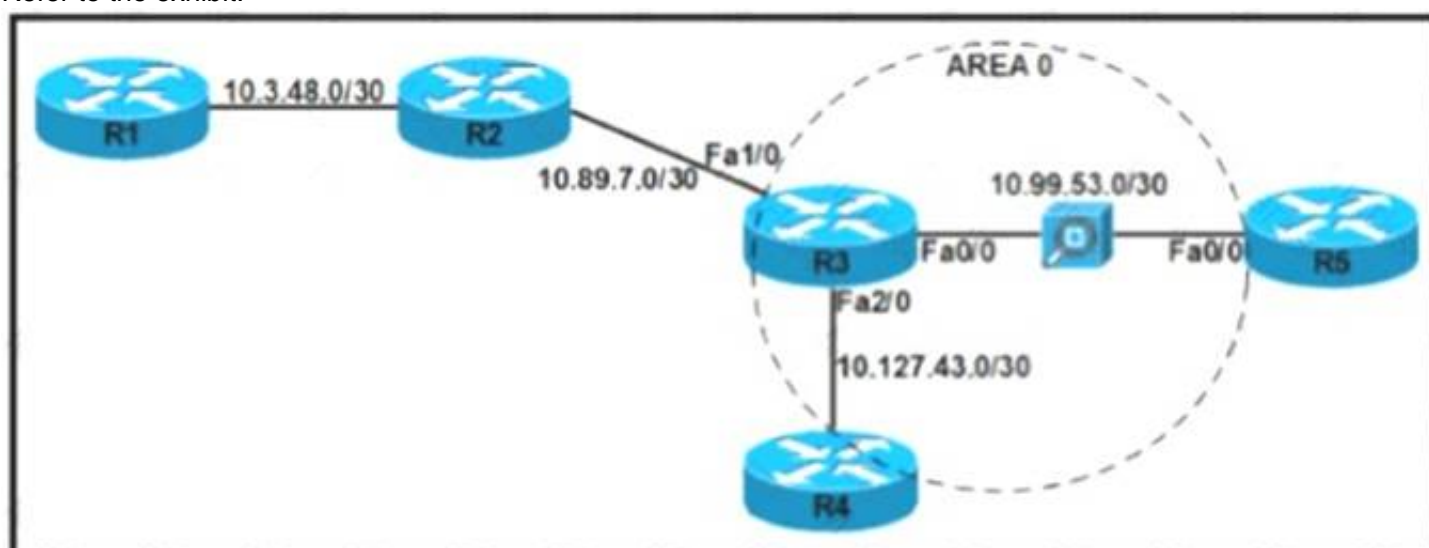
- A. Configure the logging synchronous command on line vty.
- B. Configure the exec command on line vty.
- C. Configure the login local command on line vty
- D. Configure the enable password command on line vty.

**Answer:** C

#### NEW QUESTION 216

- (Exam Topic 3)

Refer to the exhibit.



The security department recently installed a monitoring device between routers R3 and R5, which a loss of network connectivity for users connected to R5. Troubleshooting revealed that the monitoring device cannot forward multicast packets. The team already updated R5 with the correct configuration. Which configuration must be implemented on R3 to resolve the problem by ensuring R3 as the DR for the R3-R5 segment?

A)



```

interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network point-to-point
ip ospf priority 100
!
router ospf 10
router-id 10.10.3.255
network 10.99.53.0 0.0.0.3 area 0
neighbor 10.99.53.2
!
access-list 122 permit 89 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 89 any any

```

B)

```

interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network non-broadcast
ip ospf priority 0
!
router ospf 10
router-id 10.10.3.255
network 10.99.53.0 0.0.0.3 area 0
neighbor 10.99.53.2
!
access-list 122 permit 89 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 89 any any
access-list 122 permit tcp any any
access-list 122 permit udp any any
access-list 122 permit icmp any any

```

C)

```

interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network non-broadcast
ip ospf priority 100
!
router ospf 10
router-id 10.10.3.255
network 10.99.53.0 0.0.0.3 area 0
neighbor 10.99.53.2
!
access-list 122 permit 89 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 89 any any
access-list 122 permit tcp any any
access-list 122 permit udp any any
access-list 122 permit icmp any any

```

D)

```
interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network point-to-point
ip ospf priority 100
!

router ospf 10
router-id 10.10.3.255
network 10.99.53.0 0.0.0.3 area 0
neighbor 10.99.53.2
!

access-list 122 permit 88 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 88 any any
!
```

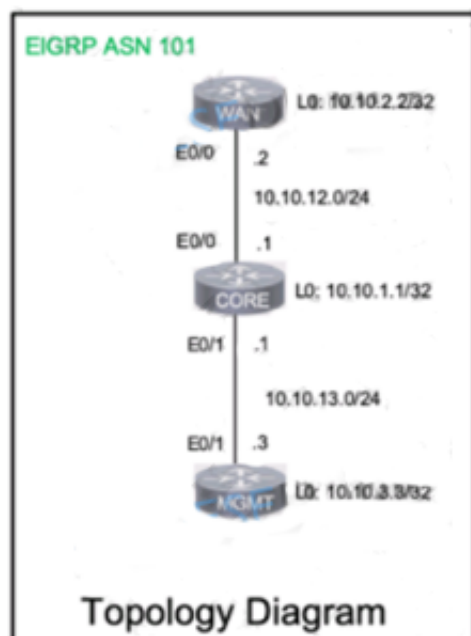
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** C

#### NEW QUESTION 217

- (Exam Topic 3)

A network is configured with CoPP to protect the CORE router route processor for stability and DDoS protection. As a company policy, a class named class-default is preconfigured and must not be modified or deleted. Troubleshoot CoPP to resolve the issues introduced during the maintenance window to ensure that:



Guidelines Topology **Tasks**

A network is configured with CoPP to protect the CORE router route processor for stability and DDoS protection. As a company policy, a class named class-default is preconfigured and must not be modified or deleted. Troubleshoot CoPP to resolve the issues introduced during the maintenance window to ensure that:

1. Dynamic routing policies are under CoPP-CRITICAL and are allowed only from the 10.10.x.x range.
2. Telnet, SSH, and ping are under CoPP-IMPORTANT and are allowed strictly to/from 10.10.x.x to the CORE router (Hint: you can verify using Loopback1).
3. All devices ping (UDP) any CORE router interface successfully to/from the 10.10.x.x range and do not allow any other IP address. NORMAL (Hint: Traceroute port range 33434 33464).

WAN

```
!
!
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
 ip address 172.16.2.2 255.255.255.0
!
```

WAN CORE MGMT

```
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
 ip address 172.16.2.2 255.255.255.0
!
interface Ethernet0/0
 ip address 10.10.12.2 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 network 172.16.2.0 0.0.0.255
 eigrp router-id 10.10.2.2
```

```
!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 network 172.16.2.0 0.0.0.255
 eigrp router-id 10.10.2.2
!
```

## CORE

```
!
class-map match-all CoPP-CRITICAL
 match access-group 120
class-map match-all CoPP-NORMAL
 match access-group 122
class-map match-all CoPP-IMPORTANT
 match access-group 121
!
policy-map CoPP
 class CoPP-CRITICAL
  police 1000000 50000 50000 conform-action transmit exceed-
-action drop
 class CoPP-IMPORTANT
  police 100000 20000 20000 conform-action transmit exceed-
action drop
 class CoPP-NORMAL
  police 64000 6400 64000 conform-action transmit exceed-ac
tion drop
 class class-default
  police 8000 1500 1500 conform-action drop exceed-action d
rop
!
```

```
!
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.10.12.1 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 10.10.13.1 255.255.255.0
 duplex auto
!
```



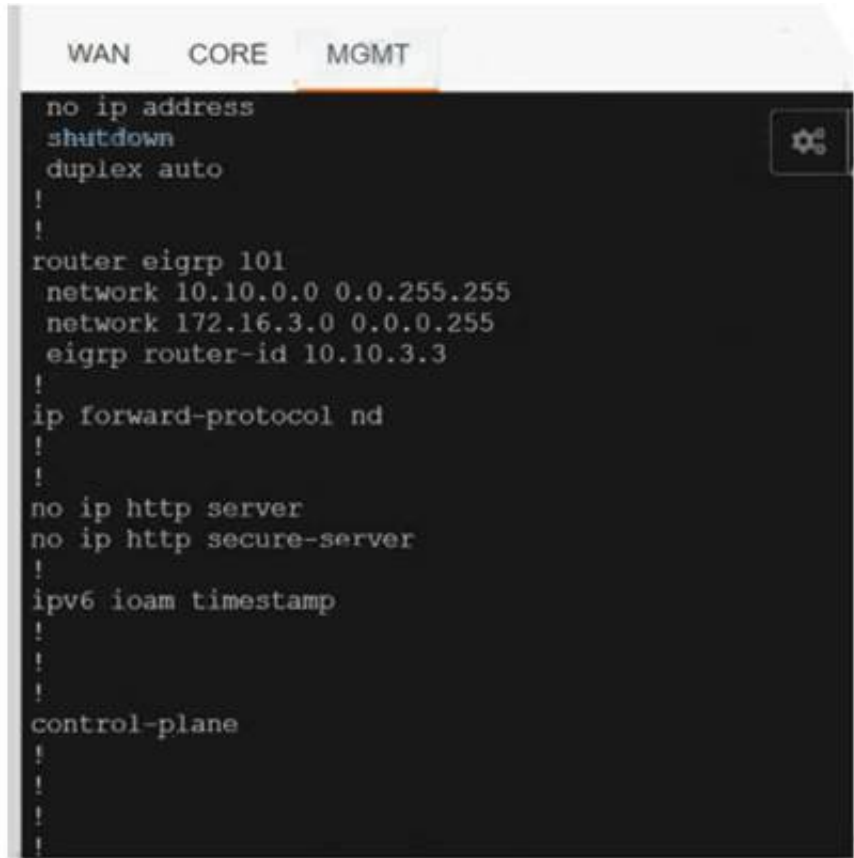
```
!
interface Ethernet0/1
 ip address 10.10.13.1 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 eigrp router-id 10.10.1.1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
```

```
!
!
access-list 120 remark *** ACL for CoPP-Critical ***
access-list 121 remark *** ACL for CoPP-IMPORTANT
access-list 122 remark *** ACL for CoPP-NORMAL
!
control-plane
 service-policy input CoPP
!
!
```

MGMT

WAN CORE **MGMT**

```
interface Loopback0
 ip address 10.10.3.3 255.255.255.255
!
interface Loopback1
 ip address 172.16.3.3 255.255.255.0
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/1
 ip address 10.10.13.3 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 network 172.16.3.0 0.0.0.255
 eigrp router-id 10.10.3.3
```

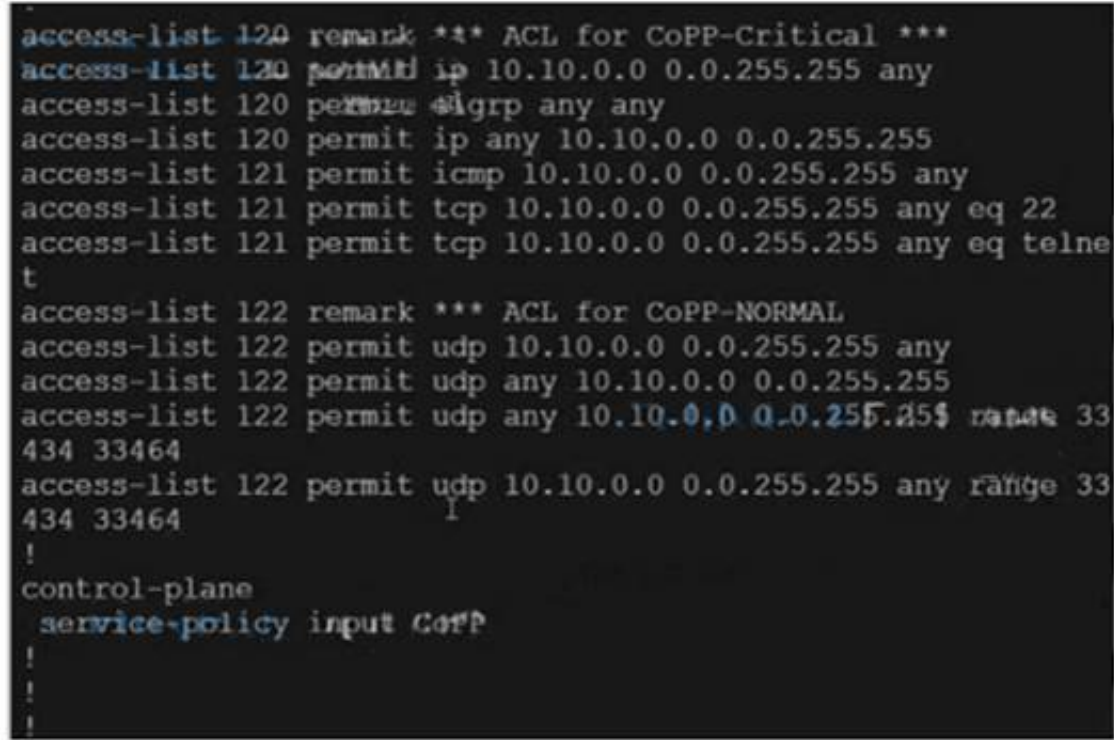


- A. Mastered
- B. Not Mastered

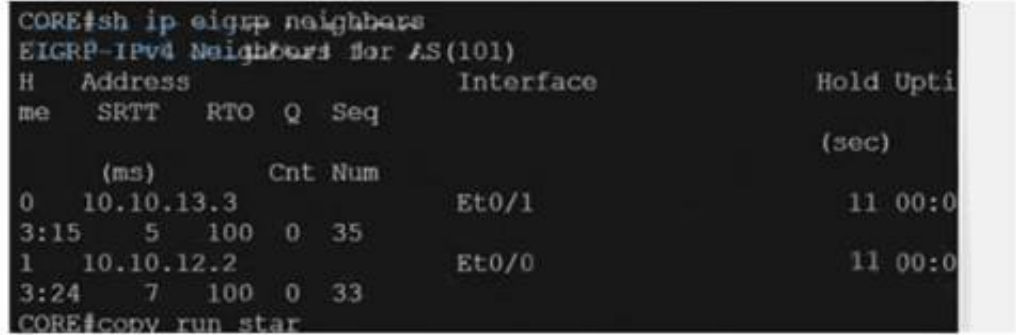
Answer: A

Explanation:

CORE  
 policy-mao CoPP  
 class CoPP-CRITICAL  
 police 1000000 50000 50000 conform-action transmit exceed-action transmit  
 Text Description automatically generated with medium confidence



CORE# Copy run start TESTING: CORE  
 Graphical user interface Description automatically generated with medium confidence



MGMT  
 Graphical user interface, text Description automatically generated

```

MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ...
% Connection refused by remote host

MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ... Open

Password required, but none set
[Connection to 10.10.13.1 closed by foreign host]
MGMT#
    
```

#### NEW QUESTION 222

- (Exam Topic 3)

An engineer creates a default static route on a router with a hop of 10.1.1.1. On inspection, the engineer finds the router has two VRFs, Red and Blue. The next hop is valid for both VRFs and exists in each assigned VRF. Which configuration achieves connectivity?

A)

```

ip route vrf BLUE 0.0.0.0 255.255.255.255 10.1.1.1
ip route vrf RED 0.0.0.0 255.255.255.255 10.1.1.1
    
```

B)

```

ip route vrf Red 0.0.0.0 0.0.0.0 10.1.1.1
ip route vrf Blue 0.0.0.0 0.0.0.0 10.1.1.1
    
```

C)

```

ip route 0.0.0.0 0.0.0.0 10.1.1.1
    
```

D)

```

ip route vrf Red 0.0.0.0 255.255.255.255 10.1.1.1
ip route vrf Blue 0.0.0.0 255.255.255.255 10.1.1.1
    
```

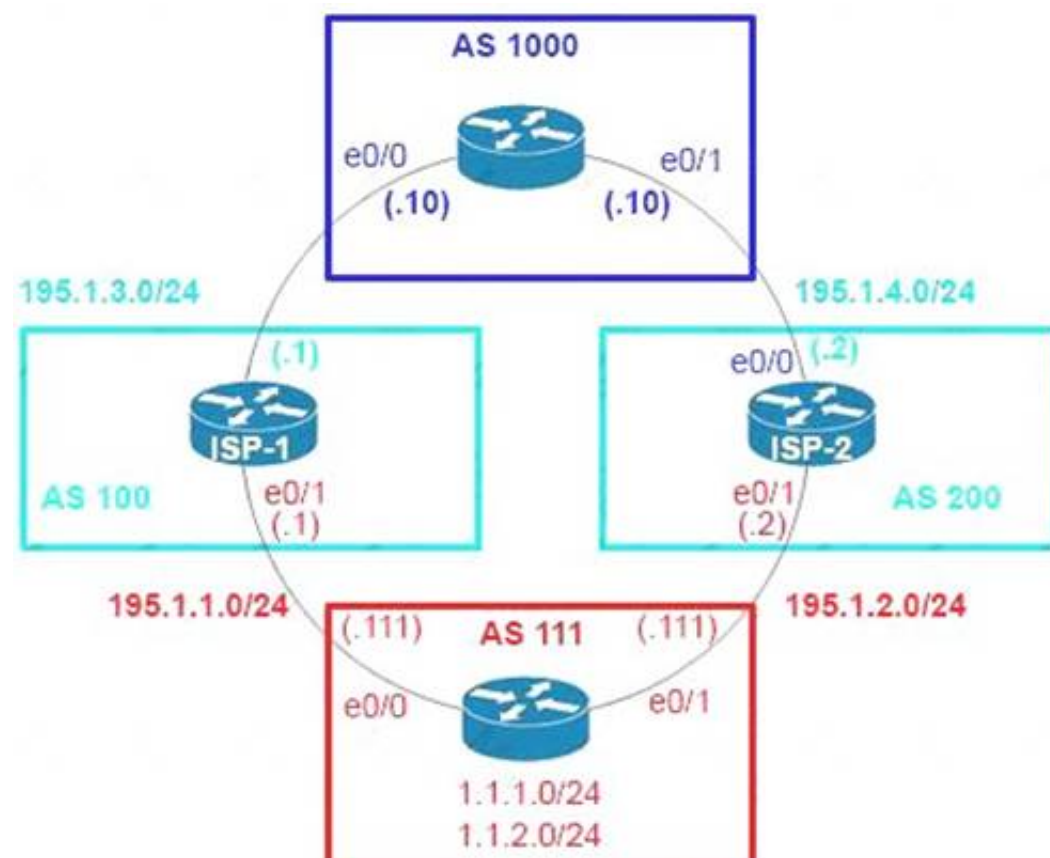
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

#### NEW QUESTION 223

- (Exam Topic 3)

Refer to the exhibit.





## AS111

```
Router bgp 111
Neighbor 195.1.1.1 remote-as 100
Neighbor 195.1.1.1 allowas-in
Neighbor 195.1.2.2 remote-as 200
Neighbor 195.1.2.2 allowas-in
```

AS111 is receiving its own routes from AS200 causing a loop in the network. Which configuration provides loop prevention?

- A)  
`router bgp 111`  
`neighbor 195.1.1.1 as-override`  
`neighbor 195.1.2.2 as-override`
- B)  
`router bgp 111`  
`neighbor 195.1.1.1 as-override`  
`no neighbor 195.1.2.2 allowas-in`
- C)  
`router bgp 111`  
`no neighbor 195.1.1.1 allowas-in`  
`no neighbor 195.1.2.2 allowas-in`
- D)  
`router bgp 111`  
`neighbor 195.1.2.2 as-override`  
`no neighbor 195.1.1.1 allowas-in`

- A. Option A  
 B. Option B  
 C. Option C  
 D. Option D

**Answer: C**

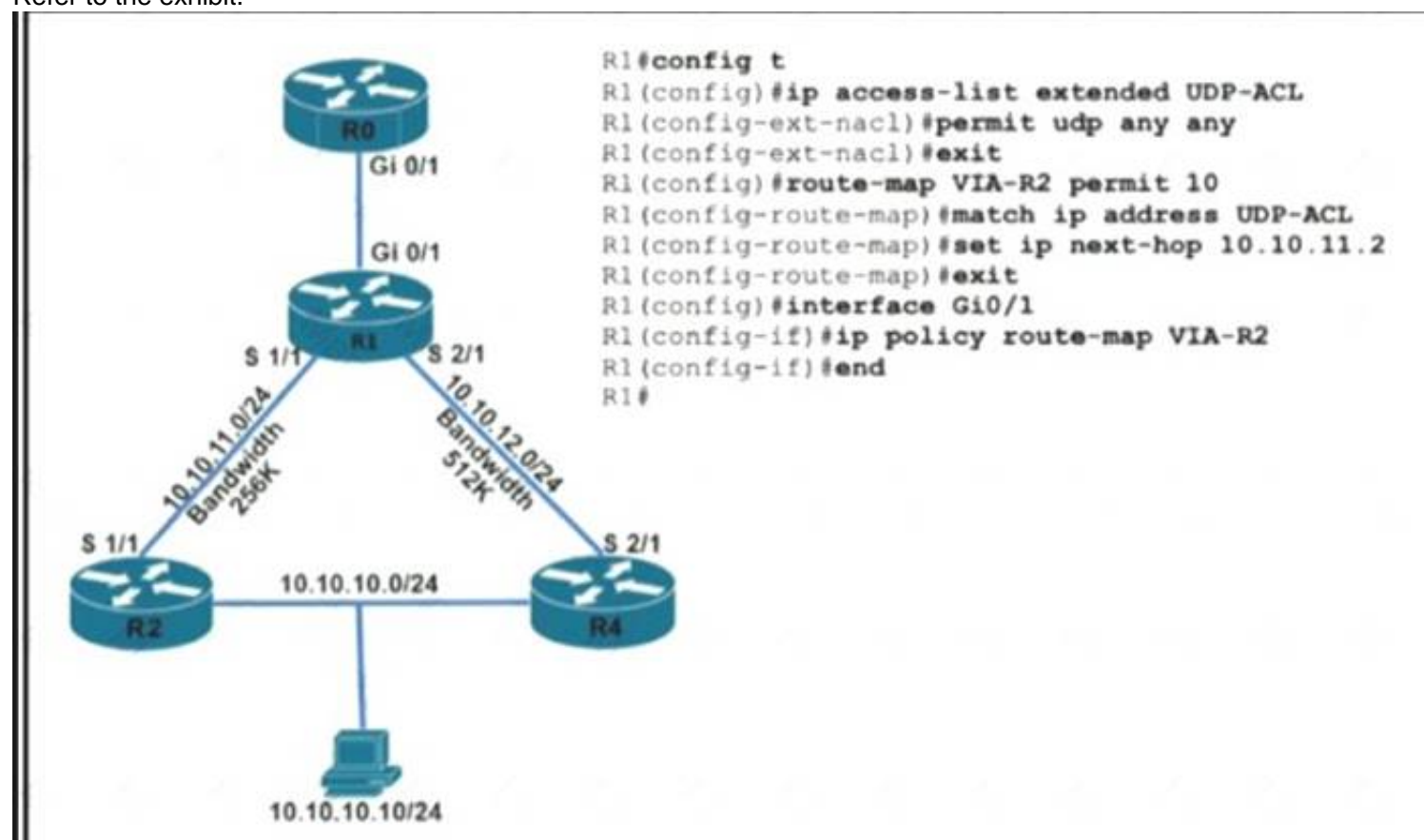
### Explanation:

A router discards BGP network prefixes if it sees its ASN in AS-Path as a loop prevention mechanism. The "allowas-in" feature allows routes to be received and processed even if router detects its own ASN in AS-Path.

## NEW QUESTION 228

- (Exam Topic 3)

Refer to the exhibit.



TCP traffic should be reaching host 10.10.10.10/24 via R2. Which action resolves the issue?

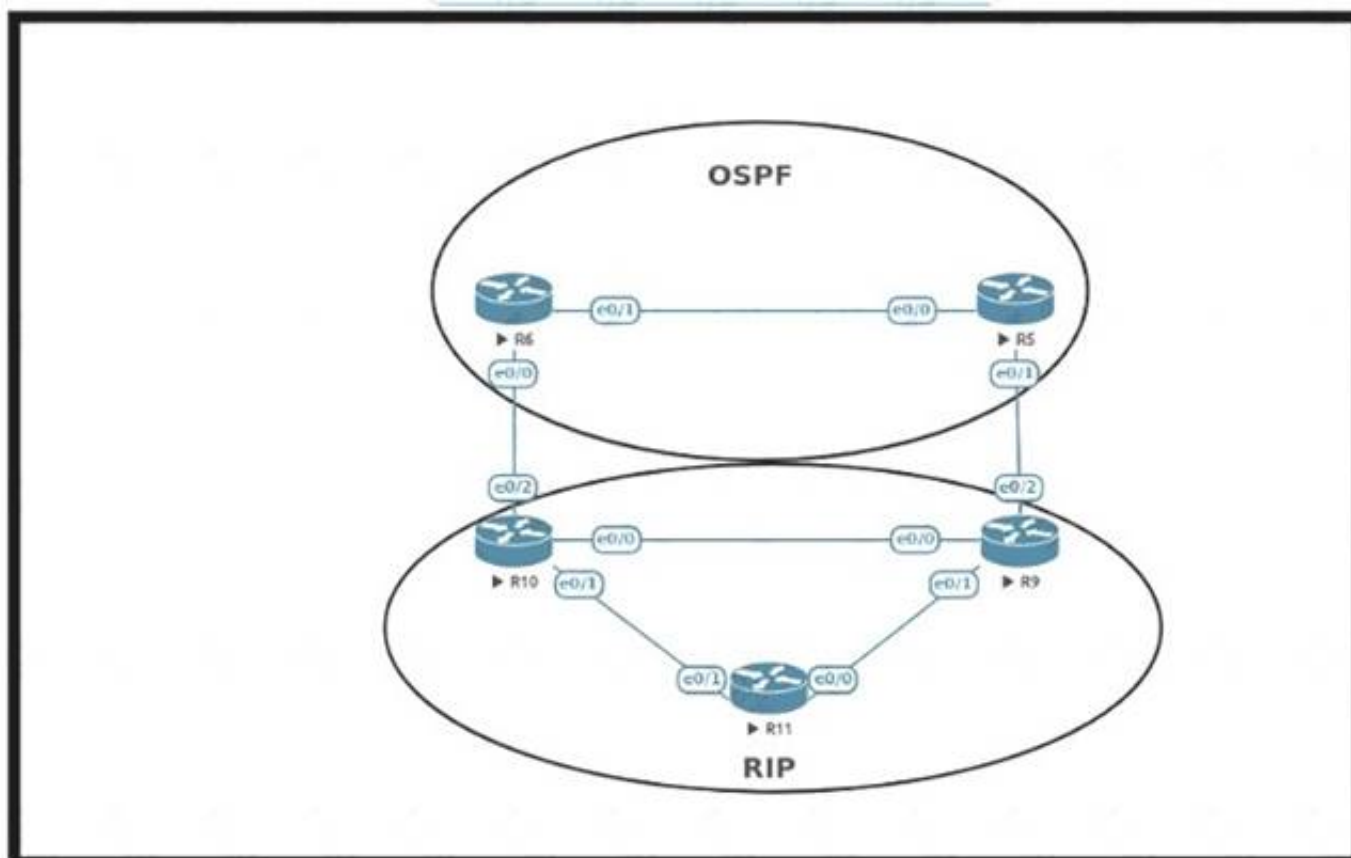
- A. TCP traffic will reach the destination via R2 without any changes  
 B. Add a permit 20 statement in the route map to allow TCP traffic  
 C. Allow TCP in the access list with no changes to the route map  
 D. Set IP next-hop to 10.10.12.2 under the route-map permit 10 to allow TCP traffic.

**Answer: C**

**NEW QUESTION 229**

- (Exam Topic 3)

Refer to the exhibit.



An engineer must configure OSPF with R9 and R10 and configure redistribution between OSPF and RIP causing a routing loop Which configuration on R9 and R10 meets this objective?

A)

```
router ospf 1
 redistribute rip subnets tag 20
!
route-map deny_tag20 deny 10
 match tag 20
route-map deny_tag20 permit 20
!
router ospf 1
 distribute-list route-map deny_tag20 in
```

B)

```
router ospf 1
 redistribute rip subnets tag 20
!
route-map deny_tag20 permit 10
 match tag 20
route-map deny_tag20 permit 20
!
router ospf 1
 distribute-list route-map deny_tag20 in
```

C)

```
router ospf 1
 redistribute rip subnets tag 20
!
route-map deny_tag20 deny 10
 match tag 20
route-map deny_tag20 deny 20
!
router ospf 1
 distribute-list route-map deny_tag20 in
```

D)

```
router ospf 1
 redistribute rip subnets tag 20
!
route-map deny_tag20 deny 10
 match tag 20
route-map deny_tag20 permit 20
!
router rip 1
 distribute-list route-map deny_tag20 in
```

A. Option A

B. Option B

C. Option C

D. Option D

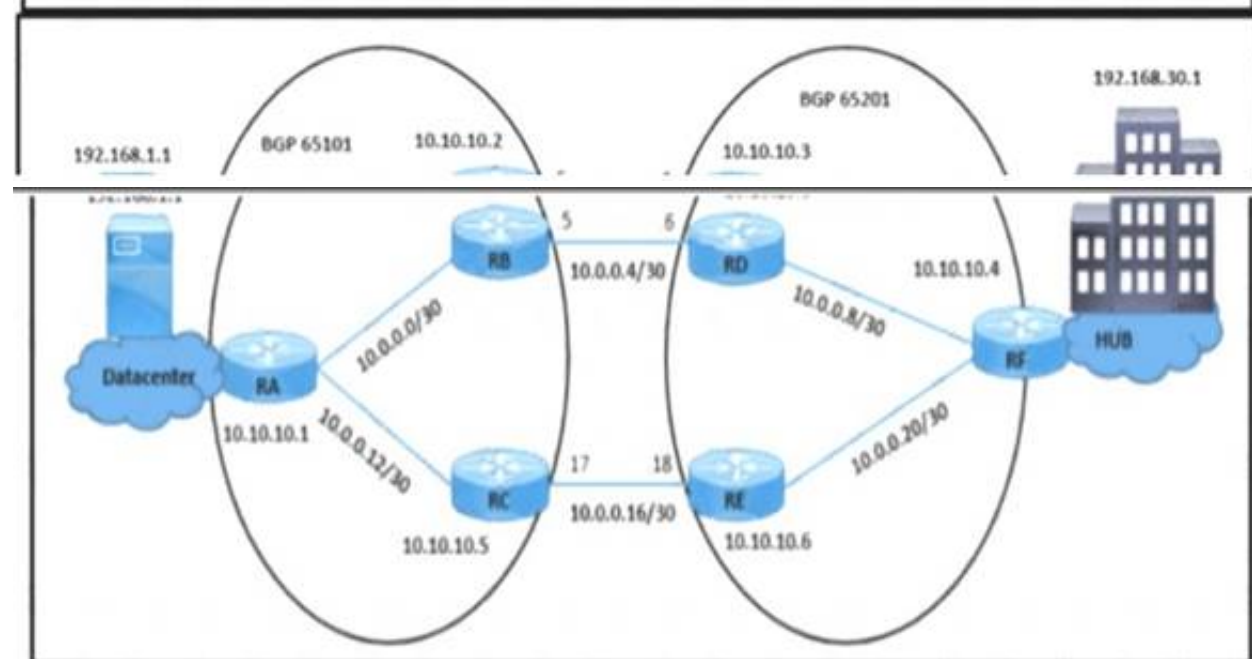
**Answer: A**

**NEW QUESTION 234**

- (Exam Topic 3)

```
RD#show ip bgp 192.168.1.1
Advertised to update-groups:
  3
 65101
 10.10.10.2 (metric 2) from 10.10.10.2 (10.10.10.2)
  Origin IGP, metric 100, localpref 100, weight 65535, valid, external,
best
 65101
 10.0.0.17 (metric 2) from 10.10.10.6 (172.16.20.1)
  Origin IGP, metric 0, localpref 100, valid, internal

RB#show ip bgp 192.168.1.1
BGP routing table entry for 192.168.1.1/32, version 10
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Advertised to update-groups:
  2
Local
 10.10.10.1 (metric 2) from 10.10.10.1 (192.168.1.1)
  Origin IGP, metric 0, localpref 100, valid, internal, best
```



Refer to the exhibit. A customer finds that traffic from the application server (192.168.1.1) to the HUB site passes through a congested path that causes random packet drops. The NOC team influences the BGP path with MED on RB, but RD still sees that traffic coming from RA is not taking an alternate route. Which configuration resolves the issue?

A)

```
RD(config)#router bgp 65201
RD(config-router)#no neighbor 10.10.10.2 weight 65535
```

B)

```
RB(config)#router bgp 65101
RB(config-router)#no neighbor 10.10.10.3 route-map HIGH-LP out
```

C)

```
RB(config)#router bgp 65101
RB(config-router)#neighbor 10.10.10.3 weight 50
```

D)

```
RC(config)#router bgp 65101
RC(config-router)#neighbor 10.10.10.6 route-map HIGH-LP out
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

**NEW QUESTION 237**

- (Exam Topic 3)

Which protocol must be secured with MD-5 authentication across the MPLS cloud to prevent hackers from introducing bogus routers?

- A. MP-BGP



- B. LSP
- C. RSVP
- D. LDP

**Answer:** A

#### NEW QUESTION 238

- (Exam Topic 3)

A network administrator added a new spoke site with dynamic IP on the DMVPN network. Which configuration command passes traffic on the DMVPN tunnel from the spoke router?

- A. ip nhrp registration ignore
- B. ip nhrp registration no-registration
- C. ip nhrp registration dynamic
- D. ip nhrp registration no-unique

**Answer:** D

#### NEW QUESTION 240

- (Exam Topic 3)

How is VPN routing information distributed in an MPLS network?

- A. The top level of the customer data packet directs it to the correct CE device
- B. It is established using VPN IPsec peers.
- C. It is controlled using of VPN target communities.
- D. It is controlled through the use of RD.

**Answer:** C

#### Explanation:

The distribution of virtual private network (VPN) routing information is controlled through the use of VPN route target communities, implemented by Border Gateway Protocol (BGP) extended communities.

Reference:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp\\_l3\\_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/m](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/m)

#### NEW QUESTION 241

- (Exam Topic 3)

Refer to the exhibit. An engineer is trying to log in to R1 via R3 loopback address. Which action resolves the issue?

- A. Add transport input SCP
- B. Add transport input none
- C. Remove the IPv6 traffic filter from R1, which is blocking the Telnet.
- D. Remove the IPv6 traffic from R1, which is blocking the SSH

**Answer:** C

#### NEW QUESTION 242

- (Exam Topic 3)

Which function does LDP provide in an MPLS topology?

- A. It enables a MPLS topology to connect multiple VPNs to P routers.
- B. It provides hop-by-hop forwarding in an MPLS topology for LSRs.
- C. It exchanges routes for MPLS VPNs across different VRFs.
- D. It provides a means for LSRs to exchange IP routes.

**Answer:** B

#### Explanation:

LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward label traffic across an MPLS backbone to particular destinations.

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp\\_ldp/configuration/12-4t/mp-ldp-12-4t-book.pdf](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4t/mp-ldp-12-4t-book.pdf)

#### NEW QUESTION 245

- (Exam Topic 3)

```
admin@linux:~$ telnet 198.51.100.64
Trying 198.51.100.64...
Connected to 198.51.100.64.
Escape character is '^]'.

User Access Verification

Password: admin
CPE> exit
Connection closed by foreign host.
admin@linux:~$ ssh 198.51.100.64
admin@198.51.100.64's password: admin
Permission denied, please try again.
admin@198.51.100.64's password: admin
Permission denied, please try again.
admin@198.51.100.64's password: admin
Connection closed by 198.51.100.64 port 22
admin@linux:~$
```

Refer to the exhibit. An administrator can log in to the device using Telnet but the attempts to log in to the same device using SSH with the same credentials fail. Which action resolves this issue?

- A. Configure SSH service on the router
- B. Configure transport input all on the VTY lines to allow SSH
- C. Configure to use the Telnet user database for SSH as well
- D. Configure the VTY lines with login local

**Answer:** A

#### NEW QUESTION 246

- (Exam Topic 3)

Refer to the exhibits.

##### London – "show ip route" output

Gateway of last resort is not set

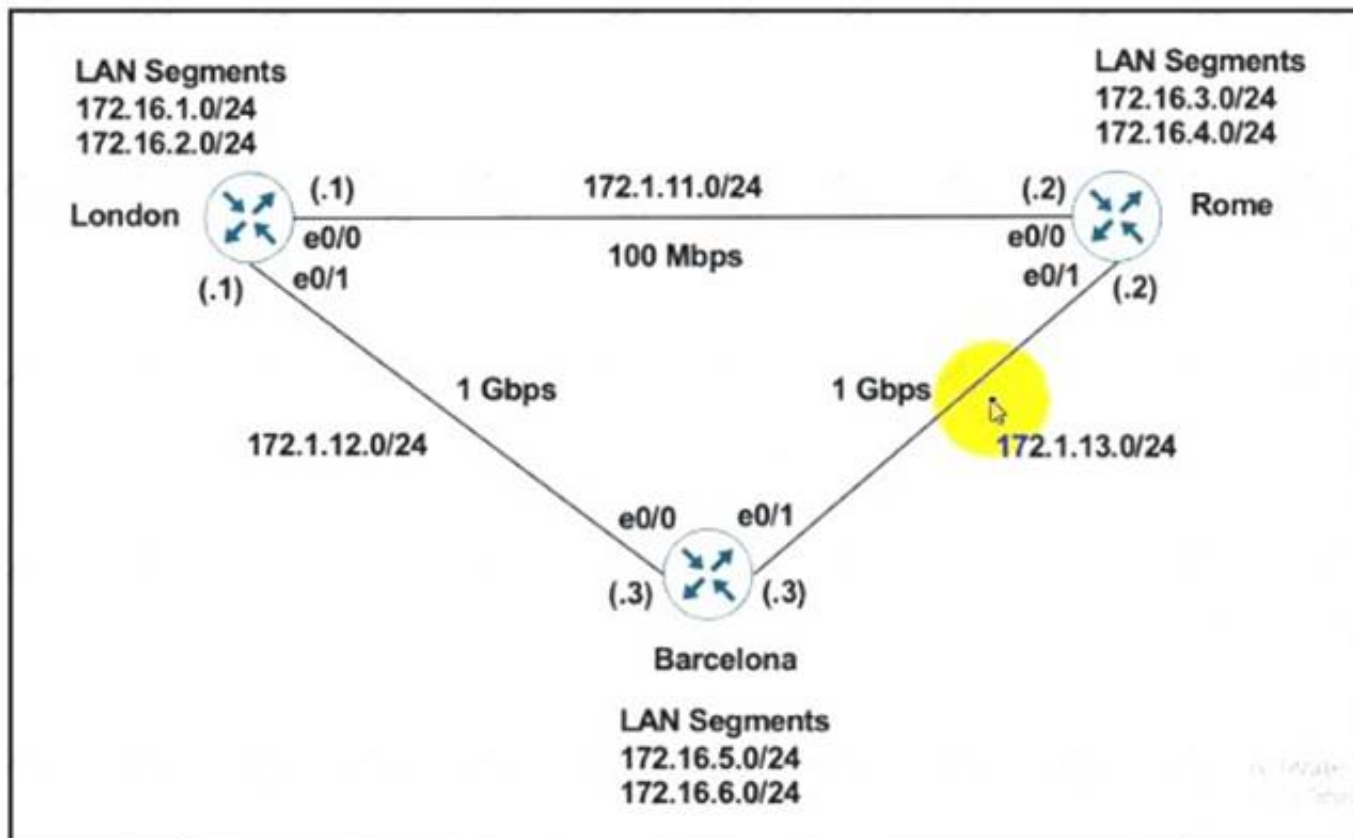
```

172.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
C    172.1.11.0/24 is directly connected, Ethernet0/0
L    172.1.11.1/32 is directly connected, Ethernet0/0
C    172.1.12.0/24 is directly connected, Ethernet0/1
L    172.1.12.1/32 is directly connected, Ethernet0/1
D    172.1.13.0/24 [90/76800] via 172.1.11.2, 00:00:50, Ethernet0/0
172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C    172.16.1.0/24 is directly connected, Loopback0
L    172.16.1.1/32 is directly connected, Ethernet0/0
C    172.16.2.0/24 is directly connected, Loopback1
L    172.16.2.1/32 is directly connected, Loopback1
R    172.16.3.0/24 [120/1] via 172.1.11.2, 00:00:08, Ethernet0/0
R    172.16.4.0/24 [120/1] via 172.1.11.2, 00:00:08, Ethernet0/0
D    172.16.5.0/24 [90/156160] via 172.1.12.3, 00:00:50, Ethernet0/1
D    172.16.6.0/24 [90/156160] via 172.1.12.3, 00:00:50, Ethernet0/1
```

##### Rome - "show run | section router" output

```

router eigrp 111
 network 172.1.0.0
 network 172.16.0.0
 no auto-summary
```



London must reach Rome using a faster path via EIGRP if all the links are up but it failed to take this path Which action resolves the issue?

- A. Increase the bandwidth of the link between London and Barcelona
- B. Use the network statement on London to inject the 172.16.X.0/24 networks into EIGRP.
- C. Change the administrative distance of RIP to 150
- D. Use the network statement on Rome to inject the 172.16.X.0/24 networks into EIGRP

**Answer: D**

#### NEW QUESTION 250

- (Exam Topic 3)

Which OSI model is used to insert an MPLS label?

- A. between Layer 5 and Layer 6
- B. between Layer 1 and Layer 2
- C. between Layer 3 and Layer 4
- D. between Layer 2 and Layer 3

**Answer: D**

#### NEW QUESTION 255

- (Exam Topic 3)

An engineer configured routing between multiple OSPF domains and introduced a routing loop that caused network instability. Which action resolves the problem?

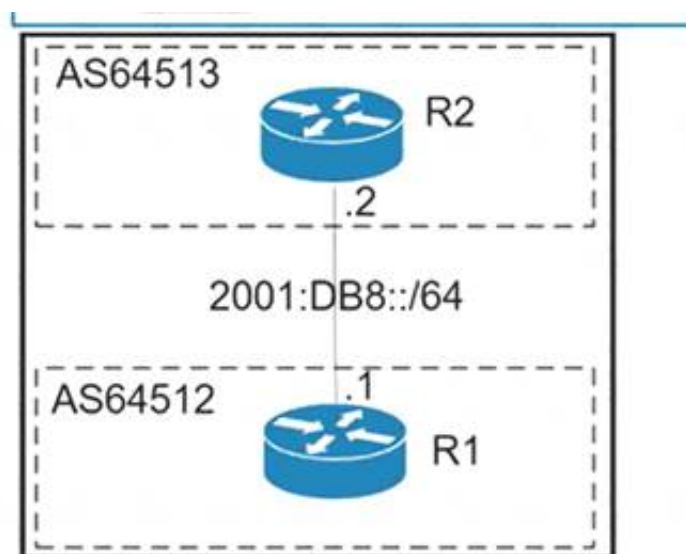
- A. Set a tag using the redistribute command toward a domain and deny inbound in the other domain by a matching tag
- B. Set a tag using the redistribute command toward a different domain and deny the matching tag when exiting from that domain
- C. Set a tag using the network command in a domain and use the route-map command to deny the matching tag when exiting toward a different domain
- D. Set a tag using the network command in a domain and use the route-map command to deny the matching tag when entering into a different domain

**Answer: A**

#### NEW QUESTION 257

- (Exam Topic 3)





```
R1#show ipv6 access-list
IPv6 access list inbound-acl
  permit tcp host 2001:DB8::2 eq bgp host 2001:DB8::1 (75 matches) sequence 20
  permit tcp host 2001:DB8::2 host 2001:DB8::1 eq bgp (17 matches) sequence 30
  deny ipv6 2001:DB8::/32 any (77 matches) sequence 40
  permit ipv6 any (20 matches) sequence 1000
R1#ping ipv6 2001:DB8::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8::2, timeout is 2 seconds:
```

```
.....
Success rate is 0 percent (0/5)
R1#show ipv6 access-list
IPv6 access list inbound-acl
  permit tcp host 2001:DB8::2 eq bgp host 2001:DB8::1 (77 matches) sequence 20
  permit tcp host 2001:DB8::2 host 2001:DB8::1 eq bgp (19 matches) sequence 30
  deny ipv6 2001:DB8::/32 any (95 matches) sequence 40
  permit ipv6 any (23 matches) sequence 1000
R1#
```

Refer to the exhibit. An engineer applied filter on R1. The interface flapped between R1 and R2 and cleaning the BGP session did not restore the BGP session and failed. Which action must the engineer take to restore the BGP session from R2 to R1?

- A. Apply the IPv6 traffic filter in the outbound direction on the interface
- B. ICMPv6 must be permitted by the IPv6 traffic filter
- C. Enable the BGP session, which went down when the session was cleared.
- D. Swap the source and destination IP addresses in the IPv6 traffic filter

**Answer: B**

#### NEW QUESTION 260

- (Exam Topic 3)

Refer to the exhibit.

```
router ospfv3 1
router-id 10.1.1.1
address-family ipv4 unicast
passive-interface Loopback0
exit-address-family
address-family ipv6 unicast
passive-interface Loopback0
exit-address-family
interface Loopback0
ip address 10.1.1.1 255.255.255.255
ipv6 address 2001:DB8::1/64
ospfv3 10 ipv4 area 10
ospfv3 10 ipv6 area 0
interface GigabitEthernet2
ip address 10.10.10.1 255.255.255.0
ipv6 enable
ospfv3 10 ipv4 area 10
ospfv3 10 ipv6 area 0
```

An engineer noticed that the router log messages do not have any information about when the event occurred. Which action should the engineer take when

enabling service time stamps to improve the logging functionality at a granular level?

- A. Replace OSPF process 10 on the interfaces with OSPF process 1 and configure an additional router ID with IPv6 address
- B. Replace OSPF process 10 on the interfaces with OSPF process 1. and remove process 10 from the global configuration
- C. Replace OSPF process 10 on the interfaces with OSPF process 1 for the IPv6 address and remove process 10 from the global configuration
- D. Replace OSPF process 10 on the interfaces with OSPF process 1 for the IPv4 address and remove process 10 from the global configuration

**Answer:** D

#### NEW QUESTION 265

- (Exam Topic 3)

Refer to the exhibit.

```
Tunnel source 199.1.1.1, destination 200.1.1.3
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
```

An engineer must establish a point-to-point GRE VPN between R1 and the remote site. Which configuration accomplishes the task for the remote site?

- A. Interface Tunnel1 tunnel source 199.1.1.1 tunnel destination 200.1.1.3 ip address 192.168.1.3 255.255.255.0
- B. Interface Tunnel1 tunnel source 200.1.1.3 tunnel destination 199.1.1.1 ip address 192.168.1.1 255.255.255.0
- C. Interface Tunnel1 tunnel source 200.1.1.3 tunnel destination 199.1.1.1 ip address 192.168.1.3 255.255.255.0
- D. Interface Tunnel tunnel source 199.1.1.1 tunnel destination 200.1.1.3 ip address 192.168.1.1 255.255.255.0

**Answer:** C

#### NEW QUESTION 270

- (Exam Topic 3)

What is a MPLS PHP label operation?

- A. Downstream node signals to remove the label.
- B. It improves P router performance by not performing multiple label lookup.
- C. It uses implicit-NULL for traffic congestion from source to destination forwarding
- D. PE removes the outer label before sending to the P router.

**Answer:** A

#### NEW QUESTION 273

- (Exam Topic 3)

What is a characteristic of Layer 3 MPLS VPNs?

- A. LSP signaling requires the use of unnumbered IP links for traffic engineering.
- B. Traffic engineering supports multiple IGP instances
- C. Traffic engineering capabilities provide QoS and SLAs.
- D. Authentication is performed by using digital certificates or preshared keys.

**Answer:** C

#### Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp\\_te\\_diffserv/configuration/15-mt/mp-te-diffserv-15-mt-bo](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_diffserv/configuration/15-mt/mp-te-diffserv-15-mt-bo)

MPLS traffic engineering supports only a single IGP process/instance

The MPLS traffic engineering feature does not support routing and signaling of LSPs over unnumbered IP links.

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp\\_te\\_path\\_setup/configuration/xs-3s/mp-te-path-setup-xe-3s-book/mp-te-enhance-xe.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_path_setup/configuration/xs-3s/mp-te-path-setup-xe-3s-book/mp-te-enhance-xe.html)

#### NEW QUESTION 277

- (Exam Topic 3)

```
R1 (config)# ip vrf CCNP
R1 (config-vrf)# rd 1:100
R1 (config-vrf)# exit
R1 (config)# interface Loopback0
R1 (config-if)# ip address 10.1.1.1 255.255.255.0
R1 (config-if)# ip vrf forwarding CCNP
R1 (config-if)# exit
R1 (config)# exit
R1# ping vrf CCNP 10.1.1.1
% Unrecognized host or address, or protocol not running.
```

Refer to the exhibit Which command must be configured to make VRF CCNP work?

- ☒ interface Loopback0  
ip address 10.1.1.1 255.255.255.0  
vrf forwarding CCNP
- ☐ interface Loopback0  
ip address 10.1.1.1 255.255.255.0
- ☐ interface Loopback0  
vrf forwarding CCNP
- ☐ interface Loopback0  
ip address 10.1.1.1 255.255.255.0  
ip vrf forwarding CCNP

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

#### NEW QUESTION 279

- (Exam Topic 3)

A company is redesigning WAN infrastructure so that all branch sites must communicate via the head office and the head office can directly communicate with each site independently. The network engineer must configure the head office router by considering zero-touch technology when adding new sites in the same WAN infrastructure. Which configuration must be applied to the head office router to meet this requirement?

- ☐ interface Tunnel0  
tunnel mode ip  
ip nhrp map multicast dynamic
- ☒ interface Tunnel0  
tunnel mode dmvrp  
ip nhrp redirect
- ☐ interface Tunnel0  
tunnel mode ip  
ip nhrp redirect
- ☐ interface Tunnel0  
tunnel mode gre multipoint  
ip nhrp map multicast dynamic

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

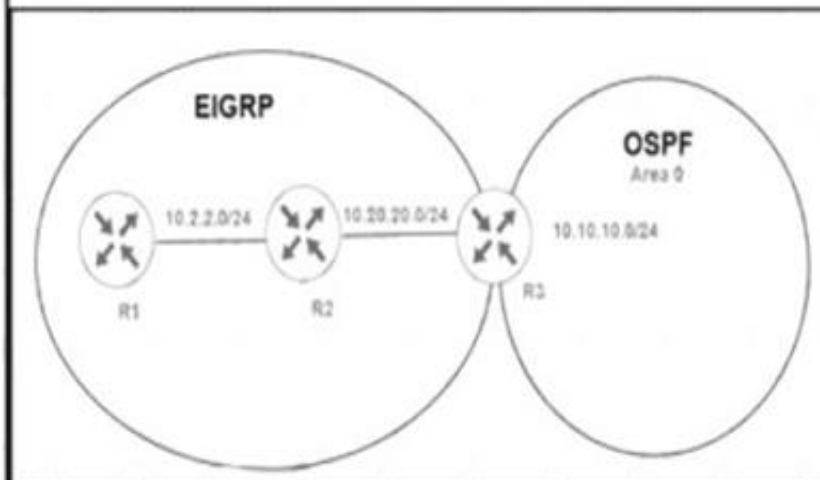
#### NEW QUESTION 281

- (Exam Topic 3)



```
R2#show ip eigrp topology 10.10.10.0 255.255.255.0
IP-EIGRP (AS 1): Topology entry for 10.10.10.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD
  is 256005120
  Routing Descriptor Blocks:
    10.20.20.3 (FastEthernet0/1), from 10.20.20.3, Send flag is
    0x0
    Composite metric is (256005120/256002560), Route is
    External
    Vector metric:
      Minimum bandwidth is 10 Kbit
      Total delay is 200 microseconds
      Reliability is 10/255
      Load is 10/255
      Minimum MTU is 10
      Hop count is 1
    External data:
      Originating router is 10.1.1.1
      AS number of route is 1
      External protocol is OSPF, external metric is 0
      Administrator tag is 0 (0x00000000)

R1#sh run | s eigrp
router eigrp 1
  router-id 10.1.1.1
  network 10.2.2.0 0.0.0.255
  no auto-summary
```



Refer to the exhibit. An engineer configured router R3 to redistribute the prefix 10.10.10.0/24 from OSPF into EIGRP. R1 has no connectivity to the prefix. Which action enables receipt of prefixes on R1?

- A. R3 is advertising the 10.20.20.0/24 prefix with a TTL of 1, R3 must set the TTL to 2 for this prefix.
- B. R1 does not have a neighbor relationship with R2. The EIGRP process should be cleared on R1.
- C. Duplicate router IDs on R1 and R3, R1 should modify its router ID.
- D. R1 is not receiving the next-hop IP address of R3. R2 must enable the network 10.20.20.0/24 within EIGRP.

**Answer: B**

## NEW QUESTION 282

- (Exam Topic 3)

The network administrator configured the router for Control Plane Policing to limit OSPF traffic to be policed to 1 Mbps. Any traffic that exceeds this limit must also be allowed at this point for traffic analysis. The router configuration is:

```
access-list 100 permit ospf any any
```

```
!
```

```
class-map CM-OSPF match access-group 100
```

```
!
```

```
policy-map PM-COPP class CM-OSPF
```

```
  police 1000000 conform-action transmit
```

```
!
```

```
control-plane
```

```
  service-policy output PM-COPP
```

The Control Plane Policing failed to monitor and police OSPF traffic. Which configuration resolves this issue?

- ☐ no access-list 100  
 access-list 100 permit tcp any any eq 179  
 access-list 100 permit ospf any any  
 access-list 101 permit tcp any any range 22 23  
 !  
 !  
 class-map CM-MGMT  
 no match access-group 100  
 match access-group 101  
 !  
 control-plane  
 no service-policy output PM-COPP  
 service-policy input PM-COPP
- ☐ No access-list 100  
 access-list 100 permit tcp any any eq 179  
 access-list 100 permit tcp any any range eq 22  
 access-list 100 permit tcp any any range eq 23  
 access-list 100 permit ospf any any
- ☐ control-plane  
 no service-policy output PM-COPP  
 service-policy input PM-COPP
- ☐ no access-list 100  
 access-list 100 permit tcp any any eq 179  
 access-list 100 permit ospf any any  
 access-list 101 permit tcp any any range 22 23  
 !  
 !  
 class-map CM-MGMT  
 no match access-group 100  
 match access-group 101

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

#### NEW QUESTION 285

- (Exam Topic 3)

A newly installed spoke router is configured for DMVPN with the `ip mtu 1400` command. Which configuration allows the spoke to use fragmentation with the maximum negotiated TCP MTU over GRE?

- A. `ip tcp adjust-mss 1360``crypto ipsec fragmentation after-encryption`
- B. `ip tcp adjust-mtu 1360``crypto ipsec fragmentation after-encryption`
- C. `ip tcp adjust-mss 1360``crypto ipsec fragmentation mtu-discovery`
- D. `ip tcp adjust-mtu 1360``crypto ipsec fragmentation mtu-discovery`

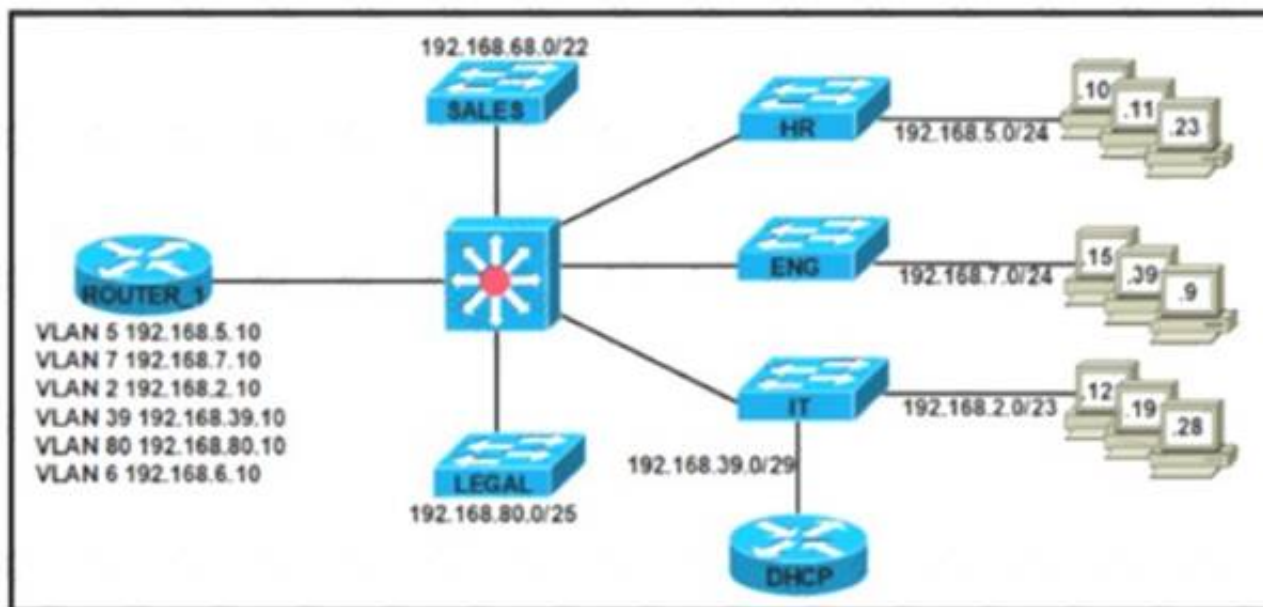
Answer: A

#### Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troublesh>

#### NEW QUESTION 288

- (Exam Topic 3)



Refer to the exhibit. After an engineer configured a new Cisco router as a DHCP server, users reported two primary issues:

- > Devices in the HR subnet have intermittent connectivity problems.
- > Workstations in the LEGAL subnet cannot obtain IP addresses.

Which configurations must the engineer apply to ROUTER\_1 to restore connectivity for the affected devices?

- interface GigabitEthernet0/0.5  
  encapsulation dot1Q 5  
  ip address 192.168.5.10 255.255.255.0  
  ip helper-address 192.168.39.100  
  !  
  interface GigabitEthernet0/0.80  
  encapsulation dot1Q 80  
  ip address 192.168.80.10 255.255.255.128  
  ip helper-address 192.168.39.100  
  !  
  ip dhcp excluded-address 192.168.5.1 192.168.5.10  
  ip dhcp excluded-address 192.168.80.1 192.168.80.10  
  !  
  ip dhcp pool LEGAL  
  network 192.168.80.0 255.255.255.128  
  default-router 192.168.80.10  
  
  ip dhcp pool HR  
  network 192.168.5.0 255.255.255.0  
  default-router 192.168.5.10
- interface GigabitEthernet0/0.5  
  encapsulation dot1Q 5  
  ip address 192.168.5.10 255.255.255.0  
  ip helper-address 192.168.39.100  
  !  
  interface GigabitEthernet0/0.80  
  encapsulation dot1Q 80  
  ip address 192.168.80.10 255.255.255.128  
  ip helper-address 192.168.39.100  
  !  
  ip dhcp excluded-address 192.168.80.1 192.168.80.10  
  !  
  ip dhcp pool LEGAL  
  network 192.168.80.0 255.255.255.128  
  default-router 192.168.80.10  
  !  
  ip dhcp pool HR  
  network 192.168.5.0 255.255.255.0  
  default-router 192.168.5.10



```
○ interface GigabitEthernet0/0.5
  encapsulation dot1Q 5
  ip address 192.168.5.10 255.255.255.0
  ip helper-address 192.168.93.100
!
interface GigabitEthernet0/0.80
  encapsulation dot1Q 80
  ip address 192.168.80.10 255.255.255.128
  ip helper-address 192.168.39.100
!
ip dhcp excluded-address 192.168.5.1 192.168.5.1
ip dhcp excluded-address 192.168.80.1 192.168.80.10
!
ip dhcp pool LEGAL
  network 192.168.80.0 255.255.255.128
  default-router 192.168.80.10
!
ip dhcp pool HR
  network 192.168.5.0 255.255.255.0
  default-router 192.168.5.10

○ interface GigabitEthernet0/0.5
  encapsulation dot1Q 5
  ip address 192.168.5.10 255.255.255.0
  ip helper-address 192.168.39.100
!
interface GigabitEthernet0/0.80
  encapsulation dot1Q 80
  ip address 192.168.80.10 255.255.255.128
  ip helper-address 192.168.39.100
!
ip dhcp excluded-address 192.168.5.1 192.168.5.5
ip dhcp excluded-address 192.168.80.1 192.168.80.110
!
ip dhcp pool LEGAL
  network 192.168.80.0 255.255.255.128
  default-router 192.168.80.10
!
ip dhcp pool HR
  network 192.168.5.0 255.255.255.0
  default-router 192.168.5.10
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** A

#### NEW QUESTION 293

- (Exam Topic 3)

Refer to the exhibit.

```
*Sep 26 19:50:43.504: SNMP: Packet received via UDP from
192.168.1.2 on GigabitEthernet0/1SrParseV3SnmppMessage: No
matching Engine ID.

SrParseV3SnmppMessage: Failed.
SrDoSnmpp: authentication failure, Unknown Engine ID

*Sep 26 19:50:43.504: SNMP: Report, reqid 29548, errstat 0,
erridx 0
internet.6.3.15.1.1.4.0 = 3
*Sep 26 19:50:43.508: SNMP: Packet sent via UDP to 192.168.1.2
process_mgmt_req_int: UDP packet being de-queued
```

Which two commands provide the administrator with the information needed to resolve the issue? (Choose two.)

- A. Show snmp user
- B. debug snmp engine-id
- C. debug snmpv3 engine-id
- D. debug snmp packet
- E. showsnmpv3 user

**Answer:** AD

#### Explanation:

There are 3 values in the SNMPv3 header that must match for the communication to take place: snmpEngineID, snmpEngineTime, snmpEngineBoots. The error received indicates a problem with the EngineID value: "authentication failure, Unknown Engine ID"

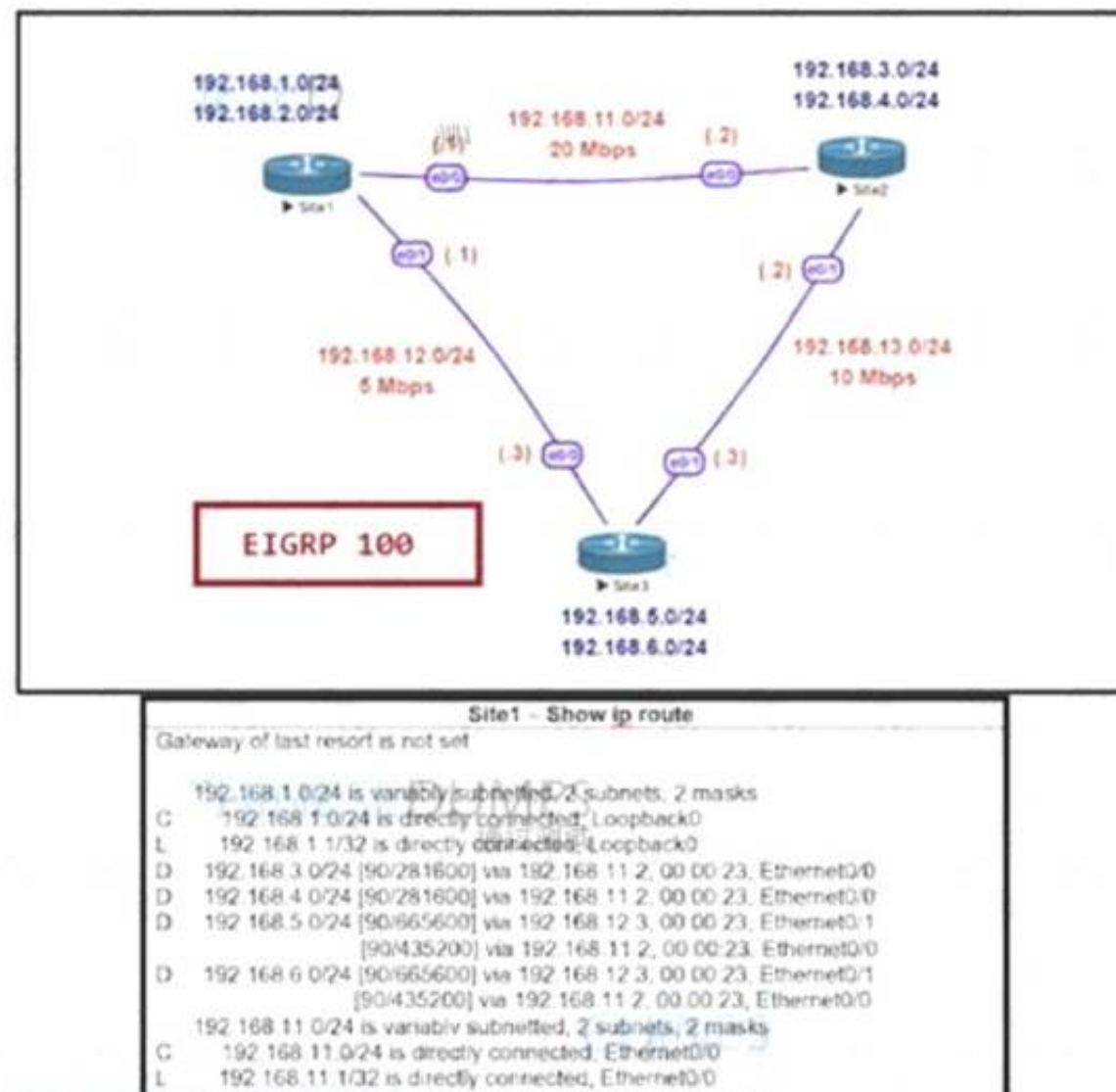
To specify the Engine ID, we can use the command "show snmp user". The following example specifies the username as abcd with Engine ID: 00000009020000000C025808:

```
Router#show snmp user abcd
User name: abcd
Engine ID: 00000009020000000C025808
storage-type: nonvolatile active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: 3DES
Group name: VacmGroupName
Group name: VacmGroupName
```

The "debug snmp packet" command displays all SNMP packets that are arriving and being replied to.

#### NEW QUESTION 294

- (Exam Topic 3)



```
D    192.168.13.0/24 [90/563200] via 192.168.12.3, 00:00:23, Ethernet0/1
    [90/307200] via 192.168.11.2, 00:00:23, Ethernet0/0

Site1 - Show ip eigrp topology
P 192.168.3.0/24, 1 successors, FD is 230400
  via 192.168.11.2 (281600/128256), Ethernet0/0
  via 192.168.12.3 (691200/204800), Ethernet0/1
P 192.168.12.0/24, 1 successors, FD is 537600
  via Connected, Ethernet0/1
P 192.168.13.0/24, 2 successors, FD is 307200
  via 192.168.12.3 (563200/76800), Ethernet0/1
  via 192.168.11.2 (307200/281600), Ethernet0/0
P 192.168.1.0/24, 1 successors, FD is 128256
  via Connected, Loopback0
P 192.168.6.0/24, 2 successors, FD is 435200
  via 192.168.12.3 (665600/128256), Ethernet0/1
  via 192.168.11.2 (435200/409600), Ethernet0/0
P 192.168.4.0/24, 1 successors, FD is 230400
  via 192.168.11.2 (281600/128256), Ethernet0/0
  via 192.168.12.3 (691200/204800), Ethernet0/1
P 192.168.5.0/24, 2 successors, FD is 435200
  via 192.168.12.3 (665600/128256), Ethernet0/1
  via 192.168.11.2 (435200/409600), Ethernet0/0
P 192.168.11.0/24, 1 successors, FD is 153600
  via Connected, Ethernet0/0

Site1 - Show run | section router eigrp
router eigrp 100
 variance 2
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.11.0
 network 192.168.12.0
```

Refer to the exhibit. Site1 must perform unequal cost load balancing toward the segments behind Site2 and Site3. Some of the routes are getting load balanced but others are not. Which configuration allows Site1 to load balance toward all the LAN segments of the remote routers?

- ☐ Site2
- router eigrp 100  
variance 3
- ☐ Site2
- router eigrp 100  
variance 2
- ☐ Site3
- router eigrp 100  
variance 2
- ☐ Site1
- router eigrp 100  
variance 3

- A. Option A  
B. Option B  
C. Option C  
D. Option D

Answer: D

NEW QUESTION 295

- (Exam Topic 3)

Which technique removes the outermost label of an MPLS-tagged packet before the packet is forwarded to an adjacent LER?

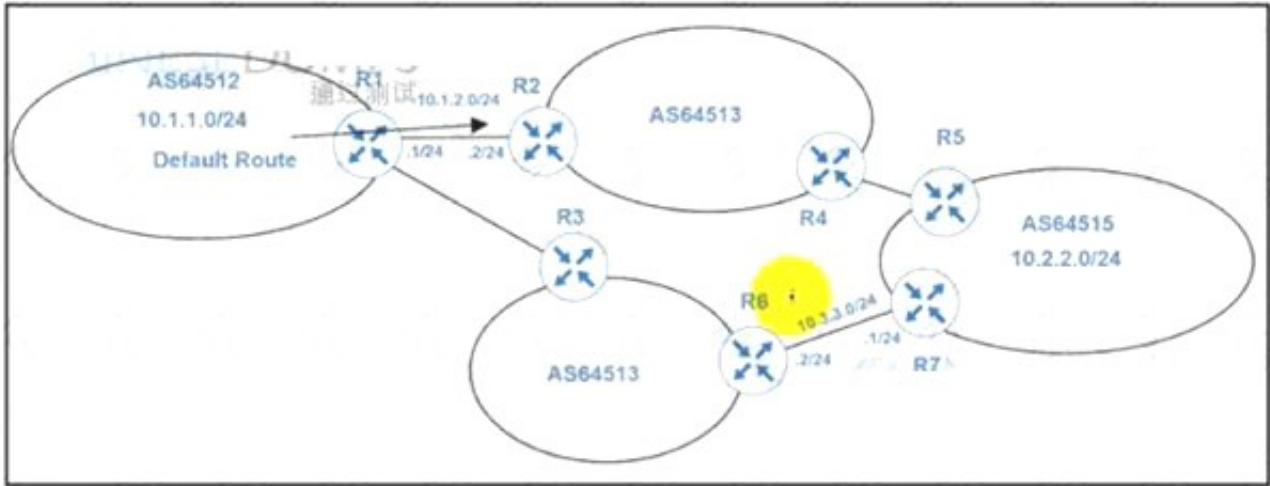
- A. label swap  
B. explicit-null  
C. label imposition  
D. PHP

Answer: D

NEW QUESTION 299

- (Exam Topic 3)

Refer to the exhibit.



An engineer must configure PBR on R1 to reach to 10.2.2.0/24 via R3 AS64513 as the primary path and a backup route through default route via R2 AS64513. All BGP routes are in the routing table of R1. but a static default route overrides BGP routes. Which PBR configuration achieves the objective?



```

access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
|
route-map PBR permit 10
match ip address 100
set ip next-hop 10.3.3.1

access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
|
route-map PBR permit 10
match ip address 100
set ip next-hop recursive 10.3.3.1

access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
|
route-map PBR permit 10
match ip address 100
set ip next-hop recursive 10.3.3.1

access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
|
route-map PBR permit 10
match ip address 100
set ip next-hop 10.3.3.1
  
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

#### NEW QUESTION 301

- (Exam Topic 3)

Refer to the exhibit.

```

R1(config)#ipv6 prefix-list PRE-PEND-PREFIX permit 2001:db8:0:a::/64
R1(config)#route-map PRE-PEND permit 10
R1(config-route-map)#match ipv6 address prefix-list PRE-PEND-PREFIX
R1(config-route-map)#set as-path prepend 65412
R1(config)#router bgp 65412
R1(config-router)#address-family ipv6
R1(config-router-af)#neighbor 2001:db8:0:20::2 route-map PRE-PEND out
  
```

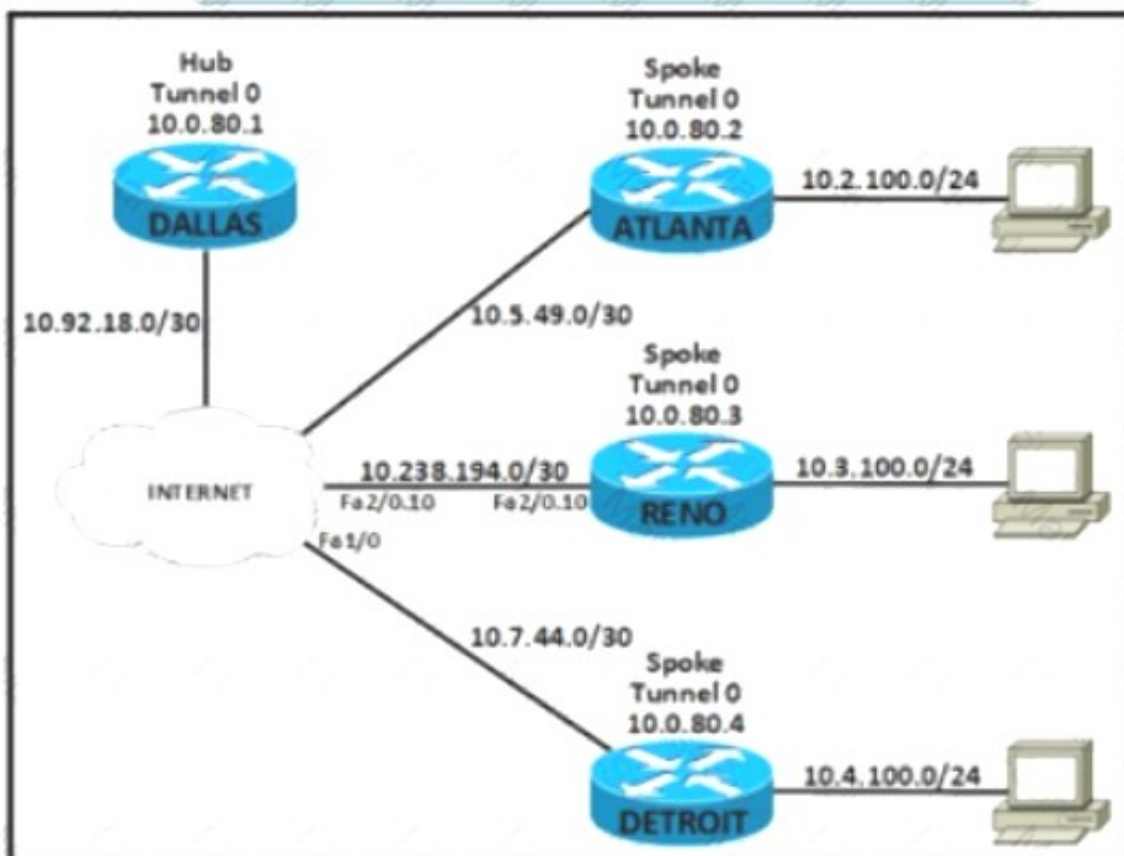
R1 has a route map configured, which results in a loss of partial IPv6 prefixes for the BGP neighbor, resulting in service degradation. How can the full service be restored?

- A. The neighbor requires a soft reconfiguration, and this will clear the policy without resetting the BGP TCP connection.
- B. The prefix list requires all prefixes that R1 is advertising to be added to it, and this will allow additional prefixes to be advertised.
- C. The route map requires a deny 20 statement without set conditions, and this will allow additional prefixes to be advertised.
- D. The route map requires a permit 20 statement without set conditions, and this will allow additional prefixes to be advertised.

**Answer: D**

#### NEW QUESTION 306

- (Exam Topic 3)



Refer to the exhibit An engineer must connect the Reno and Detroit spokes using DMVPN phase 2 Hub tunnel configuration is

QUESTION 101: Which configuration accomplishes the task?

Dallas  
interface Tunnel0  
ip address 10.0.80.1 255.255.255.0  
ip nhrp authentication cisco123  
ip nhrp map multicast dynamic  
ip nhrp network-id 5  
tunnel source Serial0/0  
tunnel mode gre multipoint

Which configuration accomplishes the task?

☐ Reno  
interface Tunnel0  
ip address 10.0.80.3 255.255.255.0  
ip nhrp authentication cisco321  
ip nhrp map multicast 10.92.18.2  
ip nhrp map 10.0.80.1 10.92.18.2  
ip nhrp network-id 5  
ip nhrp nhs 10.0.80.1  
tunnel source 10.238.194.2  
tunnel mode gre multipoint

Detroit  
interface Tunnel0  
ip address 10.0.80.4 255.255.255.0  
ip nhrp authentication cisco321  
ip nhrp map 10.0.80.1 10.92.18.2  
ip nhrp map multicast 10.92.18.2  
ip nhrp network-id 5  
ip nhrp nhs 10.0.80.1  
tunnel source 10.7.44.2  
tunnel mode gre multipoint

☐ Reno  
interface Tunnel0  
ip address 10.0.80.3 255.255.255.0  
ip nhrp authentication cisco123  
ip nhrp map multicast 10.92.18.2  
ip nhrp map 10.92.18.2 10.0.80.1  
ip nhrp network-id 5  
ip nhrp nhs 10.0.80.1  
tunnel source 10.238.194.2  
tunnel mode gre multipoint

Detroit  
interface Tunnel0  
ip address 10.0.80.4 255.255.255.0  
ip nhrp authentication cisco123  
ip nhrp map 10.92.18.2 10.0.80.1  
ip nhrp map multicast 10.92.18.2  
ip nhrp network-id 5  
ip nhrp nhs 10.0.80.1  
tunnel source 10.7.44.2  
tunnel mode gre multipoint

☐ Reno  
interface Tunnel0  
ip address 10.0.80.3 255.255.255.0  
ip nhrp authentication cisco123  
ip nhrp map broadcast 10.92.18.2  
ip nhrp map 10.0.80.1 10.92.18.2  
ip nhrp network-id 5  
ip nhrp nhs 10.0.80.1  
tunnel source 10.238.194.2  
tunnel mode gre multipoint

Detroit  
interface Tunnel0  
ip address 10.0.80.4 255.255.255.0  
ip nhrp authentication cisco123  
ip nhrp map 10.0.80.1 10.92.18.2  
ip nhrp map broadcast 10.92.18.2  
ip nhrp network-id 5  
ip nhrp nhs 10.0.80.1  
tunnel source 10.7.44.2  
tunnel mode gre multipoint

```

Reno
interface Tunnel0
ip address 10.0.80.3 255.255.255.0
ip nhrp authentication cisco123
ip nhrp map multicast 10.92.18.2
ip nhrp map 10.0.80.1 10.92.18.2
ip nhrp network-id 5
ip nhrp nhs 10.0.80.1
tunnel source 10.238.194.2
tunnel mode gre multipoint
  
```

```

Detroit
interface Tunnel0
ip address 10.0.80.4 255.255.255.0
ip nhrp authentication cisco123
ip nhrp map 10.0.80.1 10.92.18.2
ip nhrp map multicast 10.92.18.2
ip nhrp network-id 5
ip nhrp nhs 10.0.80.1
tunnel source 10.7.44.2
tunnel mode gre multipoint
  
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

#### NEW QUESTION 308

- (Exam Topic 3)

A network administrator cannot connect to a device via SSH. The line vty configuration is as follows:

```

line vty 0 4
location S421T50E27F86
session-timeout 10
transport preferred ssh
transport input all
transport output telnet ssh
stopbits 1
  
```

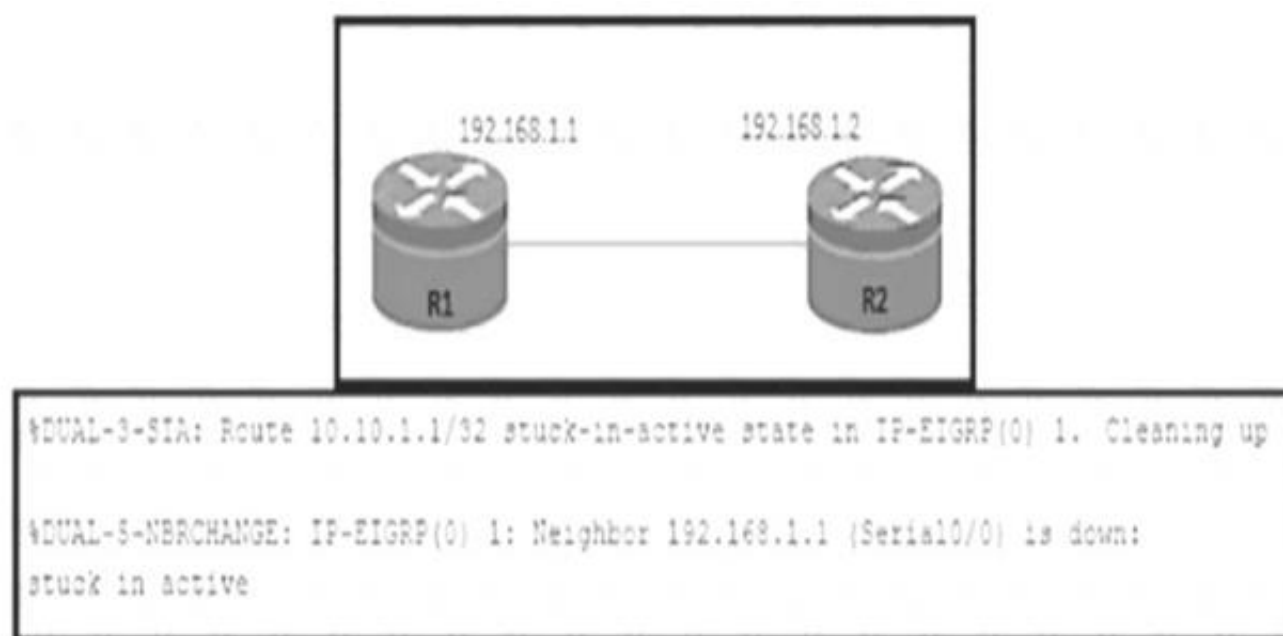
Which action resolves this issue?

- A. Increase the session timeout
- B. Change the stopbits to 10.
- C. Configure the transport input SSH
- D. initialize the SSH key

**Answer: D**

#### NEW QUESTION 311

- (Exam Topic 3)



Refer to the exhibit. An engineer notices a connectivity problem between routers R1 and R2. The frequency of this problem is high during peak business hours. Which action resolves the issue?

- A. Increase the MTU on the interfaces that connect R1 and R2.
- B. Increase the available bandwidth between R1 and R2.
- C. Decrease the EIGRP keepalive and hold down timers on R1 and R2.
- D. Set static EIGRP neighborship between R1 and R2.

**Answer: B**



#### NEW QUESTION 315

- (Exam Topic 3)

The network administrator configured CoPP so that all routing protocol traffic toward the router CPU is limited to 1 mbps. All traffic that exceeds this limit must be dropped. The router is running BGP and OSPF Management traffic for Telnet and SSH must be limited to 500kbps.

access-list 100 permit tcp any any eq 179 access-list 100 permit tcp any any range 22 23 access-list 100 permit ospf any any

!

class-map CM-ROUTING match access-group 100

class-map CM-MGMT match access-group 100

!

policy-map PM-COPP class CM-ROUTING

police 1000000 conform-action transmit class CM-MGMT

police 500000 conform-action transmit

!

control-plane

service-policy output PM-COPP

No traffic is filtering through CoPP, which is resulting in high CPU utilization, which configuration resolves the issue?

A. no access-list 100 access-list 100 permit tcp any any eq 179 access-list 100 permit ospf any any access-list 101 Permit tcp any any range 22 23! class-map CM-MGMT no match access-group 100 match access-group 101

B. control-plane no service-policy output PM-COPP service-policy input PM-COPP

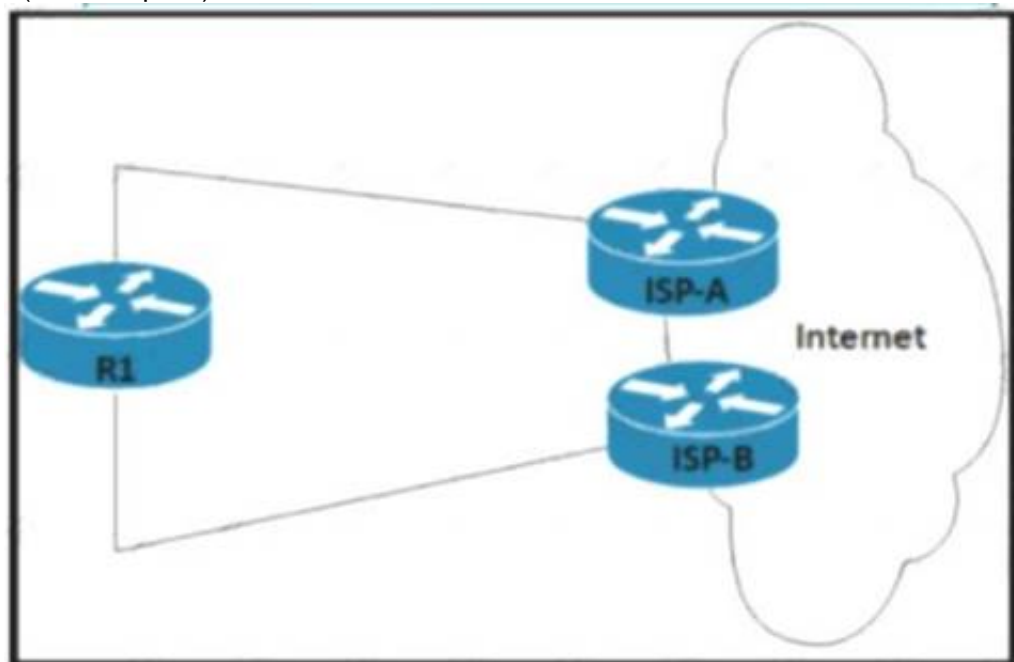
C. No access-list 100 access-list 100 permit tcp any any eq 179 access-list 100 permit tcp any any range eq 22 access-list 100 permit tcp any any range eq 23 access-list 100 permit ospf any any

D. no access-list 100 access-list 100 permit tcp any any eq 179 access-list 100 permit ospf any any access-list 101 Permit tcp any any range 22 23! class-map CM-MGMT no match access-group 100 match access-group 101! control-plane no service-policy output PM-COPP service-policy input PM-COPP

**Answer: D**

#### NEW QUESTION 319

- (Exam Topic 3)



Refer to the exhibit. Router R1 peers with two ISPs using static routes to get to the internet. The requirement is that R1 must prefer ISP-A under normal circumstances and failover to ISP-B if the connectivity to ISP-A is lost. The engineer observes that R1 is load balancing traffic across the two ISPs. Which action resolves the issue by sending traffic to ISP-A only with failover to ISP-B?

A. Configure OSPF between R1, ISP-

B. and ISP-B for dynamic failover if any ISP link to R1 fails

C. Configure two static routes on R1. one pointing to ISP-A and another pointing to ISP-B with 222 admin distance

D. Change the bandwidth of the interface on R1 so that interface to ISP-A has a higher value than the interface to ISP-B

E. Configure two static routes on R1. one pointing to ISP-B with more specific routes and another pointing to ISP-A with summary routes

**Answer: D**

#### NEW QUESTION 322

- (Exam Topic 3)

What does the MP-BGP OPEN message contain?

A. MPLS labels and the IP address of the router that receives the message

B. the version number and the AS number to which the router belongs

C. IP routing information and the AS number to which the router belongs

D. NLRI, path attributes, and IP addresses of the sending and receiving routers

**Answer: B**

#### NEW QUESTION 324

- (Exam Topic 3)

```
R1# configure terminal
R1(config)# hostname CPE1
CPE1(config)# ip domain-name example.com
CPE1(config)# crypto key generate rsa
The name for the keys will be: CPE1.example.com
Choose the size of the key modulus in the range of 360 to 4096
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

CPE1(config)# service password-encryption
CPE1(config)# username csadmin secret Secur3p4s$w0rd
CPE1(config)# line vty 0 4
CPE1(config-line)# transport input telnet ssh
CPE1(config-line)# login local
CPE1(config-line)# end
CPE1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CPE1# ssh 10.0.0.1
% No user specified nor available for SSH client
```

Refer to the exhibit. An administrator must harden a router, but the administrator failed to test the SSH access successfully to the router. Which action resolves the issue?

- A. Configure SSH on the remote device to log in using SSH
- B. SSH syntax must be `ssh -l user ip` to log in to the remote device
- C. Configure enable secret to log in to the device
- D. SSH must be allowed with the `transport output ssh` command

**Answer: B**

#### NEW QUESTION 326

- (Exam Topic 3)

Refer to the exhibit.

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 2 name ISP2
```

The administrator noticed that the connection was flapping between the two ISPs instead of switching to ISP2 when the ISP1 failed. Which action resolves the issue?

- A. Include a valid source-interface keyword in the `icmp-echo` statement.
- B. Reference the track object 1 on the default route through ISP2 instead of ISP1.
- C. Modify the static routes to refer both to the next hop and the outgoing interface.
- D. Modify the threshold to match the administrative distance of the ISP2 route.

**Answer: A**

#### Explanation:

<https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-withdefault-routes-using-l.html>

#### NEW QUESTION 329

- (Exam Topic 3)

Refer to the exhibit.

```
ip prefix-list DMZ-STATIC seq 5 permit 10.1.1.0/24
!
route-map DMZ permit 10
    match ip address prefix-list DMZ-STATIC
!
router ospf 1
network 0.0.0.0 0.0.0.0 area 0
redistribute static route-map DMZ
!
ip route 10.1.1.0 255.255.255.0 10.20.20.1
```

The static route is not present in the routing table of an adjacent OSPF neighbor router. Which action resolves the issue?

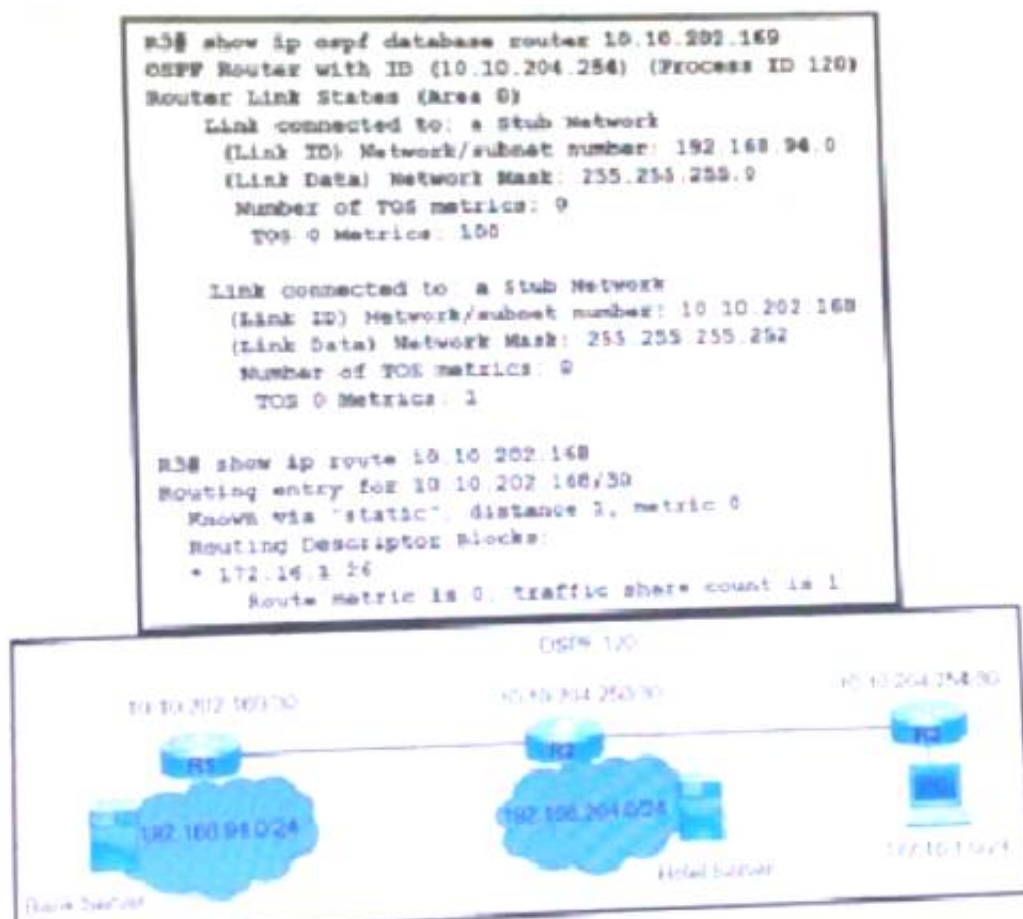
- A. Configure the next hop of 10.20.20.1 in the prefix list DMZ-STATIC
- B. Configure the next-hop interface at the end of the static router for it to get redistributed
- C. Configure a permit 20 statement to the route map to redistribute the static route
- D. Configure the subnets keyword in the redistribution command

**Answer: D**

### NEW QUESTION 332

- (Exam Topic 3)

Refer to the exhibit.



A network engineer finds that PC1 is accessing the hotel website to do the booking but fails to make payment. Which action resolves the issue?

- A. Allow stub network 10.10.202.168/30 on router R3 OSPF.
- B. Decrease the AD to 5 OSPF route 192.168.94.0 on R1.
- C. Increase the AD to 200 of static route 192.168.94.0 on R3.
- D. Configure a reverse route on R1 for PC1 172.16.1.0/24.

**Answer: A**

### NEW QUESTION 333

- (Exam Topic 3)

A network administrator is troubleshooting a high utilization issue on the route processor of a router that was reported by NMS. The administrator logged into the router to check the control plane policing and observed that the BGP process is dropping a high number of routing packets and causing thousands of routes to recalculate frequently. Which solution resolves this issue?

- A. Police the cir for BGP, conform-action transmit, and exceed action transmit.
- B. Shape the pir for BGP, conform-action set-prec-transmit, and exceed action set-frde-transmit.
- C. Shape the cir for BG
- D. conform-action transmit, and exceed action transmit.
- E. Police the pir for BGP, conform-action set-prec-transmit, and exceed action set-clp-transmit.

**Answer: D**

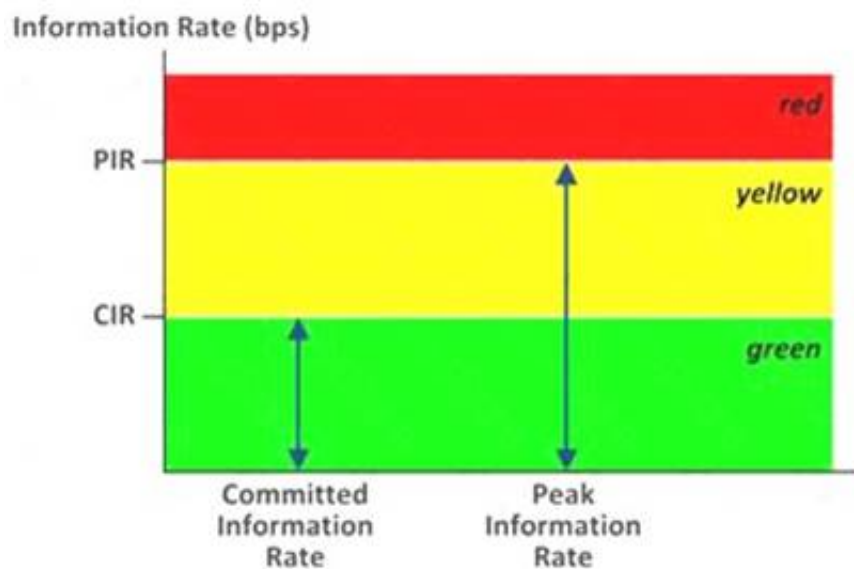
### Explanation:

CIR (Committed Information Rate) is the minimum guaranteed traffic delivered in the network.



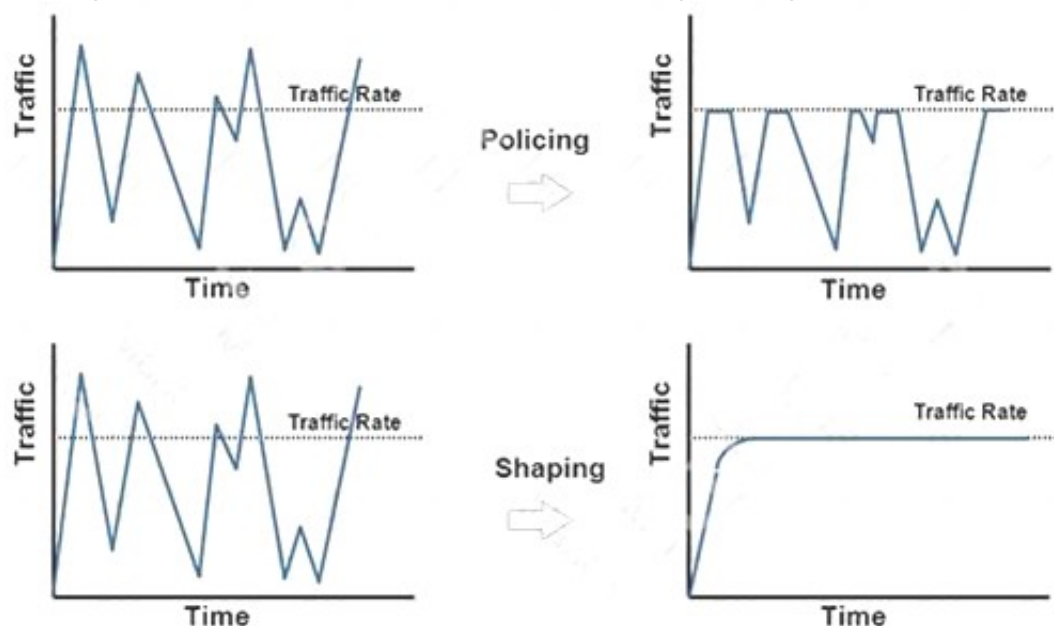
PIR (Peak Information Rate) is the top bandwidth point of allowed traffic in a non busy times without any guarantee.

## Two Rates & Three Colors



+ Policing: is used to control the rate of traffic flowing across an interface. During a bandwidth exceed (crossed the maximum configured rate), the excess traffic is generally dropped or remarked. The result of traffic policing is an output rate that appears as a saw-tooth with crests and troughs. Traffic policing can be applied to inbound and outbound interfaces. Unlike traffic shaping, QoS policing avoids delays due to queuing. Policing is configured in bytes.

+ Shaping: retains excess packets in a queue and then schedules the excess for later transmission over increments of time. When traffic reaches the maximum configured rate, additional packets are queued instead of being dropped to proceed later. Traffic shaping is applicable only on outbound interfaces as buffering and queuing happens only on outbound interfaces. Shaping is configured in bits per second.



Therefore in this case we can only policing, not shaping as traffic shaping is applicable only on outbound interfaces as buffering and queuing happens only on outbound interfaces. Moreover, BGP traffic is not important so we can drop the excess packets without any problems.

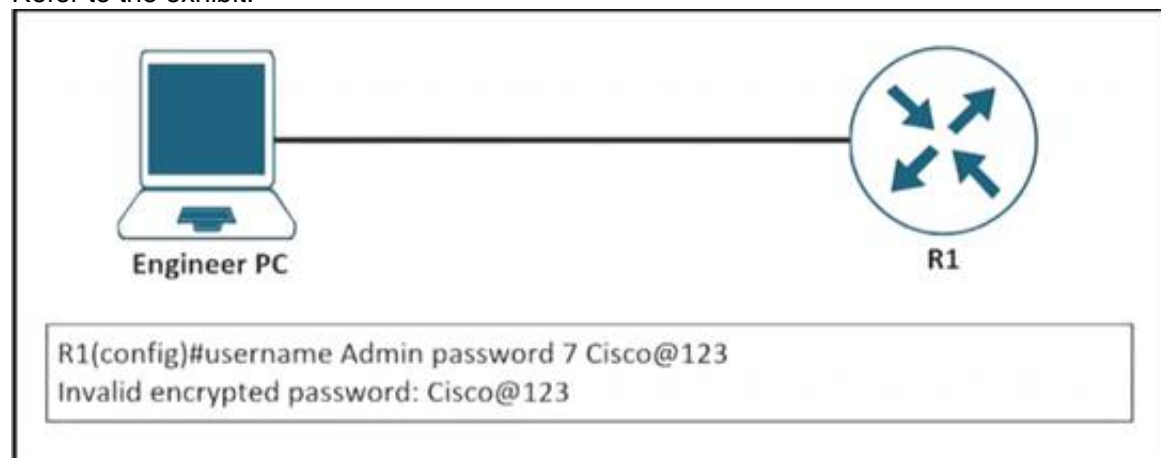
And we only policing the PIR traffic so that the route processor is not overwhelmed by BGP calculation.

Note: The "set-prec-transmit" is the same as "transmit" command except it sets the IP Precedence level as well. The "set-clp-transmit" sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet.

### NEW QUESTION 337

- (Exam Topic 3)

Refer to the exhibit.



An engineer is trying to add an encrypted user password that should not be visible in the router configuration. Which two configuration commands resolve the issue? (Choose two)

- A. password encryption aes
- B. username Admin password Cisco@maedeh motamedi
- C. username Admin password 5 Cisco@maedeh motamedi
- D. username Admin secret Cisco@maedeh motamedi
- E. no service password-encryption
- F. service password-encryption

**Answer:** DF

### NEW QUESTION 340

- (Exam Topic 3)

The network administrator configured the router for Control Plane Policing so that inbound SSH traffic is policed to 500 kbps. This policy must apply to traffic coming in from 10.10.10.0/24 and 192.168.10.0/24 networks.

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 any
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 23
!
class-map CLASS-SSH
match access-group 100
!
policy-map PM-COPP
class CLASS-SSH
police 500000 conform-action transmit
!
interface E0/0
service-policy input PM-COPP
!
interface E0/1
service-policy input PM-COPP
```

The Control Plane Policing is not applied to SSH traffic and SSH is open to use any bandwidth available. Which configuration resolves this issue?

- ☐ no access-list 100  
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22  
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22  
!  
policy-map PM-COPP  
class CLASS-SSH  
no police 500000 conform-action transmit  
police 500000 conform-action transmit exceed-action drop
- ☐ interface E0/0  
no service-policy input PM-COPP  
!  
interface E0/1  
no service-policy input PM-COPP  
!  
control-plane  
service-policy input PM-COPP
- ☒ no access-list 100  
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22  
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22  
!  
interface E0/0  
no service-policy input PM-COPP  
!  
interface E0/1  
no service-policy input PM-COPP  
!  
control-plane  
service-policy input PM-COPP
- ☐ no access-list 100  
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22  
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22

A)

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
!
policy-map PM-COPP
class CLASS-SSH
no police 500000 conform-action transmit
police 500000 conform-action transmit exceed-action drop
```

B)

```
interface E0/0
no service-policy input PM-COPP
!
interface E0/1
no service-policy input PM-COPP
!
control-plane
service-policy input PM-COPP
```

C)

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
!
interface E0/0
no service-policy input PM-COPP
!
interface E0/1
no service-policy input PM-COPP
!
control-plane
service-policy input PM-COPP
```

D)

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
```

- A. Option
- B. Option
- C. Option

D. Option

**Answer:** C

#### NEW QUESTION 345

- (Exam Topic 3)

Refer to the exhibit.

A network engineer receives a fault ticket about traffic drops from BANK SITE to BANK Users can reach BANK SITE Y from router RA as a source. Routers RB and RD are acting as route reflectors. Which configuration resolves the issue?

- A. RC(config)#router bgp 65201RC(config-router)#neighbor 10.10.10.4 route-reflector-client
- B. RF(config)#router bgp 65201RF(config-router)#neighbor 10.10.10.6 route-reflector-client
- C. RC(config)#router bgp 65201RC(config-router)#neighbor 10.10.10.2 route-reflector-client
- D. RB(config)#router bgp 65201RB(config-router)#neighbor 10.10.10.3 route-reflector-client

**Answer:** A

#### NEW QUESTION 350

- (Exam Topic 3)

An engineer creates a Cisco DNA Center cluster with three nodes, but all the services are running on one host node. Which action resolves this issue?

- A. Restore the link on the switch interface that is connected to a cluster link on the Cisco DNA Center
- B. Click the master host node with all the services and select services to be moved to other hosts
- C. Enable service distribution from the Systems 360 page.
- D. Click system updates, and upgrade to the latest version of Cisco DNA Center.

**Answer:** C

#### Explanation:

To deploy Cisco DNA Center on a three-node cluster with High Availability (HA) enabled, complete the following procedure:

Step 1: Configure Cisco DNA Center on the first node in your cluster...

Step 2: Configure Cisco DNA Center on the second node in your cluster... Step 3: Configure Cisco DNA Center on the third node in your cluster... Step 4: Enable high availability on your cluster:

\* a. In the Cisco DNA Center GUI, click and choose System Settings. The System 360 tab is displayed by default.

\* b. In the Hosts area, click Enable Service Distribution.

After you click Enable Service Distribution, Cisco DNA Center enters into maintenance mode. In this mode, Cisco DNA Center is unavailable until the redistribution of services is completed. You should take this into account when scheduling an HA deployment.

Reference: [https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automationand-management/dna-center/1-3-3-0/ha\\_guide/b\\_cisco\\_dna\\_center\\_ha\\_guide\\_1\\_3\\_3\\_0.html](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automationand-management/dna-center/1-3-3-0/ha_guide/b_cisco_dna_center_ha_guide_1_3_3_0.html)

Therefore we can choose "Enable Service Distribution" to distribute services to other host nodes.

#### NEW QUESTION 355

- (Exam Topic 3)

What is an MPLS LDP targeted session?

- A. session between neighbors that are connected no more than one hop away
- B. LDP session established between LSRs by exchanging TCP hello packets
- C. label distribution session between non-directly connected neighbors
- D. LDP session established by exchanging multicast hello packets

**Answer:** C

#### NEW QUESTION 360

- (Exam Topic 3)

Refer to the exhibit.



```

ipv6 inspect udp idle-time 3600
ipv6 inspect name ipv6-firewall tcp
ipv6 inspect name ipv6-firewall udp
!

ipv6 access-list ipv6-internet
deny ipv6 any FEC0::/10
deny ipv6 any FF00::/8
permit ipv6 any FF02::/16
permit ipv6 any FF0E::/16
permit udp any any eq domain log
!

Interface gi0/1
ipv6 traffic-filter ipv6-internet in
ipv6 inspect ipv6-firewall in
ipv6 inspect ipv6-firewall out

```

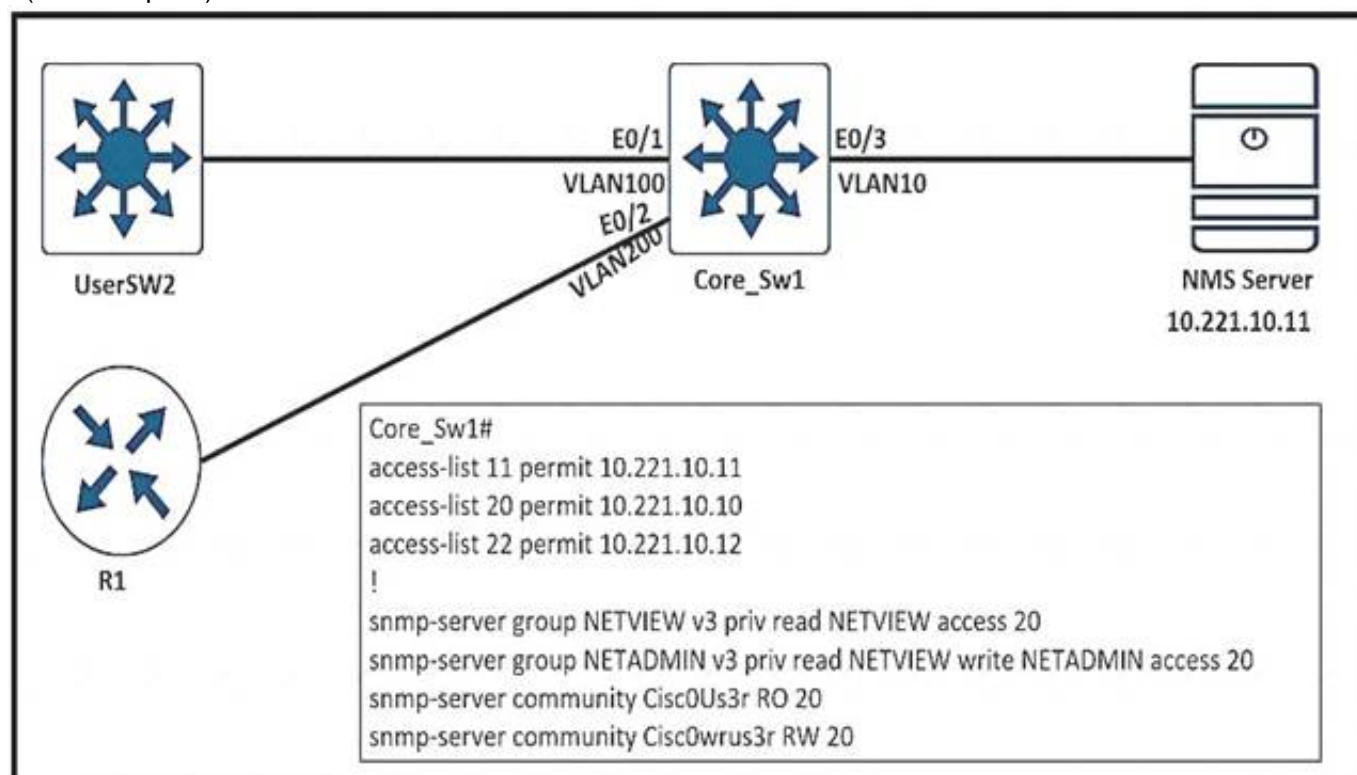
A network administrator configured name resolution for IPv6 traffic to be allowed through an inbound access list. After the access list is applied to resolve the issue, name resolution still did not work. Which action does the network administrator take to resolve the name resolution problem?

- A. Remove `ipv6 inspect ipv6-firewall in` from interface `gi0/1`
- B. Add `permit udp any eq domain any log` in the access list.
- C. `inspect ipv6 inspect name ipv6-firewall udp 53` in global config.
- D. Add `permit any eq domain 53 any log` in the access list.

**Answer:** A

#### NEW QUESTION 362

- (Exam Topic 3)



- A. `access-list 20 permit 10.221.10.12`
- B. `snmp-server group NETVIEW v2c priv read NETVIEW access 20`
- C. `snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22`
- D. `access-list 20 permit 10.221.10.11`

**Answer:** D

#### NEW QUESTION 367

- (Exam Topic 3)

What is the purpose of the DHCPv6 Guard?

- A. It messages between a DHCPv6 server and a DHCPv6 client ( or relay agent).
- B. It shows that clients of a DHCPv5 server are affected.
- C. It block DHCPv6 messages from relay agents to a DHCPv6 server.
- D. It allows DHCPv6 replay and advertisements from (rouge) DHCPv6 servers.

**Answer:** A

**Explanation:**  
[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6\\_fhsec/configuration/xe-16/ipv6xe-16-book/ip6-dhcpv6-guard.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ipv6xe-16-book/ip6-dhcpv6-guard.html)

**NEW QUESTION 372**


- (Exam Topic 3)  
Configure individual VRFs for each customer according to the topology to achieve these goals :

Comment

Guidelines

Topology

Tasks



Topology Diagram

R1R2SW1SW2SW3SW4

```
R1>
R1>
R1>
R1>
R1>
```

Guidelines

Topology

Tasks

Configure individual VRFs for each customer according to the topology to achieve these goals:

1. VRF "cu-red" has interfaces on routers R1 and R2. Both routers are preconfigured with IP addressing, VRFs, and BGP. Do not use the BGP network statement for advertisement.
2. VRF "cu-green" has interfaces on routers R1 and R2.
3. BGP on router R1 populates VRF routes between router R1 and R2.
4. BGP on router R2 populates VRF routes between router R1 and R2.
5. LAN to LAN is reachable between SW1 and SW3 for VRF "cu-red" and between SW2 and SW4 for VRF "cu-green". All switches are preconfigured.

R1R2SW1SW2SW3SW4

```
R1>
R1>
R1>
R1>
R1>
```

R1

<https://www.exambible.com/300-410-exam/> (530 Q&As)

```
R1 R2 SW1 SW2 SW3 SW4
!
!
!
!
!
ip vrf cu-green
  rd 65000:200
!
ip vrf cu-red
  rd 65000:100
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
```



R1	R2	SW1	SW2	SW3	SW4
----	----	-----	-----	-----	-----

R2

```
R1 R2 SW1 SW2 SW3 SW4  
!  
!  
!  
!  
!  
!  
!  
  
!  
ip vrf cu-green  
rd 65000:200  
!  
ip vrf cu-red  
rd 65000:100  
!  
!  
!  
no ip domain lookup  
ip cef  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!
```

```
interface Ethernet0/2.200
  encapsulation dot1Q 200
  ip address 10.10.20.2 255.255.255.252
!
interface Ethernet0/3
  no ip address
  shutdown
  duplex auto
!
router bgp 65000
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
```



```

R1  R2  SW1  SW2  SW3  SW4
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.2 255.255.255.252
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!

```

SW1

```

R1  R2  SW1  SW2  SW3  SW4
SW1>en
SW1#sh run
Building configuration...

Current configuration : 942 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!

```

```

R1    R2    SW1    SW2    SW3    SW4
!
no switchport
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.2.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
!
!
control-plane
!
```

SW2

```
R1    R2    SW1    SW2    SW3    SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
no switchport
ip address 192.168.22.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
```



```

R1  R2  SW1  SW2  SW3  SW4
!
interface Ethernet0/1
  no switchport
  ip address 192.168.22.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.22.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
!
!
control-plane
!

```

SW3

```

R1  R2  SW1  SW2  SW3  SW4
SW3>
SW3>en
SW3#show run
Building configuration...

Current configuration : 942 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0

```

```
!
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
  
interface Ethernet0/0  
no switchport  
ip address 192.168.1.1 255.255.255.0  
!  
interface Ethernet0/1  
!  
interface Ethernet0/2  
!  
interface Ethernet0/3
```

```
no switchport
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
!
!
control-plane
```

<https://www.exambible.com/300-410-exam/> (530 Q&As)

```
R1    R2    SW1    SW2    SW3    SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
no switchport
ip address 192.168.20.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
```





Guidelines      Topology

Configure individual VRFs for each customer according to the topology to achieve these goals:

1. VRF "cu-red" has interfaces on routers R1 and R2. Both routers are preconfigured with IP addressing, VRFs, and BGP. Do not use the BGP network statement for advertisement.
2. VRF "cu-green" has interfaces on routers R1 and R2.
3. BGP on router R1 populates VRF routes between router R1 and R2.
4. BGP on router R2 populates VRF routes between router R1 and R2.
5. LAN to LAN is reachable between SW1 and SW3 for VRF "cu-red" and between SW2 and SW4 for VRF "cu-green". All switches are preconfigured.

A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

**Solution:**

- Use cu-red under interfaces facing SW1 & SW3:

On R1:

```
interface Ethernet0/0
```

```
ip vrf forwarding cu-red
```

ip address 192.168.1.254 255.255.255.0

Check reachability to SW1: R1#ping vrf cu-red 192.168.1.1 Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

On R2:

```
interface Ethernet0/0
```

```
ip vrf forwarding cu-red
```

```
ip address 192.168.2.254 255.255.255.0
```

Check reachability to SW3: R2#ping vrf cu-red 192.168.2.1 Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!

- Use vrf cu-green for SW2 & SW4:

On R1:

```
interface Ethernet0/1
```

```
ip vrf forwarding cu-green
```

```
ip address 192.168.20.254 255.255.255.0
Test reachability to SW2: R1#ping vrf cu-green 192.168.20.1 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
On R2:
interface Ethernet0/1
ip vrf forwarding cu-green
ip address 192.168.22.254 255.255.255.0
Test reachability to SW4: R2#ping vrf cu-green 192.168.22.1 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
> On R1:
interface Ethernet0/2.100 mpls ip
!
interface Ethernet0/2.200 mpls ip
!
Configure BGP:
router bgp 65000
neighbor 10.10.10.2 remote-as 65000
neighbor 10.10.20.2 remote-as 65000
!
address-family vpnv4 neighbor 10.10.10.2 activate
neighbor 10.10.20.2 activate exit-address-family
!
address-family ipv4 vrf cu-green redistribute connected
exit-address-family
!
address-family ipv4 vrf cu-red redistribute connected
exit-address-family
!
R1(config)#ip vrf cu-red
R1(config-vrf)#route-target both 65000:100
!
R1(config)#ip vrf cu-green
R1(config-vrf)#route-target both 65000:200
> On R2:
interface Ethernet0/2.100
mpls ip
!
interface Ethernet0/2.200 mpls ip
!
router bgp 65000
neighbor 10.10.10.1 remote-as 65000
neighbor 10.10.20.1 remote-as 65000
!
address-family vpnv4 neighbor 10.10.10.1 activate
neighbor 10.10.20.1 activate exit-address-family
!
address-family ipv4 vrf cu-green redistribute connected
exit-address-family
!
address-family ipv4 vrf cu-red redistribute connected
exit-address-family R2(config)#ip vrf cu-red
R2(config-vrf)#route-target both 65000:100
!
R2(config)#ip vrf cu-green
R2(config-vrf)#route-target both 65000:200
> Verification:
From SW1 to SW3: SW1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
But can't Reach SW2 or SW4 in VRF cu-green: SW1#ping 192.168.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
SW1#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
Same Test for SW2: From SW2 to SW4: SW2#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
But can't Reach SW3 or SW1 in VRF cu-red: SW2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
```

SW2#ping 192.168.2.1  
 Type escape sequence to abort.  
 Sending 5, 100-byte ICMP Echoes to 192.168.2.1, timeout is 2 seconds: U.U.U  
 Success rate is 0 percent (0/5)  
 Both R1 & R2 has separate tables for VRFs cu-red and cu-green.

#### NEW QUESTION 374

- (Exam Topic 3)

```
CPE# show ip route static
<output omitted>
S* 0.0.0.0/0 is directly connected, Dialer0
S 198.51.100.0/24 [1/0] via 192.168.1.1
S 203.0.113.0/24 [1/0] via 192.168.2.1

CPE# show run | section router ospf
router ospf 1
 redistribute static subnets

CPE# show ip ospf database | begin Type-5
Type-5 AS External Link States

Link ID      ADV Router   Age         Seq#         Checksum Tag
198.51.100.0 192.168.0.1  14          0x80000001  0x0007D0 0
203.0.113.0  192.168.0.1  14          0x80000001  0x009C5C 0
```

Refer to the exhibit. The default route is not advertised to the neighboring router. Which action resolves the issue?

- A. Configure the redistribute static metric 200 subnets command under OSPF.
- B. Configure OSPF on the Dialer0 interface.
- C. Configure the network 0.0.0.0 255.255.255.255 area 0 command under OSPF.
- D. Configure the default-information originate command under OSPF.

**Answer: D**

#### NEW QUESTION 377

- (Exam Topic 3)

Refer to the exhibit.

```
R2#sh ip route
Codes: 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
       i - IS-IS, su - IS-IS summary, 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

C 192.168.10.0/24 is directly connected, Serial1/0
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C   172.16.160.0/19 is directly connected, Loopback1
C   172.16.128.0/19 is directly connected, Loopback0
C   172.16.224.0/19 is directly connected, Loopback3
C   172.16.192.0/19 is directly connected, Loopback2
D   172.16.0.0/16 is a summary, 00:01:27, Null0
```

An engineer must configure EIGRP between R1 and R2 with no summary route. Which configuration resolves the issue?

A)

```
R1(config)#router eigrp 1
R1(config-router)#no auto-summary
```

B)

```
R2 (config)#router eigrp 1
R2 (config-router)#no auto-summary
```



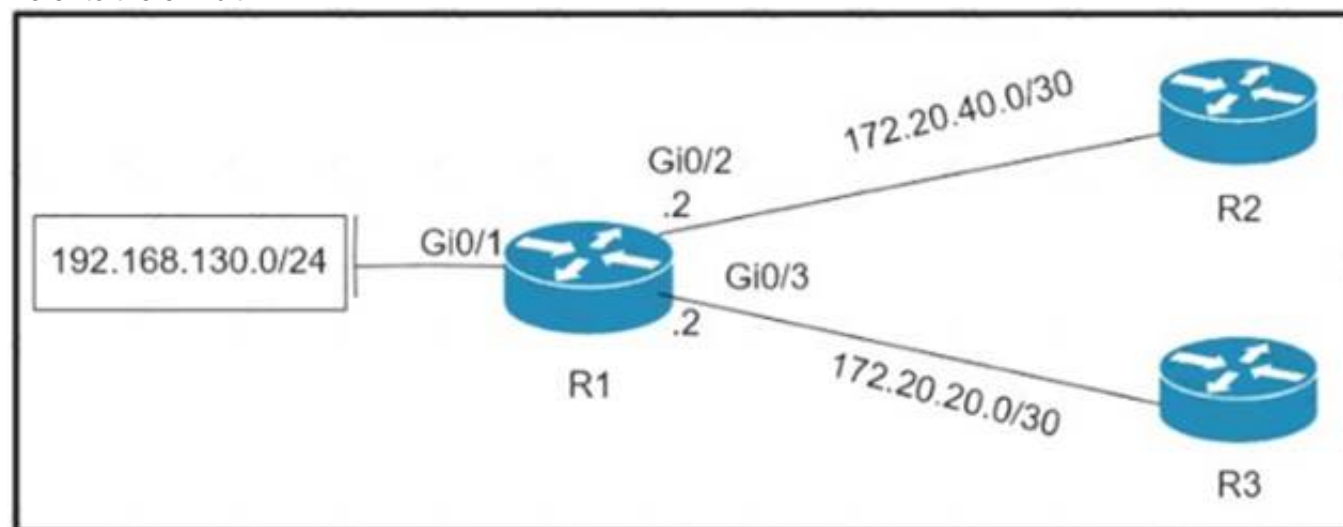
```
R2 (config)#router eigrp 1
R2 (config-router)#auto-summary
```

```
R1(config)#router eigrp 1
R1(config-router)#auto-summary
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

NEW QUESTION 380

Refer to the exhibit.



A)

```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.1
```

```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.1
```

```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.2
```

D)

```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.2
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

#### NEW QUESTION 383

- (Exam Topic 3)

Refer to the exhibit.

```
R1(config)#ip prefix-list EIGRP seq 10 deny 0.0.0.0/0 le 32
R1(config)#ip prefix-list EIGRP seq 20 permit 10.0.0.0/8
R1(config)#router eigrp 10
R1(config-router)#distribute-list prefix EIGRP in Ethernet0/0

R1#show ip route eigrp
```

A prefix list is created to filter routes inbound to an EIGRP process except for network 10 prefixes After the prefix list is applied no network 10 prefixes are visible in the routing table from EIGRP. Which configuration resolves the issue?

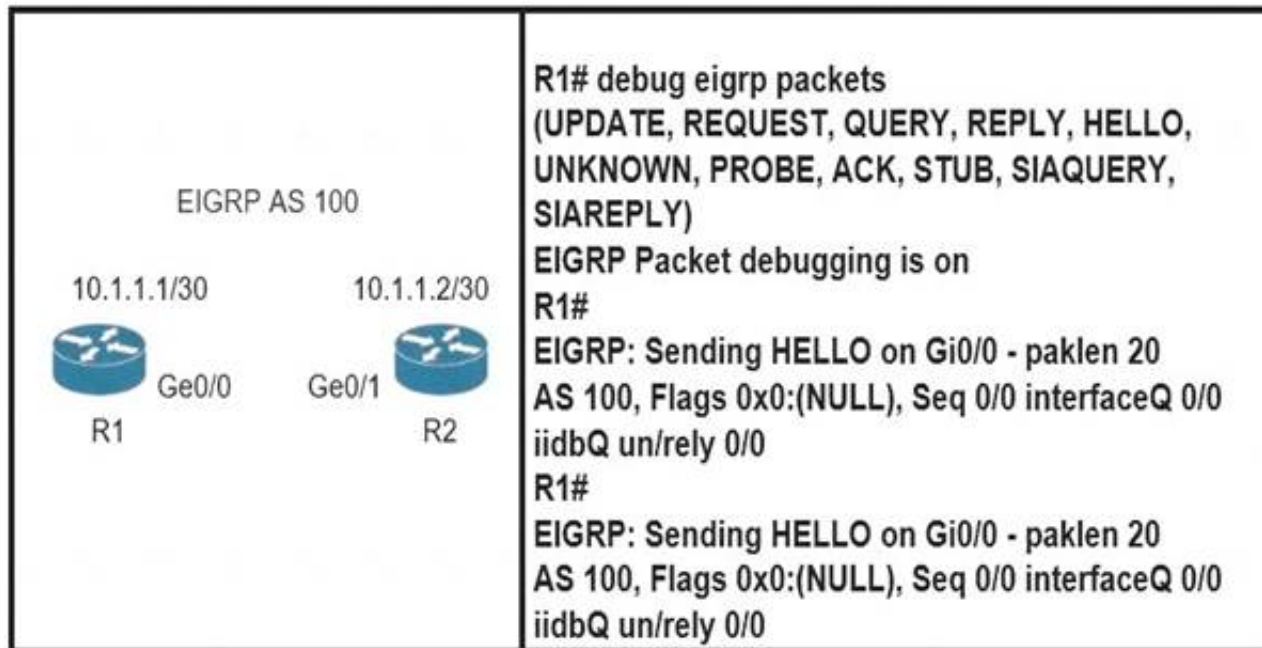
- A. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9.
- B. ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
- C. ip prefix-list EIGRP seq 5 permit 10.0.0.0/8 ge 9 no ip prefix-list EIGRP seq 20 permit 10.0.0.0/8
- D. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9 ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32

**Answer: C**

#### NEW QUESTION 388

- (Exam Topic 2)

Refer to the exhibit.



Which action resolves the adjacency issue?

- A. Match the hello interval timers.
- B. Configure the same EIGRP process IDs.
- C. Match the authentication keys.
- D. Configure the same autonomous system numbers.

**Answer: D**

#### Explanation:

EIGRP does not have process ID as it uses Autonomous System (AS) numbers only. This is not an authentication problem or we would see this error from the debug:

EIGRP: Ethernet0/0: ignored packet from 10.1.1.3, opcode = 1 (missing authentication or key-chain missing) If the AS numbers between two routers are different then the neighbor relationship cannot be formed.

#### NEW QUESTION 391

- (Exam Topic 3)

```
R1#show ip rip database
10.0.0.0/8  auto-summary
10.1.1.0/24  directly connected, GigabitEthernet0/0
10.1.3.0/24
    [2] via 10.1.12.2, 00:00:03, GigabitEthernet1/0
10.1.12.0/24  directly connected, GigabitEthernet1/0
10.1.23.0/24
    [1] via 10.1.12.2, 00:00:03, GigabitEthernet1/0
```

Refer to the exhibit. A customer reports that networks in the 10.0.1.0/24 space do not appear in the RIP database. What action resolves the issue?

- A. Remove summarization of 10.0.0.0/8.
- B. Permit 10.0.1.0/24 address in the ACL.
- C. Remove ACL on R1 blocking 10.0.1.0/24 network.
- D. Configure 10.0.1.0/24 network under RIP.

**Answer:** A

#### NEW QUESTION 394

- (Exam Topic 3)

A customer is running an mGRE DMVPN tunnel over WAN infrastructure between hub and spoke sites. The existing configuration allows NHRP to add spoke routers automatically to the multicast NHRP mappings. The customer is migrating the network from IPv4 to the IPv6 addressing scheme for those spokes' routers that support IPv6 and can run DMVPN tunnel over the IPv6 network. Which configuration must be applied to support IPv4 and IPv6 DMVPN tunnel on spoke routers?

- A. Tunnel mode ipv6ip 6to4
- B. Tunnel mode ipv6ip isatap
- C. Tunnel mode ipv6ip auto-tunnel
- D. Tunnel mode ipv6ip 6rd

**Answer:** C

#### NEW QUESTION 398

- (Exam Topic 2)

```
ip prefix-list DefaultRouteOnly seq 5 deny 0.0.0.0/0 le 32
ip prefix-list DefaultRouteOnly seq 10 permit 0.0.0.0/0

router eigrp ccnp
 address-family ipv4 unicast autonomous-system 1
  topology base
  distribute-list prefix DefaultRouteOnly out Tunnel0
```

Refer to the exhibit. The administrator configured route advertisement to a remote low resources router to use only the default route to reach any network but failed. Which action resolves this issue?

- A. Change the direction of the distribute-list command from out to in.
- B. Remove the line with the sequence number 5 from the prefix list.
- C. Remove the prefix keyword from the distribute-list command.
- D. Remove the line with the sequence number 10 from the prefix list.

**Answer:** B

#### NEW QUESTION 403

- (Exam Topic 2)

Refer to the exhibit.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
time-range Office-hour
periodic weekdays 08:00 to 17:00
!
access-list 101 permit tcp 10.0.0.0 0.0.0.0 172.16.1.0 0.0.0.255 eq ssh time-range Office-hour
```



An IT staff member comes into the office during normal office hours and cannot access devices through SSH Which action should be taken to resolve this issue?

- A. Modify the access list to use the correct IP address.
- B. Configure the correct time range.
- C. Modify the access list to correct the subnet mask
- D. Configure the access list in the outbound direction.

Answer: A

Explanation:

To ACL should be permit tcp 101 10.1.1.1 0.0.0.0

NEW QUESTION 404

- (Exam Topic 2)

Drag and drop the MPLS concepts from the left onto the descriptions on the right.

label edge router	allows an LSR to remove the label before forwarding the packet
label switch router	accepts unlabeled packets and imposes labels
forwarding equivalence class	group of packets that are forwarded in the same manner
penultimate hop popping	receives labeled packets and swaps labels

- A. Mastered
- B. Not Mastered

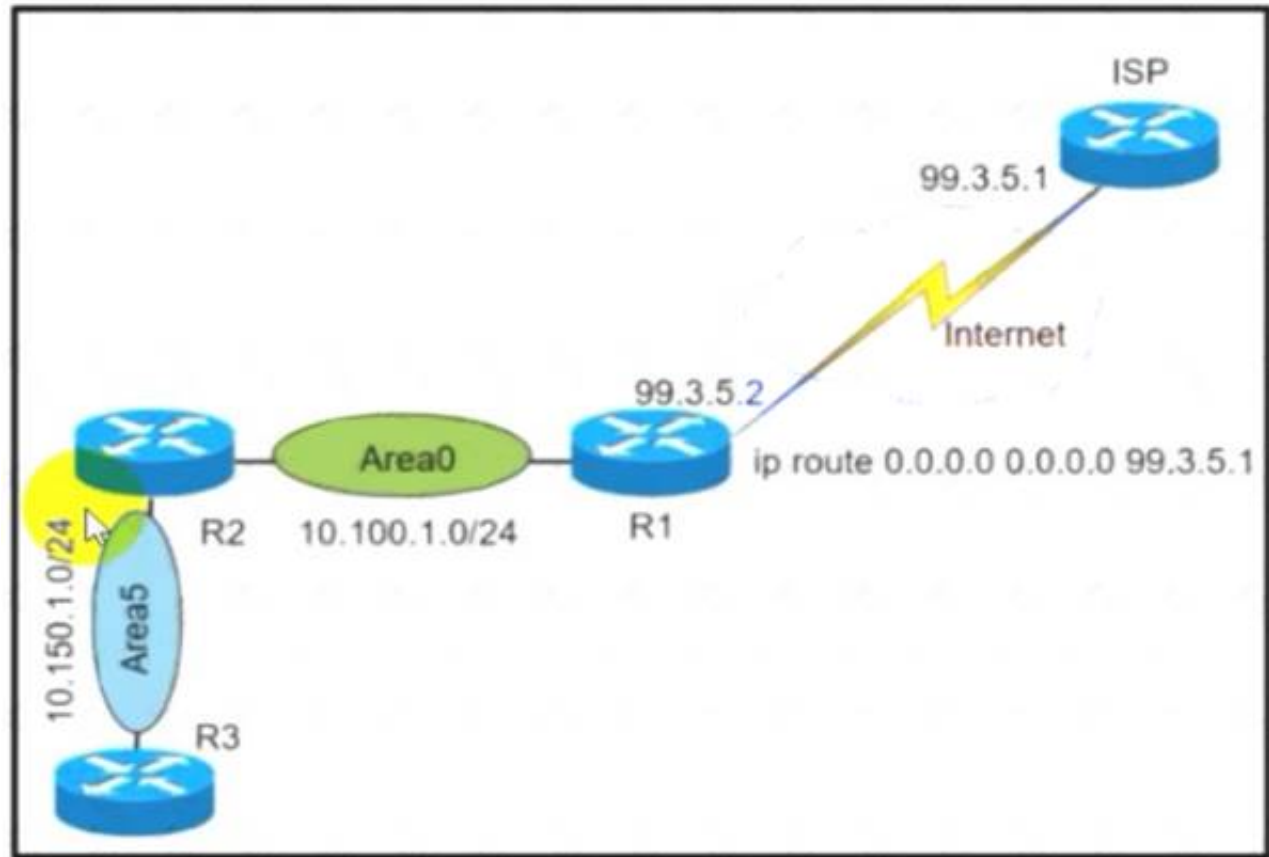
Answer: A

Explanation:

A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERpush an MPLS label onto an incoming packet and pop it off an outgoing packet.  
A forwarding equivalence class (FEC) is a term

NEW QUESTION 405

- (Exam Topic 2)



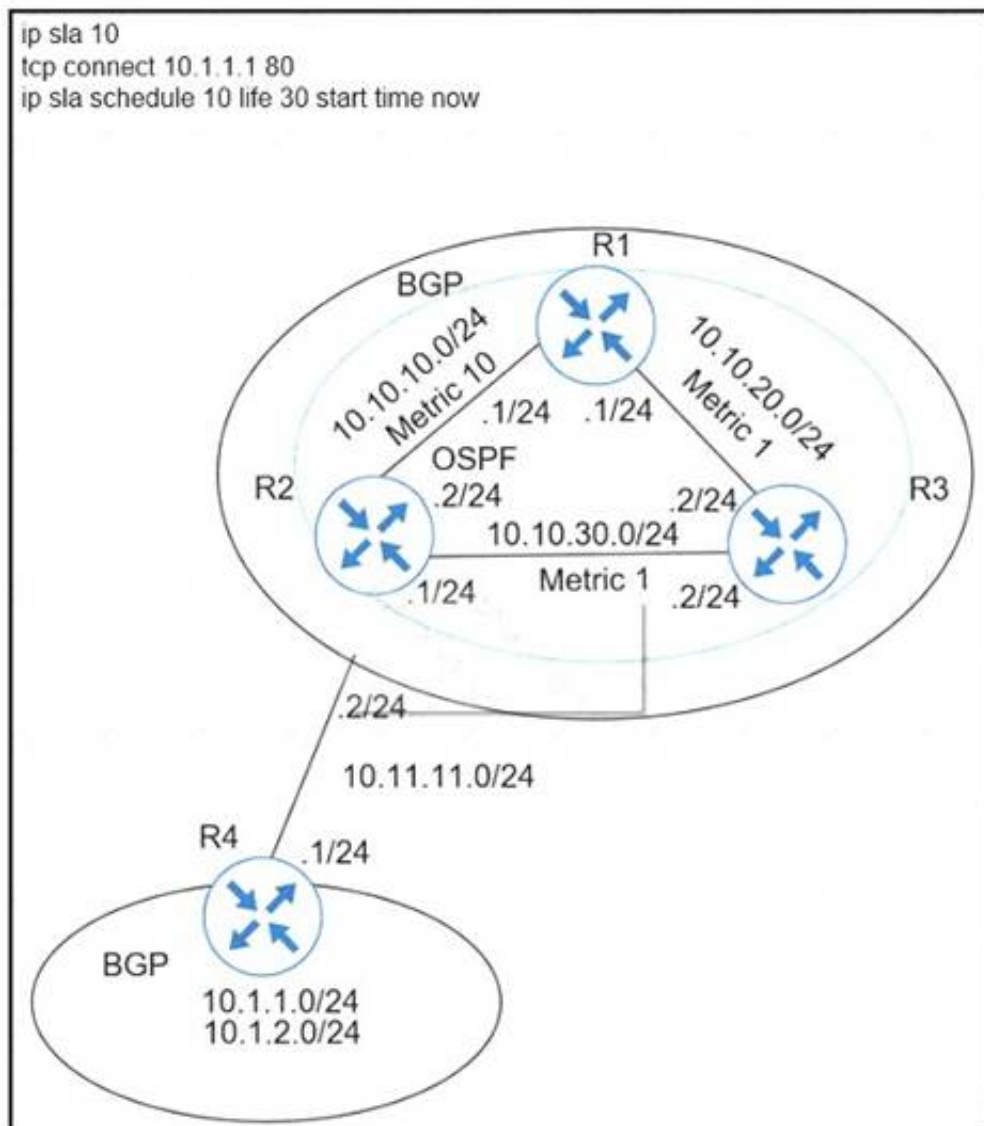
Refer to the exhibit. A network administrator redistributed the default static route into OSPF toward all internal routers to reach to Internet. Which set of commands restores reachability to the Internet by internal routers?

- A. router ospf 1default-information originate
- B. router ospf 1network 0.0.0.0 0.0.0.0 area 0
- C. router ospf 1redistribute connected 0.0.0.0
- D. router ospf 1redistribute static subnets

Answer: A

NEW QUESTION 406

- (Exam Topic 2)  
Refer to the exhibit.



A user has set up an IP SLA probe to test if a non-SLA host web server on IP address 10.1.1.1 accepts HTTP sessions prior to deployment. The probe is failing. Which action should the network administrator recommend for the probe to succeed?

- A. Re-issue the ip sla schedule command.
- B. Add icmp-echo command for the host.
- C. Add the control disable option to the tcp connect.
- D. Modify the ip sla schedule frequency to forever.

**Answer: C**

#### NEW QUESTION 409

- (Exam Topic 2)  
Refer to the exhibit.

```

MASS-RTR#show running-config
!
hostname MASS-RTR
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization commands 15 default local
!
username admin privilege 15 password 7 0236244818115F3348
username cisco privilege 15 password 7 0607072C494A5B
archive
 log config
  logging enable
  logging size 1000
!
interface GigabitEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
line vty 0 4
!

MASS-RTR#show archive log config all
idx  sess  user@line  Logged command
  1    1    console@console |interface GigabitEthernet0/0
  2    1    console@console | no shutdown
  3    1    console@console | ip address dhcp
  4    2    admin@vty0    |username cisco privilege 15 password cisco
  5    2    admin@vty0    |!config: USER TABLE MODIFIED

```

A client is concerned that passwords are visible when running this show archive log config all. Which router configuration is needed to resolve this issue?

- A. MASS-RTR(config-archive-log-cfg)#password encryption aes
- B. MASS-RTR(config)#aaa authentication arap

- C. MASS-RTR(config)#service password-encryption  
D. MASS-RTR(config-archive-log-cfg)#hidekeys

**Answer: D**

**Explanation:**

Step 7 hidekeys

Example:

```
Device(config-archive-log-config)# hidekeys
```

(Optional) Suppresses the display of password information in configuration log files.

**Note** Enabling the **hidekeys** command increases security by preventing password information from being displayed in configuration log files.

**NEW QUESTION 411**

- (Exam Topic 2)  
Refer to the exhibit.

```
Router# show ip route

      2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Ethernet0/0
C       3.0.0.0/8 is directly connected, Serial1/0
O E2 200.1.1.0/24 [110/20] via 2.2.2.2, 00:16:17, Ethernet0/0
O E1 200.2.2.0/24 [110/104] via 2.2.2.2, 00:00:41, Ethernet0/0
      131.108.0.0/24 is subnetted, 2 subnets
O       131.108.2.0 [110/74] via 2.2.2.2, 00:16:17, Ethernet0/0
O IA    131.108.1.0 [110/84] via 2.2.2.2, 00:16:17, Ethernet0/0

Router# show ip bgp

      Network          Next Hop        Metric LocPrf Weight Path
*> 2.2.2.0/24         0.0.0.0              0     32768 ?
*> 131.108.1.0/24     2.2.2.2             84     32768 ?
*> 131.108.2.0/24     2.2.2.2             74     32768 ?
```

The OSPF routing protocol is redistributed into the BGP routing protocol, but not all the OSPF routes are distributed into BGP Which action resolves the issue?

- A. Include the word external in the redistribute command  
B. Use a route-map command to redistribute OSPF external routes defined in an access list  
C. Include the word internal external in the redistribute command  
D. Use a route-map command to redistribute OSPF external routes defined in a prefix list.

**Answer: C**

**Explanation:**

If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default. You can use the internal keyword along with the redistribute command under router bgp to redistribute OSPF intra- and inter-area routes.

Use the external keyword along with the redistribute command under router bgp to redistribute OSPF external routes into BGP.

-> In order to redistribute all OSPF routes into BGP, we must use both internal and external keywords. The full command would be (suppose we are using OSPF 1):

redistribute ospf 1 match internal external

Note: The configuration shows match internal external 1 external 2. This is normal because OSPF automatically appends "external 1 external 2" in the configuration. In other words, keyword external = external 1 external 2. External 1 = O E1 and External 2 = O E2. Reference:

<https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5242-bgp-ospf-redistribution.html>

**NEW QUESTION 413**

- (Exam Topic 2)  
Refer to the exhibit.

```
ipv6 access-list INTERNET
permit ipv6 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA14::/64
permit tcp 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA13::/64 eq telnet
permit tcp 2001:DB8:AD59:BA21::/64 any eq http
permit ipv6 2001:DB8:AD59::/48 any
deny ipv6 any any log
```

When monitoring an IPv6 access list, an engineer notices that the ACL does not have any hits and is causing unnecessary traffic to pass through the interface Which command must be configured to resolve the issue?

- A. access-class INTERNET in



- B. ipv6 traffic-filter INTERNET in
- C. ipv6 access-class INTERNET in
- D. ip access-group INTERNET in

**Answer:** C

#### NEW QUESTION 417

- (Exam Topic 2)

Refer to the exhibit.

```
router ospf 1
 redistribute eigrp 1 subnets route-map EIGRP->OSPF
!
router eigrp 1
 network 10.0.106.0 0.0.0.255
!
route-map EIGRP->OSPF permit 10
 match ip address WAN_PREFIXES
route-map EIGRP->OSPF permit 20
 match ip address LOCAL_PREFIXES
route-map EIGRP->OSPF permit 30
 match ip address VPN_PREFIXES
!
ip prefix-list LOCAL_PREFIXES seq 5 permit 172.16.0.0/12 le 24
ip prefix-list VPN_PREFIXES seq 5 permit 192.168.0.0/16 le 24
ip prefix-list WAN_PREFIXES seq 5 permit 10.0.0.0/8 le 24
!
```

The network administrator configured redistribution on an ASBR to reach to all WAN networks but failed Which action resolves the issue?

- A. The route map must have the keyword prefix-list to evaluate the prefix list entries
- B. The OSPF process must have a metric when redistributing prefixes from EIGRP.
- C. The route map EIGRP->OSPF must have the 10.0.106.0/24 entry to exist in one of the three prefix lists to pass
- D. EIGRP must redistribute the 10.0.106.0/24 route instead of using the network statement

**Answer:** A

#### Explanation:

In order to use a prefix-list in a route-map, we must use the keyword "prefix-list" in the "match" statement. . For example:

match ip address prefix-list WAN\_PREFIXES

Without this keyword, the router will try to find an access-list with the same name instead.

#### NEW QUESTION 421

- (Exam Topic 2)

Refer to the exhibit.

```
L 172.1.12.3/32 is directly connected, Ethernet0/0
C 172.1.13.0/24 is directly connected, Ethernet0/1
L 172.1.13.3/32 is directly connected, Ethernet0/1
O 192.168.1.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O 192.168.2.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O 192.168.3.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
O 192.168.4.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
 192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.5.0/24 is directly connected, Loopback0
L 192.168.5.1/32 is directly connected, Loopback0
 192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.6.0/24 is directly connected, Loopback1
L 192.168.6.1/32 is directly connected, Loopback1
```

SanFrancisco and Boston routers are choosing slower links to reach each other despite the direct links being up Which configuration fixes the issue?

- ☐ Boston Router
- `router ospf 1`  
`auto-cost reference-bandwidth 1000`
- ☐ SanFrancisco Router
- `router ospf 1`  
`auto-cost reference-bandwidth 1000`
- ☐ All Routers
- `router ospf 1`  
`auto-cost reference-bandwidth 100`
- ☐ All Routers
- `router ospf 1`  
`auto-cost reference-bandwidth 1000`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 426

- (Exam Topic 2)

When configuring Control Plane Policing on a router to protect it from malicious traffic, an engineer observes that the configured routing protocols start flapping on that device. Which action in the Control Plane Policy prevents this problem in a production environment while achieving the security objective?

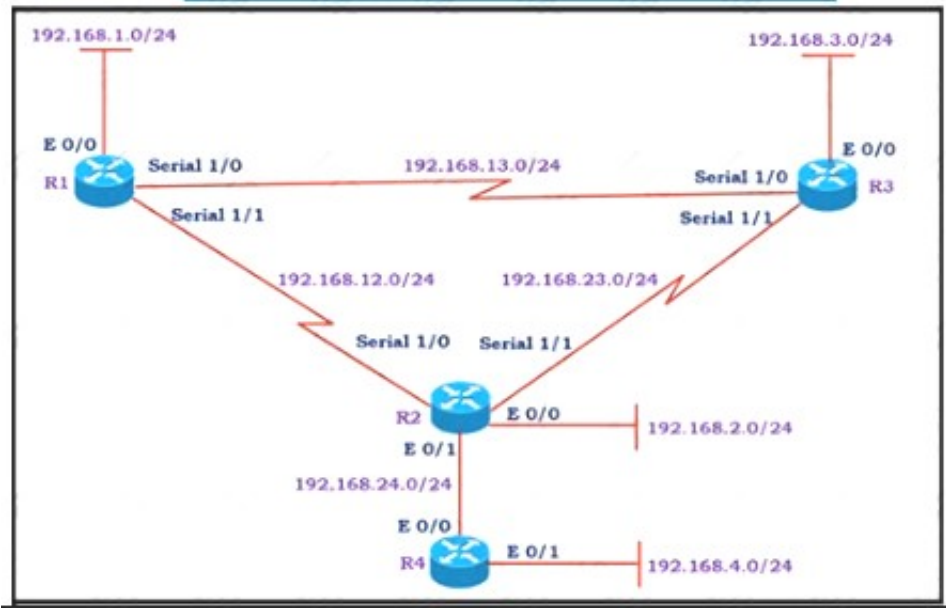
- A. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit rates and apply the Control Plane Policy in the output direction
- B. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit rates and apply the Control Plane Policy in the input direction
- C. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy m the input direction
- D. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy m the output direction

Answer: B

NEW QUESTION 429

- (Exam Topic 2)

Refer to the exhibit.



#### # Show IP route on R1

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, Ethernet0/0
L    192.168.1.1/32 is directly connected, Ethernet0/0
D    192.168.2.0/24 [90/2297856] via 192.168.12.2, 00:02:14, Serial1/1
S    192.168.3.0/24 [1/0] via 192.168.12.2
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/24 is directly connected, Serial1/1
L    192.168.12.1/32 is directly connected, Serial1/1
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/24 is directly connected, Serial1/0
L    192.168.13.1/32 is directly connected, Serial1/0
D    192.168.23.0/24 [90/2681856] via 192.168.13.3, 00:06:38, Serial1/0
    [90/2681856] via 192.168.12.2, 00:06:38, Serial1/1
```

All the serial between R1, R2, and R3 have the Same bandwidth. User on the 192.168.1.0/24 network report slow response times while they access resource on network 192.168.3.0/24. When a traceroute is run on the path. It shows that the packet is getting forwarded via R2 to R3 although the link between R1 and R3 is still up. What must the network administrator to fix the slowness?

- A. Change the Administrative Distance of EIGRP to 5.
- B. Add a static route on R1 using the next hop of R3.
- C. Remove the static route on R1.
- D. Redistribute the R1 route to EIGRP

**Answer: C**

#### NEW QUESTION 432

- (Exam Topic 2)

Exhibit:

```
11:27:07.532: AAA/BIND (00000055): Bind i/
11:27:07.532: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
11:27:07.532: TPLUS: Queuing AAA Authentication request 85 for processing
11:27:07.532: TPLUS (00000055) login timer started 1020 sec timeout
11:27:07.532: TPLUS: processing authentication start request id 85
11:27:07.532: TPLUS: Authentication start packet created for 85()
11:27:07.532: TPLUS: Using server 10.106.60.182
11:27:07.532: TPLUS (00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
11:27:07.532: TPLUS (00000055)/0/NB_WAIT: socket event 2
11:27:07.532: TPLUS (00000055)/0/NB_WAIT: wrote entire 38 bytes request
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: Would block while reading
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
13:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: read entire 18 bytes response
11:27:07.532: TPLUS (00000055)/0/225FE2DC: Processing the reply packet
11:27:07.532: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
11:27:07.532: TPLUS: Invalid AUTHEN packet (check keys).
```

Which action resolves the authentication problem?

- A. Configure the user name on the TACACS+ server
- B. Configure the UDP port 1812 to be allowed on the TACACS+ server
- C. Configure the TCP port 49 to be reachable by the router
- D. Configure the same password between the TACACS+ server and router.

**Answer: D**

#### Explanation:

From the last line of the output, we notice that the result was "Invalid AUTHEN packet". Therefore something went wrong with the username or password.

Reference:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-taca>

#### NEW QUESTION 434

- (Exam Topic 2)

Drag and drop the MPLS VPN device types from the left onto the definitions on the right.



Customer (C) device	device in the core of the provider network that switches MPLS packets
CE device	device that attaches and detaches the VPN labels to the packets in the provider network
PE device	device in the enterprise network that connects to other customer devices
Provider (P) device	device at the edge of the enterprise network that connects to the SP network

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 435

- (Exam Topic 2)  
Refer to the exhibit.

```
R1
ip prefix-list ccnp1 seq 5 permit 10.1.48.0/24 le 24
ip prefix-list ccnp2 seq 5 permit 10.1.80.0/24 le 32
ip prefix-list ccnp3 seq 5 permit 10.1.64.0/24 le 24

route-map ospf-to-eigrp permit 10
  match ip address prefix-list ccnp1
  set tag 30
route-map ospf-to-eigrp permit 20
  match ip address prefix-list ccnp2
  set tag 20
route-map ospf-to-eigrp permit 30
  match ip address prefix-list ccnp3
  set tag 10
```

An engineer wanted to set a tag of 30 to route 10.1.80.65/32 but it failed How is the issue fixed?

- A. Modify route-map ospf-to-eigrp permit 30 and match prefix-list ccnp2.
- B. Modify route-map ospf-to-eigrp permit 10 and match prefix-list ccnp2.
- C. Modify prefix-list ccnp3 to add 10.1.64.0/20 le 24
- D. Modify prefix-list ccnp3 to add 10.1.64.0/20 ge 32

Answer: B

NEW QUESTION 436

- (Exam Topic 2)  
Refer to the exhibit.

```
R1#show run | begin line
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synohronous
  transport preferred telnet
  transport output none
  stopbits 0 4
line vty 0 4
  login
  transport referred telnet
  transport input none
  transport output telnet
R1#

R1#ssh -l cisco 192.168.12.2
% ssh connections not permitted from this terminal
R1#
```

An engineer receives this error message when trying to access another router in-band from the serial interface connected to the console of R1. Which configuration is needed on R1 to resolve this issue?

- ☐ R1(config)#**line console 0**  
R1(config-line)# **transport preferred ssh**
- ☐ R1(config)#**line vty 0**  
R1(config-line)# **transport output ssh**
- ☐ R1(config)#**line vty 0**  
R1(config-line)# **transport output ssh**  
R1(config-line)# **transport preferred ssh**
- ☐ R1(config)#**line console 0**  
R1(config-line)# **transport output ssh**

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

**Explanation:**

<https://community.cisco.com/t5/other-network-architecture/out-of-band-router-access/td-p/333295> The “transport output none” command prevents any protocol connection made from R1. Therefore our SSH connection to 192.168.12.2 was refused. In order to fix this problem we can configure “transport output ssh” under “line console 0” of R1.

Note: The parameter “-l” specifies the username to log in as on the remote machine.

**NEW QUESTION 439**

- (Exam Topic 2)

Refer to the exhibit.

```
Router#show access-lists
Standard IP access list 1
  10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, deny, sequence 10
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
  network 192.168.1.1 0.0.0.0 area 0
  network 192.168.12.0 0.0.0.255 area 0
  distribute-list route-map RM-OSPF-DL in
Router#
```

Which two actions should be taken to access the server? (Choose two.)

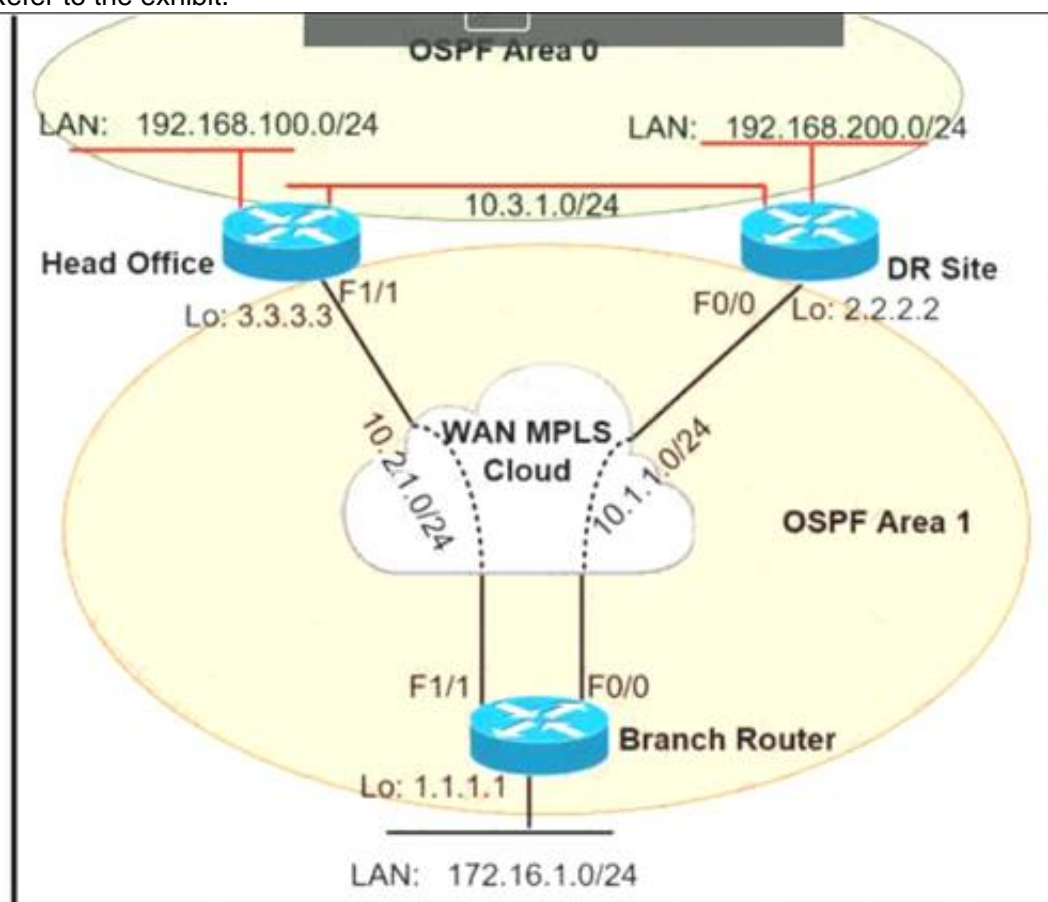
- A. Modify the access list to add a second line of permit ip any
- B. Modify the access list to deny the route to 192.168.2.2.
- C. Modify distribute list seq 10 to permit the route to 192.168.2.2.
- D. Add a sequence 20 in the route map to permit access list 1.
- E. Add a floating static route to reach to 192.168.2.2 with administrative distance higher than OSPF

**Answer:** BE

#### NEW QUESTION 444

- (Exam Topic 2)

Refer to the exhibit.



A network administrator reviews the branch router console log to troubleshoot the OSPF adjacency issue with the DR router. Which action resolves this issue?

- A. Advertise the branch WAN interface matching subnet for the DR site.
- B. Configure matching hello and dead intervals between sites.
- C. Configure the WAN interface for DR site in the related OSPF area.
- D. Stabilize the DR site flapping link to establish OSPF adjacency.

**Answer:** A

#### NEW QUESTION 447

- (Exam Topic 2)

Refer to the exhibit.



**Configuration Output:**

```
aaa new-model
!
aaa authentication login default local
aaa authentication login VTY_AUTH local
aaa authorization exec default none
aaa authorization exec VTY_AUTH local
aaa accounting exec default start-stop group radius
!

password 7 K0AyUubDrfOgO4s
authorization exec VTY_AUTH
login authentication VTY_AUTH
!
```

**Debug Output:**

```
AAA/AUTHEN/LOGIN (000004B6): Pick method list 'default'
AAA/AUTHOR (0x4B6): Pick method list 'VTY_AUTH'
AAA/AUTHOR/EXEC(000004B6): Authorization FAILED
```

Which action resolves the failed authentication attempt to the router?

- A. Configure aaa authorization login command on line vty 0 4
- B. Configure aaa authorization login command on line console 0
- C. Configure aaa authorization console global command
- D. Configure aaa authorization console command on line vty 0 4

**Answer: C**

**Explanation:**

In the debug output, we see that the Authorization (not Authentication) failed so we need to correct the authorization. In order to enable authorization, we must use the global command “aaa authorization console” first.

Reference:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-a1.html>

**NEW QUESTION 452**

- (Exam Topic 2)

What is the minimum time gap required by the local system before putting a BFD control packet on the wire?

- A. Detect Mult
- B. Required Min Echo RX Interval
- C. Desired Min TX Interval
- D. Required Min RX Interval

**Answer: C**

**Explanation:**

Desired Min TX Interval: This is the minimum interval, in microseconds, that the local system would like to use when transmitting BFD Control packets, less any jitter applied. The value zero is reserved.

Required Min Echo RX Interval: This is the minimum interval, in microseconds, between received BFD Echo packets that this system is capable of supporting, less any jitter applied by the sender. If this value is zero, the transmitting system does not support the receipt of BFD Echo packets.

Reference: <https://tools.ietf.org/html/rfc5880>

**NEW QUESTION 453**

- (Exam Topic 2)

Refer to Exhibit.

```
ip dhcp excluded-address 172.16.16.1 172.16.16.2
!
ip dhcp pool 0
network 172.16.16.0 255.255.255.0
domain-name cisco.com
dns-server 172.16.16.2
lease 30

interface Ethernet0/0
ip address 10.1.1.1 255.255.255.252
ip access-group 100 in

access-list 100 deny  udp any any
access-list 100 permit ip any any
```

Which two configurations allow clients to get dynamic ip addresses assigned?

- A. Configure access-list 100 permit udp any any eq 61 as the first line
- B. Configure access-list 100 permit udp any any eq 86 as the first line
- C. Configure access-list 100 permit udp any any eq 68 as the first line
- D. Configure access-list 100 permit udp any any eq 69 as the first line
- E. Configure access-list 100 permit udp any any eq 67 as the first line

**Answer:** CE

**Explanation:**

A DHCP server that receives a DHCPDISCOVER message may respond with a DHCPOFFER message on UDP port 68 (BootP client).

...

In the event that the DHCP server is not on the local subnet, the DHCP server will send the DHCPOFFER, as a unicast packet, on UDP port 67, back to the DHCP/BootP Relay Agent from which the DHCPDISCOVER came.

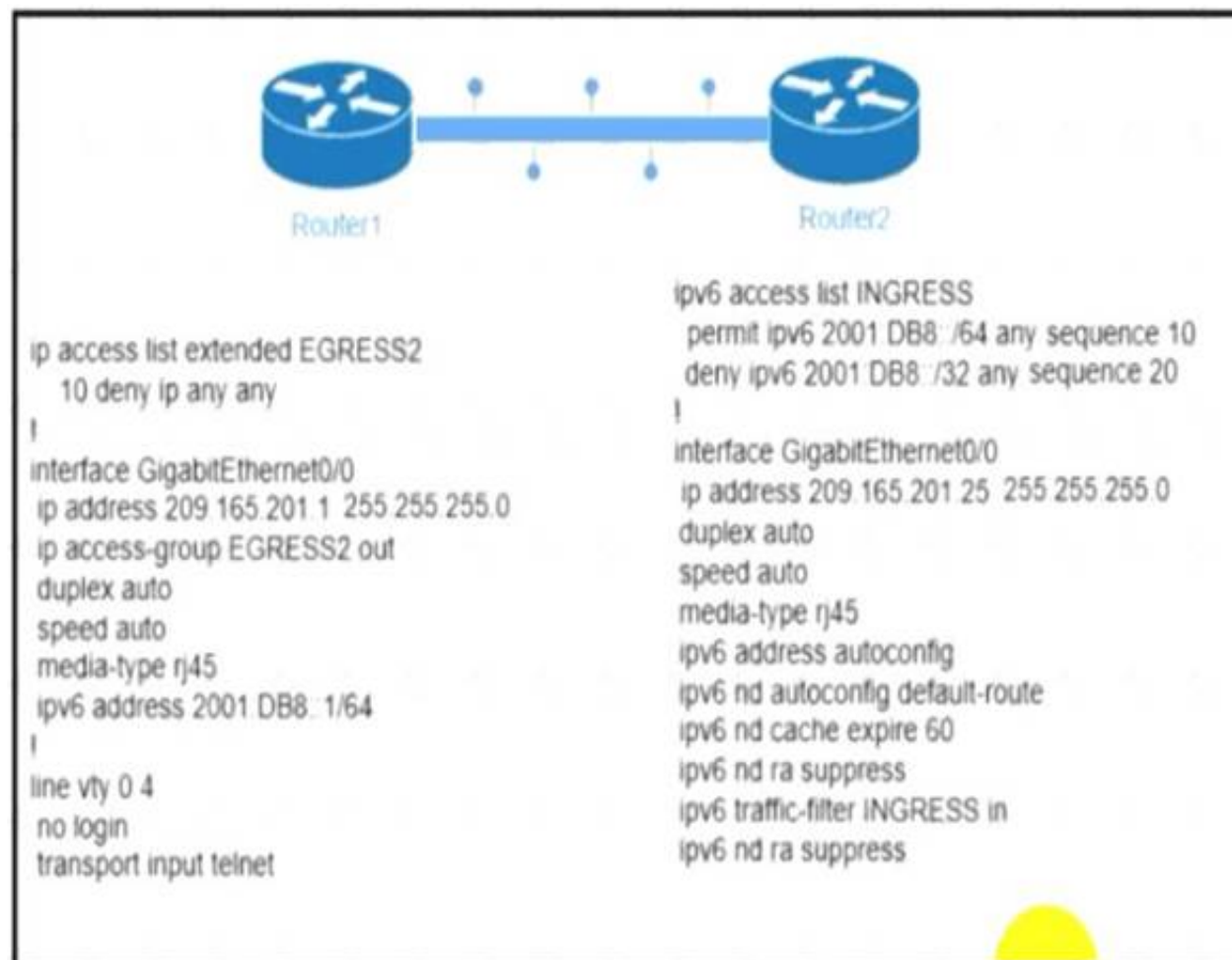
Reference:

<https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html>

**NEW QUESTION 457**

- (Exam Topic 2)

Refer to the exhibit.



The engineer configured and connected Router2 to Router1. The link came up but could not establish a Telnet connection to Router1 IPv6 address of 2001:DB8::1. Which configuration allows Router2 to establish a Telnet connection to Router1?

- A. ipv6 unicast-routing
- B. permit ICMPv6 on access list INGRESS for Router2 to obtain IPv6 address
- C. permit ip any any on access list EGRESS2 on Router1
- D. IPv6 address on GigabitEthernet0/0

**Answer:** D

**Explanation:**

```
-----R1-----
interface Ethernet0/0
ip address 209.165.201.1 255.255.255.0
ip access-group EGRESS2 out ipv6 address 2001:DB8::1/64 end
-----R2-----
interface Ethernet0/0
ip address 209.165.201.25 255.255.255.0
ipv6 address 2001:DB8::2/64 ipv6 address autoconfig
ipv6 nd autoconfig default-route ipv6 nd cache expire 60
ipv6 nd ra suppress
ipv6 traffic-filter INGRESS in end
IOU_Router2#telnet 2001:DB8::1 Trying 2001:DB8::1 ... Open IOU_Router1>
-----
```

**NEW QUESTION 458**

.....



## Relate Links

**100% Pass Your 300-410 Exam with ExamBible Prep Materials**

<https://www.exambible.com/300-410-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>