

## Exam Questions 300-410

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)

<https://www.2passeasy.com/dumps/300-410/>



## 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

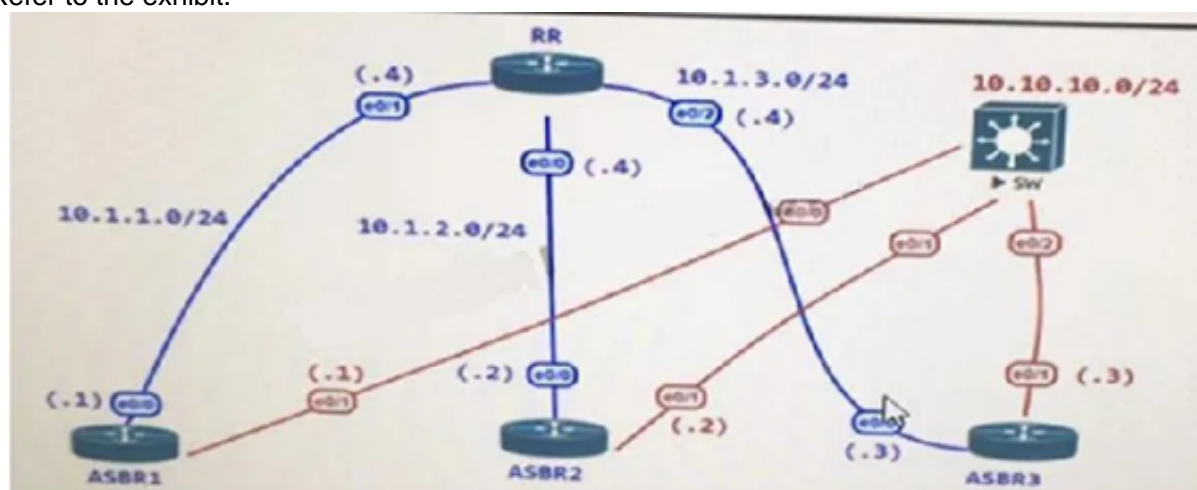
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

## NEW QUESTION 2

- (Exam Topic 3)

Refer to the exhibit.



```
RR
router bgp 100
neighbor 10.1.1.1 remote-as 100
neighbor 10.1.2.2 remote-as 100
neighbor 10.1.3.3 remote-as 100

ASBR2
router bgp 100
neighbor 10.1.1.4 remote-as 100

ASBR3
router bgp 100
neighbor 10.1.2.4 remote-as 100

ASBR4
router bgp 100
neighbor 10.1.3.4 remote-as 100
```

The administrator configured the network device for end-to-end reachability, but the ASBRs are not propagation routes to each other. Which set of configuration resolves this issue?

- A. router bgp 100 neighbor 10.1.1.1 route-reflector-client neighbor 10.1.2.2 route-reflector-client neighbor 10.1.3.3 route-reflector-client
- B. 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
- C. router bgp 100 neighbor 10.1.1.1 update-source Loopback0 neighbor 10.1.2.2 update-source Loopback0 neighbor 10.1.3.3 update-source Loopback0
- D. router bgp 100 neighbor 10.1.1.1 ebgp-multihop neighbor 10.1.2.2 ebgp-multihop neighbor 10.1.3.3 ebgp-multihop

Answer: A

### 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?

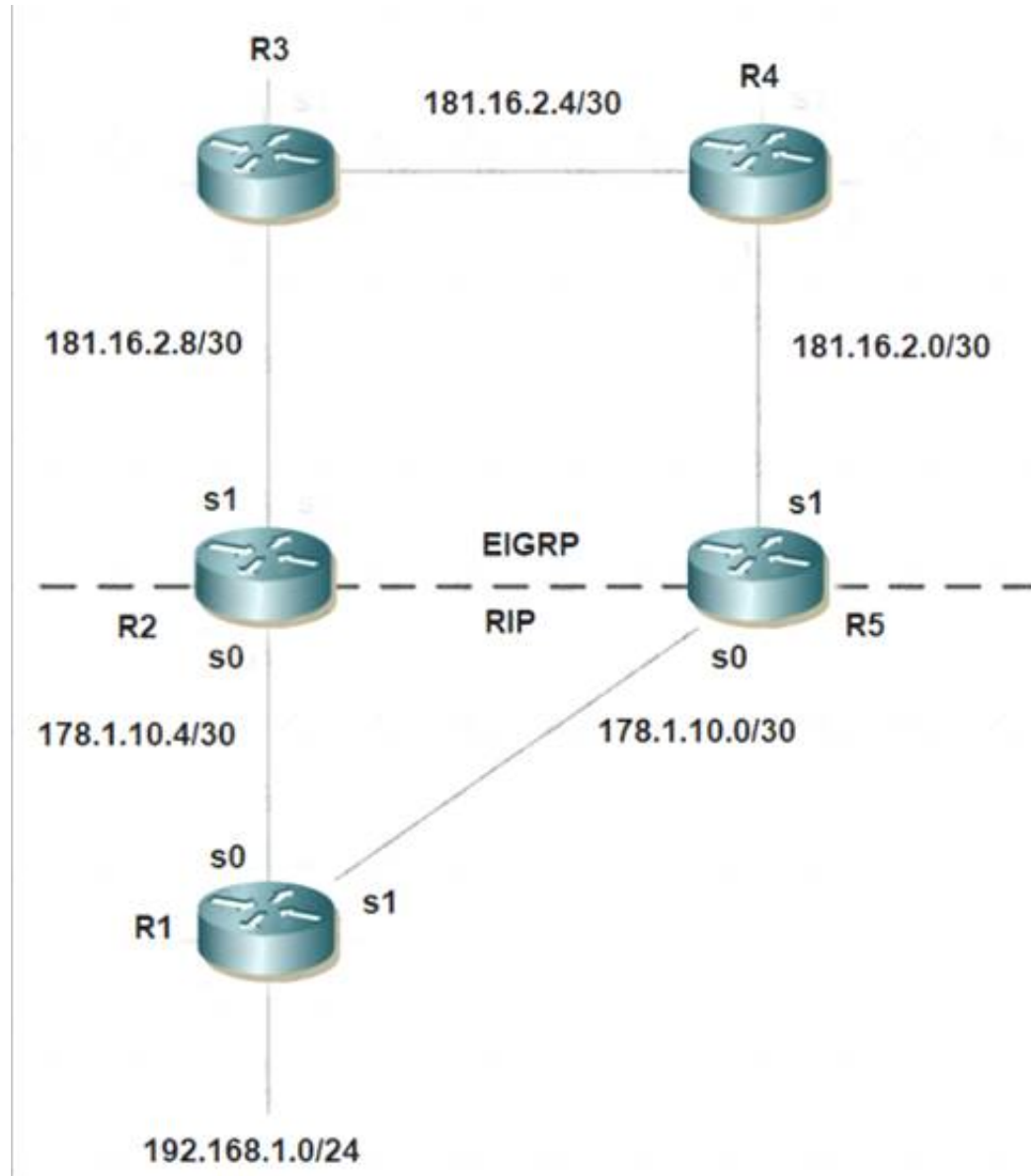
- A. access-list 1 permit 10.10.10.0 0.0.0.255 access-list 2 permit any route-map CCNP permit 10 match ip address 1 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 match ip address 2 set ip next-hop 10.1.1.2 set ip precedence 0 ! route-map CCNP permit 30
- B. access-list 100 permit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

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 10 network 181.16.0.0 redistribute rip metric 1 1 1 1 distribute-list 1 in s1 ! router rip network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any R5:router eigrp 10 network 181.16.0.0 redistribute rip metric 1 1 1 1 distribute-list 1 in s0 ! router rip network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any
- B. R2:router eigrp 10 network 181.16.0.0 redistribute rip metric 1 1 1 1 distribute-list 1 in s0 ! router rip network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any R5:router eigrp 10 network 181.16.0.0 redistribute rip metric 1 1 1 1 distribute-list 1 in s0 ! router rip network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any
- C. R2:router eigrp 10 network 181.16.0.0 redistribute rip metric 1 1 1 1 distribute-list 1 in s0 ! router rip network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any R5:router eigrp 10 network 181.16.0.0 redistribute rip metric 1 1 1 1 distribute-list 1 in s1 ! router rip network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any
- D. R2:router eigrp 7 network 181.16.0.0 redistribute rip metric 1 1 1 1 distribute-list 1 in s1 ! router rip network 178.1.0.0 redistribute eigrp 7 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any R5:router eigrp 7 network 181.16.0.0 redistribute rip metric 1 1 1 1 distribute-list 1 in s1 ! router rip network 178.1.0.0 redistribute eigrp 7 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any

Answer: D

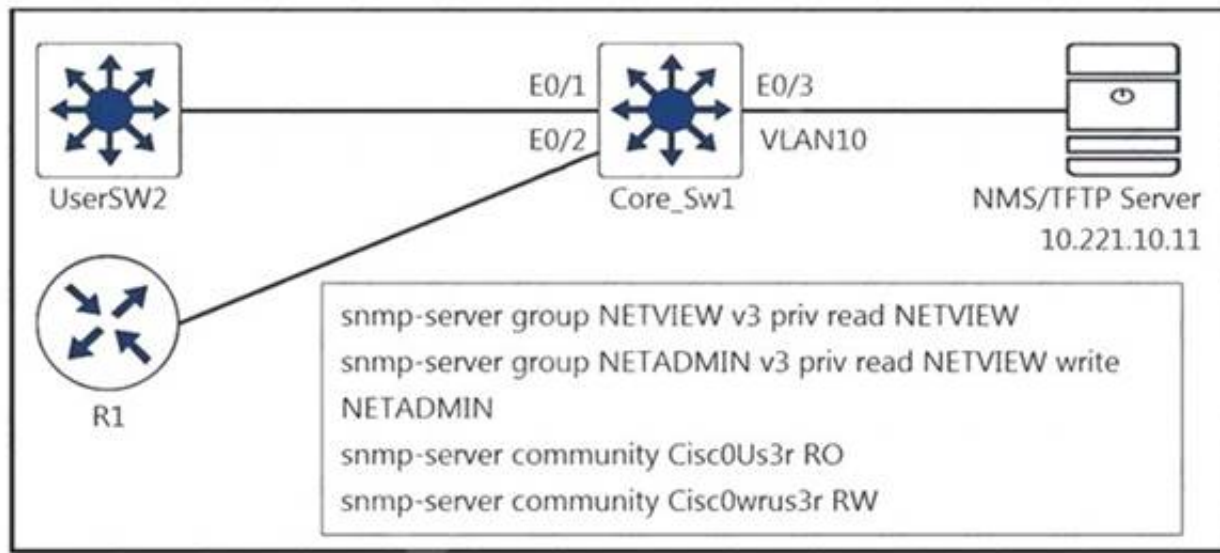
### Explanation:

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

### NEW QUESTION 5

- (Exam Topic 3)

Refer to the exhibit.



A junior engineer configured SNMP to network devices. Malicious users have uploaded different configurations to the network devices using SNMP and TFTP servers.

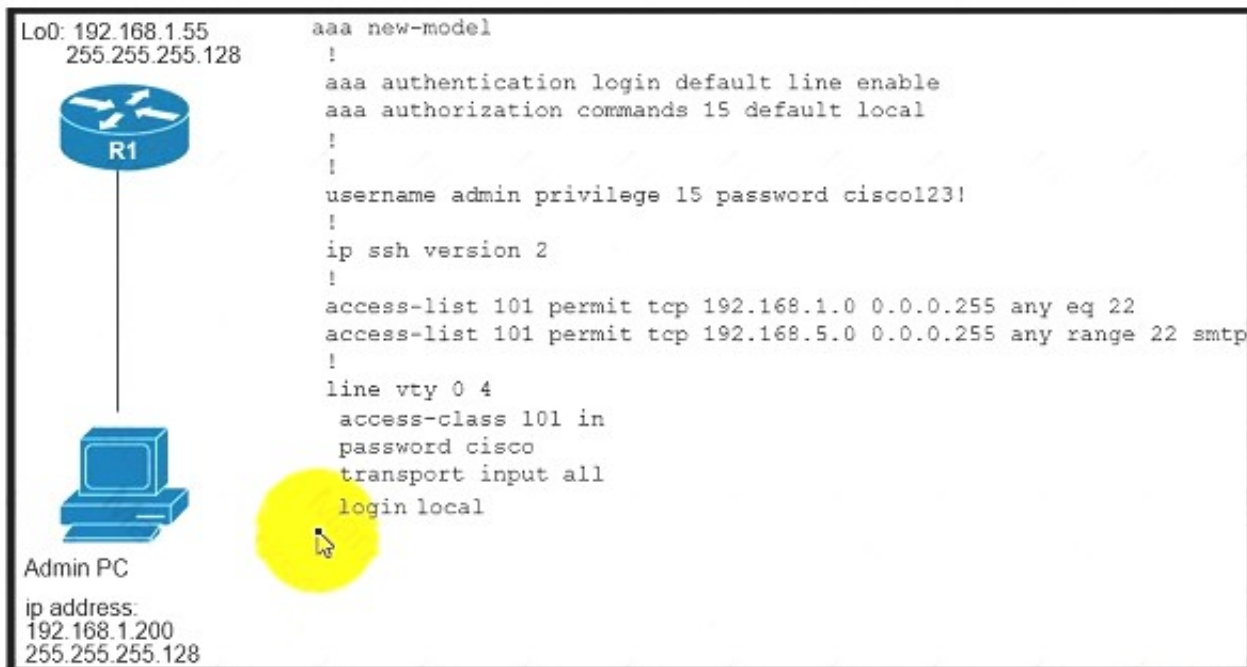
Which configuration prevents changes from unauthorized NMS and TFTP servers?

- A. access-list 20 permit 10.221.10.11 access-list 20 deny any log!snmp-server group NETVIEW v3 priv read NETVIEW access 20snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 20 snmp-server community Cisc0Us3r RO 20snmp-server community Cisc0wrus3r RW 20snmp-server tftp-server-list 20
- B. access-list 20 permit 10.221.10.11 access-list 20 deny any log!snmp-server group NETVIEW v3 priv read NETVIEW access 20snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 20 snmp-server community Cisc0wrus3r RO 20snmp-server community Cisc0Us3r RW 20 snmp-server tftp-server-list 20
- C. access-list 20 permit 10.221.10.11 access-list 20 deny any log
- D. access-list 20 permit 10.221.10.11

**Answer: A**

#### NEW QUESTION 6

- (Exam Topic 3)



Refer to the exhibit. An engineer configured user login based on authentication database on the router, but no one can log into the router. Which configuration resolves the issue?

- A. aaa authentication login default enable
- B. aaa authorization network default local
- C. aaa authentication login default local
- D. aaa authorization exec default local

**Answer: C**

#### NEW QUESTION 7

- (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 8

- (Exam Topic 3)

Refer to the exhibit.



```
!-- ACL for CoPP Routing class-map
!
access-list 120 permit tcp any gt 1024 eq bgp log
access-list 120 permit tcp any bgp gt 1024 established
access-list 120 permit tcp any gt 1024 eq 639
access-list 120 permit tcp any eq 639 gt 1024 established
access-list 120 permit tcp any eq 646
access-list 120 permit udp any eq 646
access-list 120 permit ospf any
access-list 120 permit ospf any host 224.0.0.5
access-list 120 permit ospf any host 224.0.0.6
access-list 120 permit eigrp any
access-list 120 permit eigrp any host 224.0.0.10
access-list 120 permit udp any any eq pim-auto-rp
```

The control plane is heavily impacted after the CoPP configuration is applied to the router. Which command removal lessens the impact on the control plane?

- A. access-list 120 permit udp any any eq pim-auto-rp
- B. access-list 120 permit eigrp any host 224.0.0.10
- C. access-list 120 permit ospf any
- D. access-list 120 permit tcp any gt 1024 eq bgp log

**Answer:** A

#### NEW QUESTION 9

- (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?

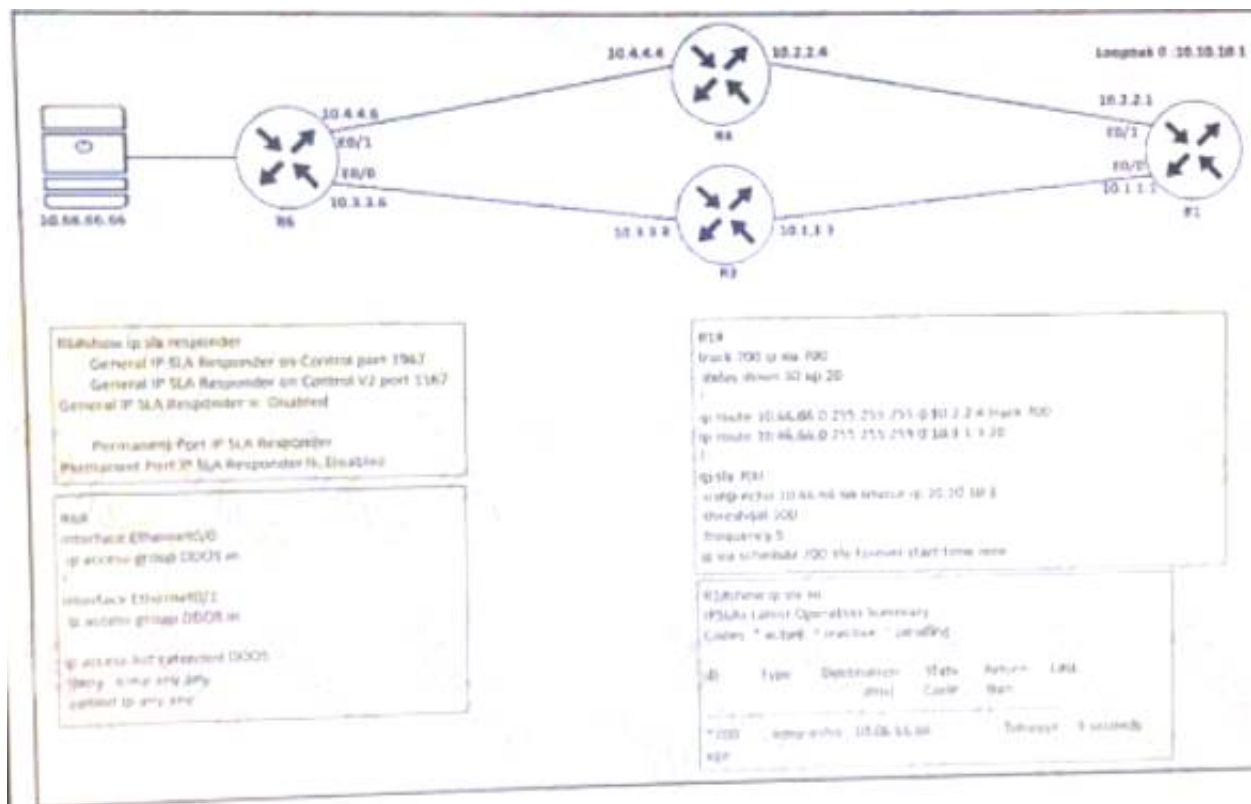
- A. Router R1 should configure ip summary address eigrp (AS number) 10.0.0.0 255.0.0.0 for the R1 Fast Ethernet 0/0 connected interface.
- B. Router R1 should configure ip route 10.0.0.0 255.0.0.0 null 0 for the routes that are received on R1.
- C. Router 10.1.100.10 should configure ip route 10.0.0.0 255.0.0.0 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 10

- (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 summary route is not shown in the RouterB routing table after this below configuration on Router\_A

```
interface ethernet 0
description location ID:S4289T9E09F39
ip address 192.168.3.1 255.255.255.0
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
```

Which Router\_A configuration resolves the issue by advertising the summary route to Router B?

- ☐ interface loopback 0
  - ip address 172.16.96.1 255.255.255.0
 interface Ethernet 0
  - ip address 192.168.3.1 255.255.255.0
  - ip summary-address eigrp 1 172.16.80.0 255.255.240.0
- ☐ interface loopback 0
  - ip address 172.16.81.1 255.255.255.0
 interface Ethernet 0
  - ip address 192.168.3.1 255.255.255.0
  - ip summary-address eigrp 1 172.16.80.0 255.255.240.0
- ☐ interface loopback 0
  - ip address 172.16.79.1 255.255.255.0
 interface Ethernet 0
  - ip address 192.168.3.1 255.255.255.0
  - ip summary-address eigrp 1 172.16.80.0 255.255.240.0
- ☐ interface loopback 0
  - ip address 172.18.81.1 255.255.255.0
 interface Ethernet 0
  - ip address 192.168.3.1 255.255.255.0
  - ip summary-address eigrp 1 172.16.80.0 255.255.240.0

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

Answer: B

#### NEW QUESTION 14

- (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 16

- (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 19

- (Exam Topic 3)

Refer to the exhibit.

```
aaa new-model
aaa group server radius RADIUS-SERVERS
aaa authentication login default group RADIUS-SERVERS local
aaa authentication enable default group RADIUS-SERVERS enable
aaa authorization exec default group RADIUS-SERVERS if-authenticated
aaa authorization network default group RADIUS-SERVERS if-authenticated
aaa accounting send stop-record authentication failure
aaa session-id common
!
line con 0
logging synchronous
stopbits 1
line vty 0 4
logging synchronous
transport input ssh
```

A network administrator successfully logs in to a switch using SSH from a (RADIUS server When the network administrator uses a console port to access the switch the RADIUS server returns shell:priv-lvl=15" and the switch asks to enter the enable command \ the command is entered, it gets rejected. Which command set is used to troubleshoot and reserve this issue?

- A. line con 0aaa authorization console authorization exec!line vty 0 4 transport input ssh
- B. line con 0aaa authorization console!line vty 0 4 authorization exec
- C. line con 0aaa authorization console priv15!line vty 0 4 authorization exec
- D. line con 0aaa authorization console authorization priv15!line vty 0 4 transport input ssh

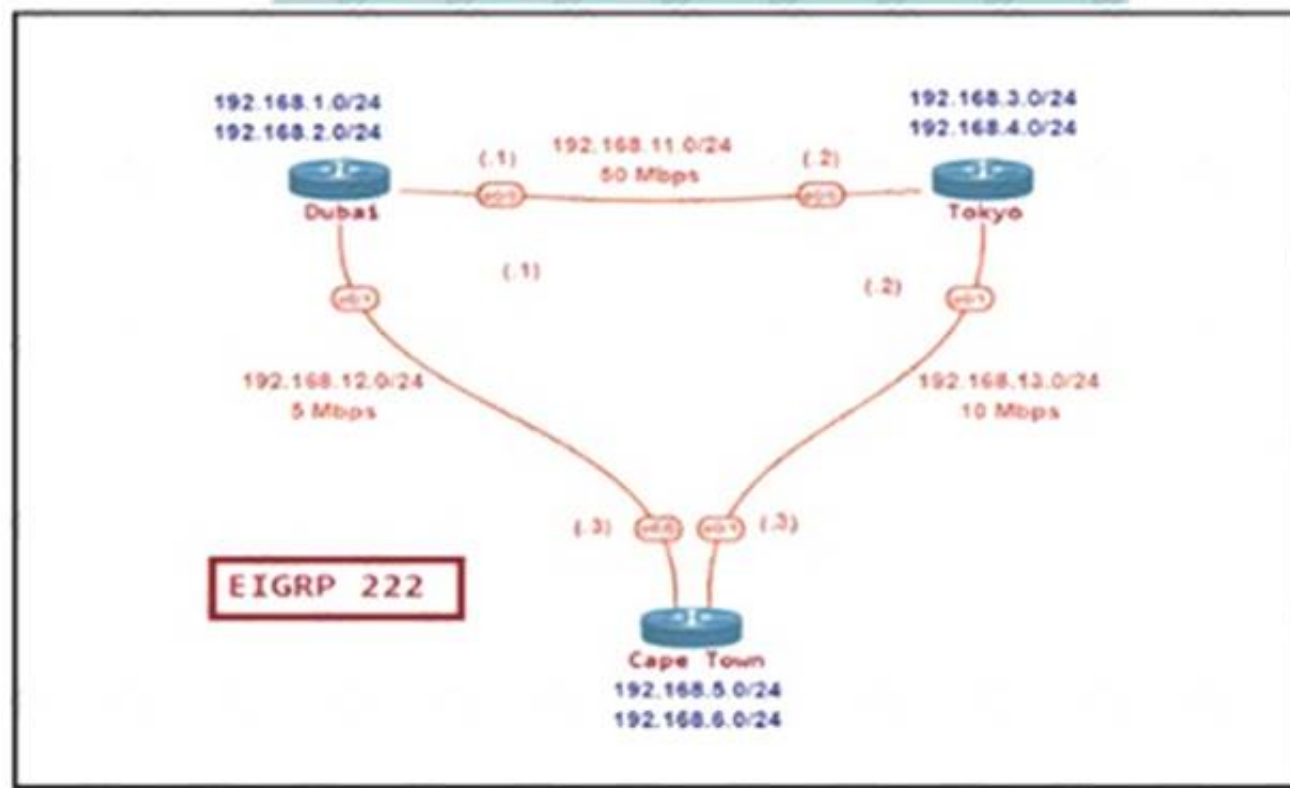
**Answer:** A

#### NEW QUESTION 24

- (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 29

- (Exam Topic 3)

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
```

While monitoring VTY access to a router, an engineer notices that the router does not have any filter and anyone can access the router with username and password even though an ACL is configured.  
Which command resolves this issue?

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

**Answer:** D

### NEW QUESTION 31

- (Exam Topic 3)

Refer to the exhibit.

```
R1#
router ospf 1
 redistribute rip subnets
 network 131.108.1.0 0.0.0.255 area 2
 network 131.108.2.0 0.0.0.255 area 2
 distribute-list 1 out
!
access-list 1 permit 132.108.4.0 0.0.0.255
```

The R1 OSPF neighbor is not receiving type 5 external LSAs for 132.108.2.0/24 and 132.108.3.0/24 networks. Which configuration command resolves the issue?

- A. access-list 1 permit 132.108.0.0 0.0.1.255
- B. access-list 1 permit 132.108.0.0 0.0.3.255
- C. access-list 1 permit 132.108.2.0 0.0.0.255
- D. access-list 1 permit 132.108.4.0 0.0.3.255

**Answer:** B

# NEW QUESTION 36

- (Exam Topic 3)

```

RF#traceroute 192.168.1.1
 1 10.0.0.9 40 msec 28 msec 24 msec
 2 * * *
 3 * * *

RE#show ip prefix-list detail
Prefix-list with the last deletion/insertion: Customer
ip prefix-list Customer:
  count: 2, range entries: 1, sequences: 5 - 10, refcount: 3
  seq 5 deny 192.168.1.1/32 (hit count: 5, refcount: 1)
  seq 10 permit 0.0.0.0/0 le 32 (hit count: 26, refcount: 1)

RC#show ip prefix-list detail
Prefix-list with the last deletion/insertion: Customer
ip prefix-list Customer:
  count: 1, range entries: 1, sequences: 10 - 10, refcount: 4
  seq 10 permit 0.0.0.0/0 le 32 (hit count: 7, refcount: 1)
    
```

Refer to the exhibit The enterprise users fail to authenticate with the TACACS server when a direct fiber link fails between RB and RD The NOC team observes

- > Users connected on AS65201 fail to authenticate with TACACS server 192 168 1 1
- > Users connected on AS65101 successfully authenticate with TACACS server 192 168 1 1
- > All AS65101 and AS65201 users are configured to authenticate with the TACACS server

Which configuration resolves the issue?

- A)
- ```

RC(config)# ip prefix-list Customer seq 5 permit 192.168.30.1/32
    
```
- B)
- ```

RC(config)#router bgp 65101
RC(config-router)# neighbor 10.0.0.18 prefix-list Customer in
    
```
- C)
- ```

RF(config)#no ip prefix-list Customer seq 5 deny 192.168.1.1/32
    
```
- D)
- ```

RF(config)#router bgp 65201
RF(config-router)# neighbor 10.0.0.17 prefix-list Customer out
    
```

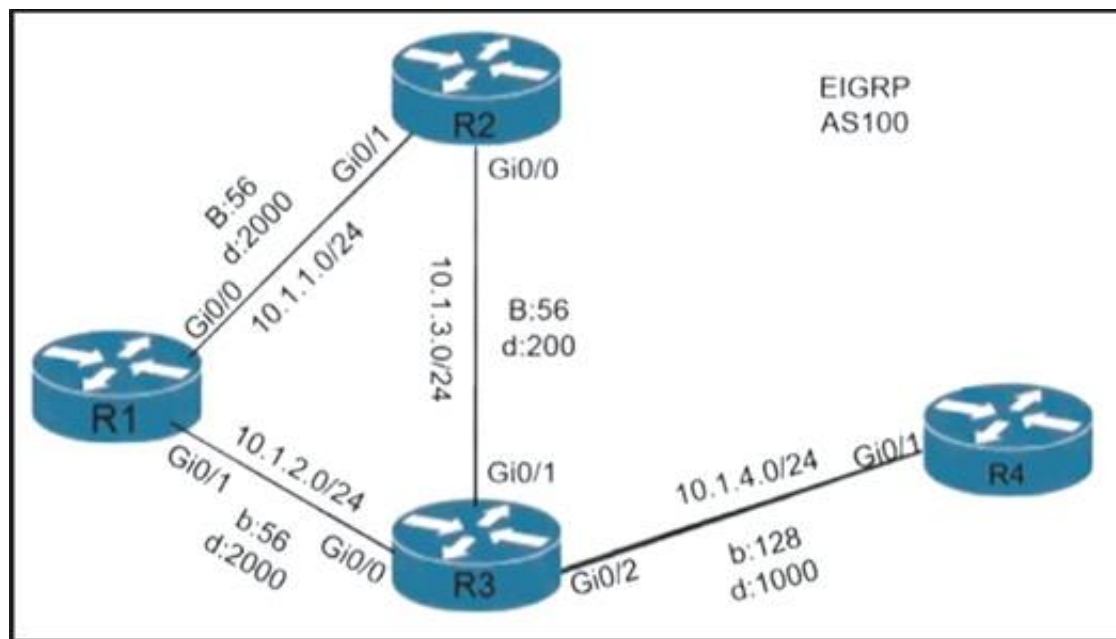
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

# NEW QUESTION 39

- (Exam Topic 3)

Refer to the exhibit.



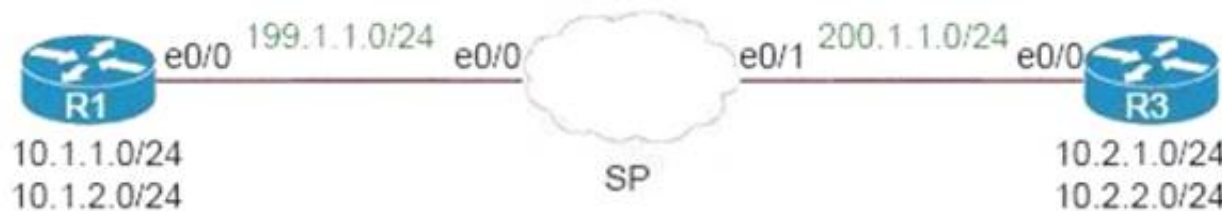
A loop occurs between R1, R2, and R3 while EIGRP is run with poison reverse enabled. Which action prevents the loop between R1, R2, and R3?

- A. Configure route tagging
- B. Enable split horizon
- C. Configure R2 as stub receive-only
- D. Configure route filtering

**Answer:** B

#### NEW QUESTION 41

- (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 46

- (Exam Topic 3)

What are the two goals of micro BFD sessions? (Choose two.)

- A. The high bandwidth member link of a link aggregation group must run BFD
- B. Run the BFD session with 3x3 ms hello timer
- C. Continuity for each member link of a link aggregation group must be verified
- D. Any member link on a link aggregation group must run BFD
- E. Each member link of a link aggregation group must run BFD.

**Answer:** CE

#### Explanation:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_bfd/configuration/xr-16-8/irb-xr-16-8-book/irb-micr](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xr-16-8/irb-xr-16-8-book/irb-micr)

#### NEW QUESTION 50

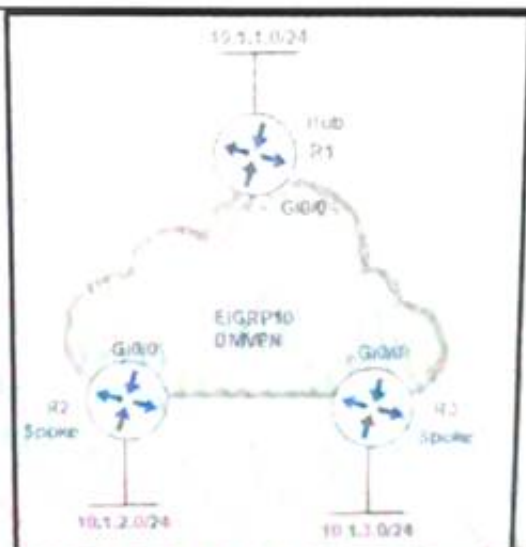
- (Exam Topic 3)

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?

- 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.
- 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.
- 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.
- 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 51

- (Exam Topic 3)

Refer to the exhibit.

```
R1# show ip ospf database self-originate
OSPF Router with ID (10.255.255.1) (Process ID 1)

Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
Link count
10.255.255.1  10.255.255.1  4          0x800003BD  0x001AD9
3

Summary Net Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
10.0.34.0    10.255.255.1  3604       0x80000380  0x00276C
10.255.255.4  10.255.255.1  3604       0x80000380  0x00762B

Type-5 AS External Link States

Link ID      ADV Router   Age         Seq#         Checksum
Tag
0.0.0.0      10.255.255.1  3604       0x800001D0  0x001CBC
0

*Feb 22 22:50:39.523: OSPF-1-FLD: Process 1 flushes LSA
ID 0.0.0.0 type-5 adv-rtr 10.255.255.1 in area 0
```

After configuring OSPF in R1, some external destinations in the network became unreachable. Which action resolves the issue?

- Clear the OSPF process on R1 to flush stale LSAs sent by other routers.
- Change the R1 router ID from 10.255.255.1 to a unique value and clear the process.
- Increase the SPF delay interval on R1 to synchronize routes.
- Disconnect the router with the OSPF router ID 0.0.0.0 from the network.

**Answer: B**

#### NEW QUESTION 56

- (Exam Topic 3)

Which router attaches the VPN label to incoming packets from CE routing?

- A. CE router
- B. core router
- C. P router
- D. PE router

Answer: D

#### NEW QUESTION 58

- (Exam Topic 3)

Refer to the exhibit.

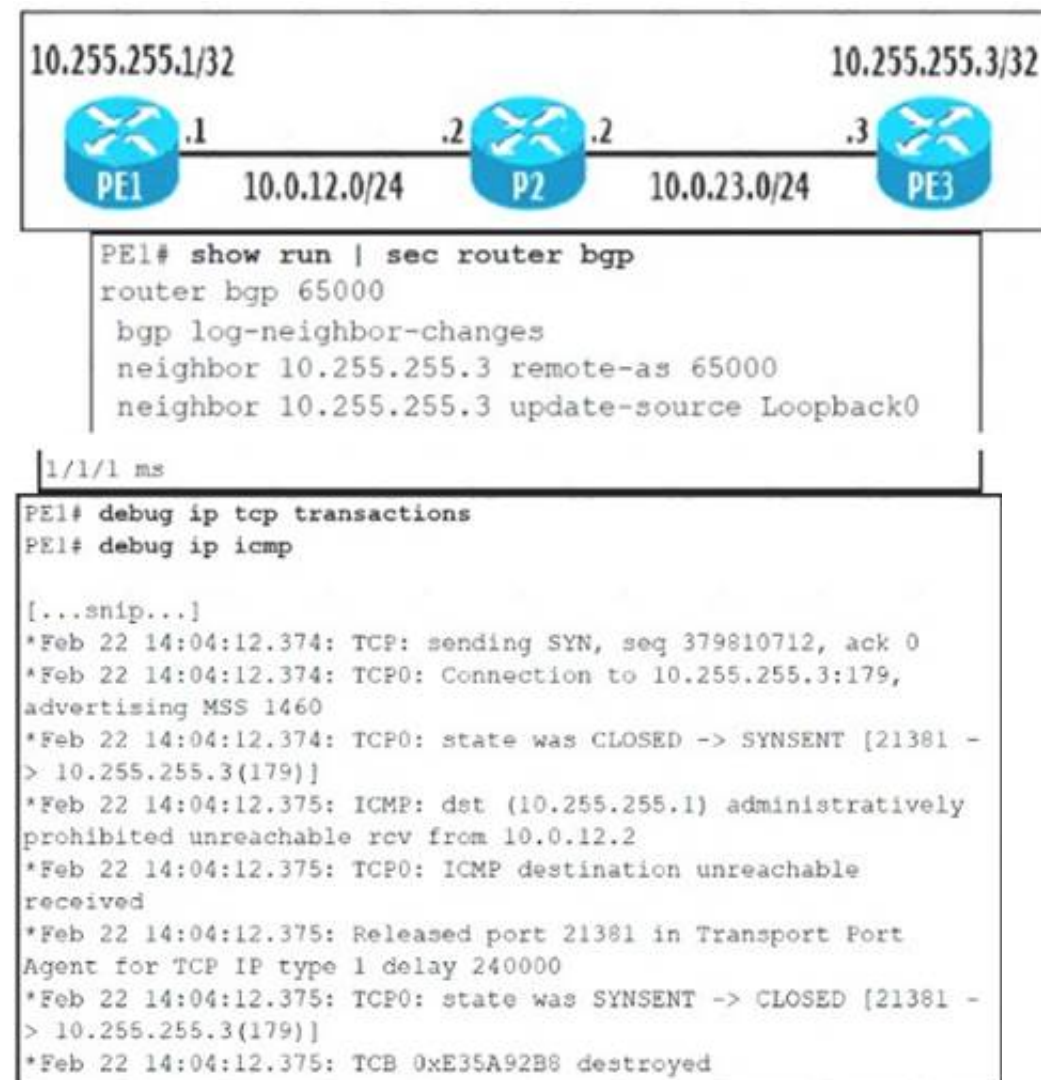
A network administrator is troubleshooting OSPF adjacency issue by going through the console logs in the router, but due to an overwhelming log message stream it is impossible to capture the problem Which two commands reduce console log messages to relevant OSPF neighbor problem details so that the issue 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 59

- (Exam Topic 3)



The diagram shows three routers: PE1, P2, and PE3. PE1 is connected to P2 via a link with IP addresses 10.0.12.1/24 on PE1 and 10.0.12.2/24 on P2. P2 is connected to PE3 via a link with IP addresses 10.0.23.2/24 on P2 and 10.0.23.3/24 on PE3. PE1 has a loopback address of 10.255.255.1/32, and PE3 has a loopback address of 10.255.255.3/32.

```

PE1# show run | sec router bgp
router bgp 65000
  bgp log-neighbor-changes
  neighbor 10.255.255.3 remote-as 65000
  neighbor 10.255.255.3 update-source Loopback0
1/1/1 ms
PE1# debug ip tcp transactions
PE1# debug ip icmp
[...snip...]
*Feb 22 14:04:12.374: TCP: sending SYN, seq 379810712, ack 0
*Feb 22 14:04:12.374: TCP0: Connection to 10.255.255.3:179,
advertising MSS 1460
*Feb 22 14:04:12.374: TCP0: state was CLOSED -> SYNSENT [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: ICMP: dst (10.255.255.1) administratively
prohibited unreachable rcv from 10.0.12.2
*Feb 22 14:04:12.375: TCP0: ICMP destination unreachable
received
*Feb 22 14:04:12.375: Released port 21381 in Transport Port
Agent for TCP IP type 1 delay 240000
*Feb 22 14:04:12.375: TCP0: state was SYNSENT -> CLOSED [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: TCB 0xE35A92B8 destroyed
  
```

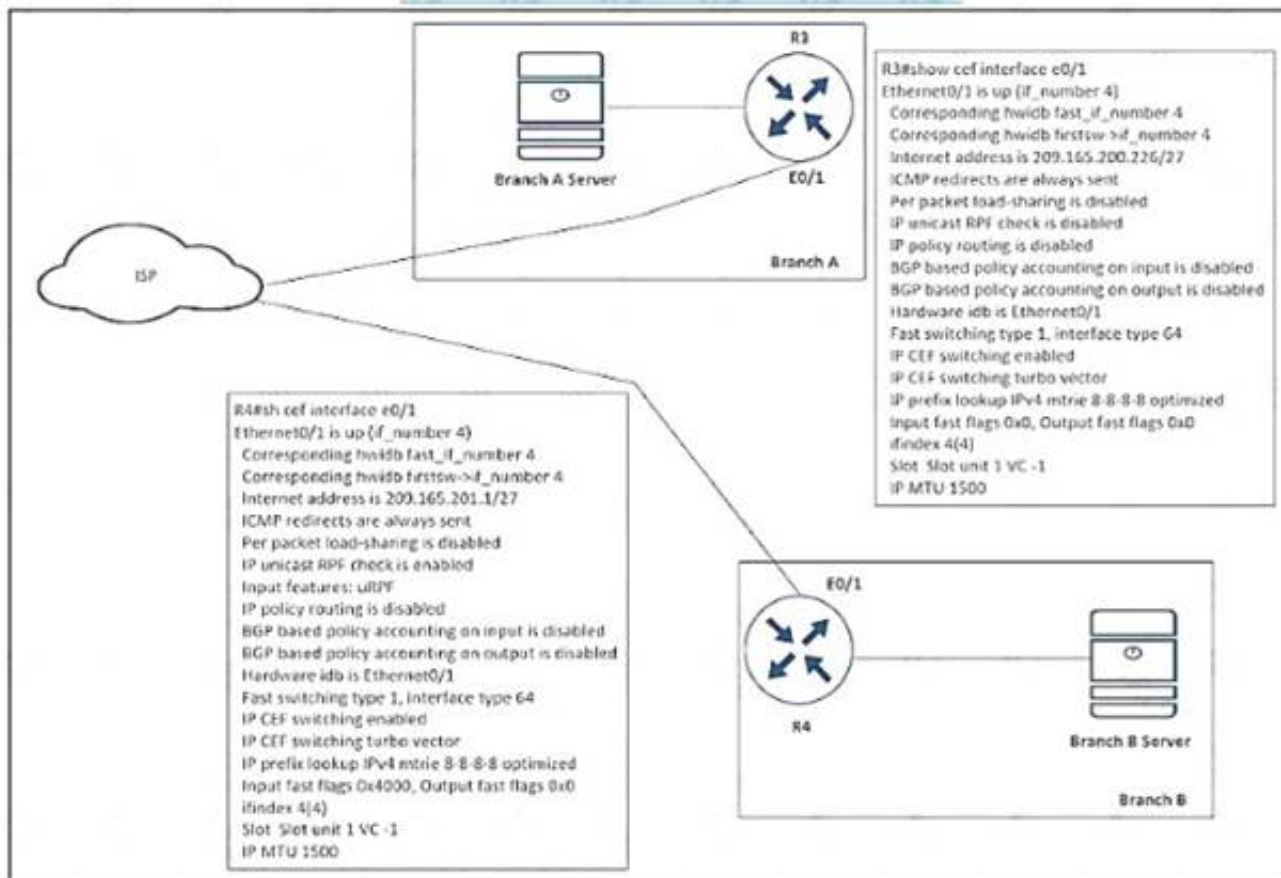
Refer to the exhibit. The administrator is troubleshooting a BGP peering between PE1 and PE3 that is unable to establish Which action resolves the issue?

- 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 63

- (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

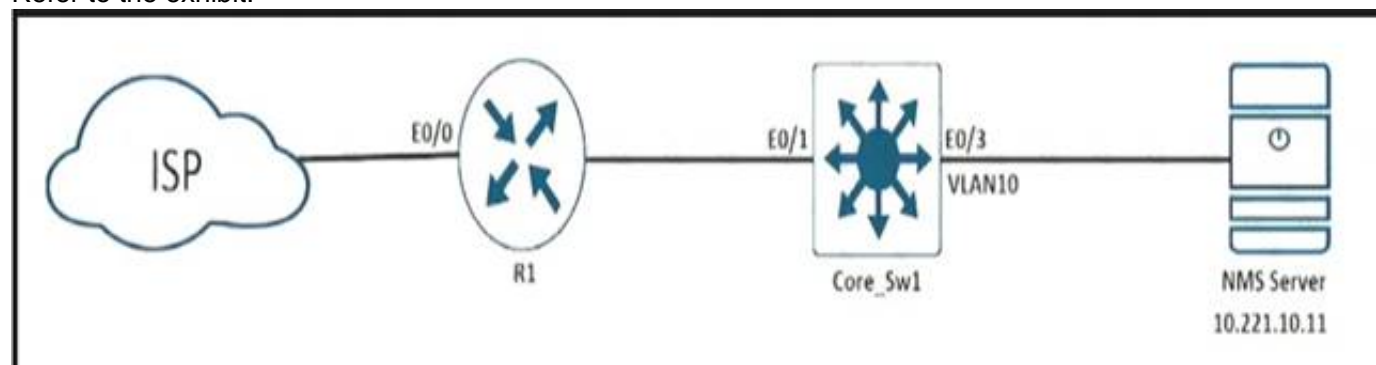
D. Option D

Answer: C

#### NEW QUESTION 65

- (Exam Topic 3)

Refer to the exhibit.



During ISP router maintenance, the network produced many alerts because of the flapping interface. Which configuration on R1 resolves the issue?

A. no snmp trap link-status

B. snmp trap link-status down



- C. snmp trap ip verify drop-rate
- D. ip verify drop-rate notify hold-down 60

Answer: D

#### NEW QUESTION 67

- (Exam Topic 3)

```

R1:
interface Loopback1
no ip address
ipv6 address 100A:0:100C::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Loopback4
no ip address
ipv6 address 400A:0:400C::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Serial1/0
no ip address
ipv6 address AB01:2011:7:100::/64 eui-64
ipv6 enable
ipv6 ospf network point-to-point
ipv6 ospf 10 area 0
ipv6 traffic-filter DENY_TELNET_Lo4 in
serial restart-delay 0
clock rate 64000
!
ipv6 router ospf 10
router-id 1.1.1.1
log-adjacency-changes
!
ipv6 access-list DENY_TELNET_LO4
sequence 20 deny tcp host 100:ABC:2011:7 host 400A:0:400C::1 eq telnet permit ipv6 any any
end

R2:
interface Loopback0
no ip address
ipv6 address 1001:ABC:2011:7::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Serial1/0
no ip address
ipv6 address AB01:2011:7:100::/64 eui-64
ipv6 enable
ipv6 ospf network point-to-point
ipv6 ospf 10 area 0
serial restart-delay 0
!
ipv6 router ospf 10
router-id 2.2.2.2
log-adjacency-changes
!
end

```

```

R1:
interface Loopback1
no ip address
ipv6 address 100A:0:100C::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Loopback4
no ip address
ipv6 address 400A:0:400C::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Serial1/0
no ip address
ipv6 address AB01:2011:7:100::/64 eui-64
ipv6 enable
ipv6 ospf network point-to-point
ipv6 ospf 10 area 0
ipv6 traffic-filter DENY_TELNET_Lo4 in
serial restart-delay 0
clock rate 64000
!
ipv6 router ospf 10
router-id 1.1.1.1
log-adjacency-changes
!
ipv6 access-list DENY_TELNET_LO4
sequence 20 deny tcp host 100:ABC:2011:7 host 400A:0:400C::1 eq telnet permit ipv6 any any
end

R2:
interface Loopback0
no ip address
ipv6 address 1001:ABC:2011:7::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Serial1/0
no ip address
ipv6 address AB01:2011:7:100::/64 eui-64
ipv6 enable
ipv6 ospf network point-to-point
ipv6 ospf 10 area 0
serial restart-delay 0
!
ipv6 router ospf 10
router-id 2.2.2.2
log-adjacency-changes
!
end

```

Refer to the exhibit. An engineer implemented an access list on R1 to allow anyone to Telnet except R2 Loopback0 to R1 Loopback4 How must sequence 20 be replaced on the R1 access list to resolve the issue?

- A. sequence 20 permit tcp host 1001 ABC:2011:7:: 1 host 400A:0:400C::1 eq telnet
- B. sequence 20 deny tcp host 400A:0:400C::1 host 1001 :ABC:2011:7::1 eq telnet
- C. sequence 20 deny tcp host 1001:ABC:2011:7::1 host 400A:0:400C::1 eq telnet
- D. sequence 20 permit tcp host 400A:0:400C::1 host 1001ABC:2011:7::1 eq telnet

Answer: C

#### NEW QUESTION 68

- (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 71

- (Exam Topic 3)

The network administrator must implement IPv6 in the network to allow only devices that not only have registered IP addresses but are also connecting from assigned locations. Which security feature must be implemented?

- A. IPv6 Snooping
- B. IPv6 Destination Guard
- C. IPv6 Prefix Guard
- D. IPv6 Router Advertisement Guard

**Answer: A**

#### NEW QUESTION 74

- (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 79

- (Exam Topic 3)

Refer to the exhibit.

```
ip prefix-list 1 permit 172.16.0.0/16
ip prefix-list 2 permit 192.168.2.0/24
!
route-map RED permit 10
match ip address prefix-list 1
set ip next hop 10.1.1.1
continue 20
exit
!
route-map RED permit 20
match ip address prefix-list 2
set ip next hop 10.2.2.2
end
```

The forwarding entries show that the next hop for prefixes from the 172.16.0.0/16 network is set to 10.2.2.2 instead of 10.1.1.1. Which action resolves the issue?

- A. Add set ip next hop 10.1.1.1 in route-map RED permit 20.
- B. Add the continue statement in route-map RED permit 10 instead of continue 20.
- C. Remove match ip address prefix-list 1 from route-map RED permit 10.
- D. Remove the continue 20 statement from route-map RED permit 10

**Answer:** D

#### NEW QUESTION 84

- (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 89

- (Exam Topic 3)

A customer requested a GRE tunnel through the provider network between two customer sites using loopback to hide internal networks. Which configuration on R2 establishes the tunnel with R1?



- A. R2(config)# interface Tunnel 1R2(config-if)# ip address 172.20.1.2 255.255.255.0R2(config-if)# ip mtu 1400 R2(config-if)# ip tcp adjust-mss 1360R2(config-if)# tunnel source 192.168.20.1 R2(config-if)# tunnel destination 192.168.10.1
- B. R2(config)# interface Tunnel 1R2(config-if)# ip address 172.20.1.2 255.255.255.0 R2(config-if)# ip mtu 1400R2(config-if)# ip tcp adjust-mss 1360 R2(config-if)# tunnel source 10.10.2.2 R2(config-if)# tunnel destination 10.10.1.1
- C. R2(config)# interface Tunnel 1R2(config-if)# ip address 172.20.1.2 255.255.255.0 R2(config-if)# ip mtu 1500R2(config-if)# ip tcp adjust-mss 1360 R2(config-if)# tunnel source 192.168.20.1 R2(config-if)# tunnel destination 10.10.1.1
- D. R2(config)# interface Tunnel 1R2(config-if)# ip address 172.20.1.2 255.255.255.0 R2(config-if)# ip mtu 1500R2(config-if)# ip tcp adjust-mss 1360 R2(config-if)# tunnel source 10.10.2.2 R2(config-if)# tunnel destination 10.10.1.1

Answer: D

### NEW QUESTION 92

- (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).

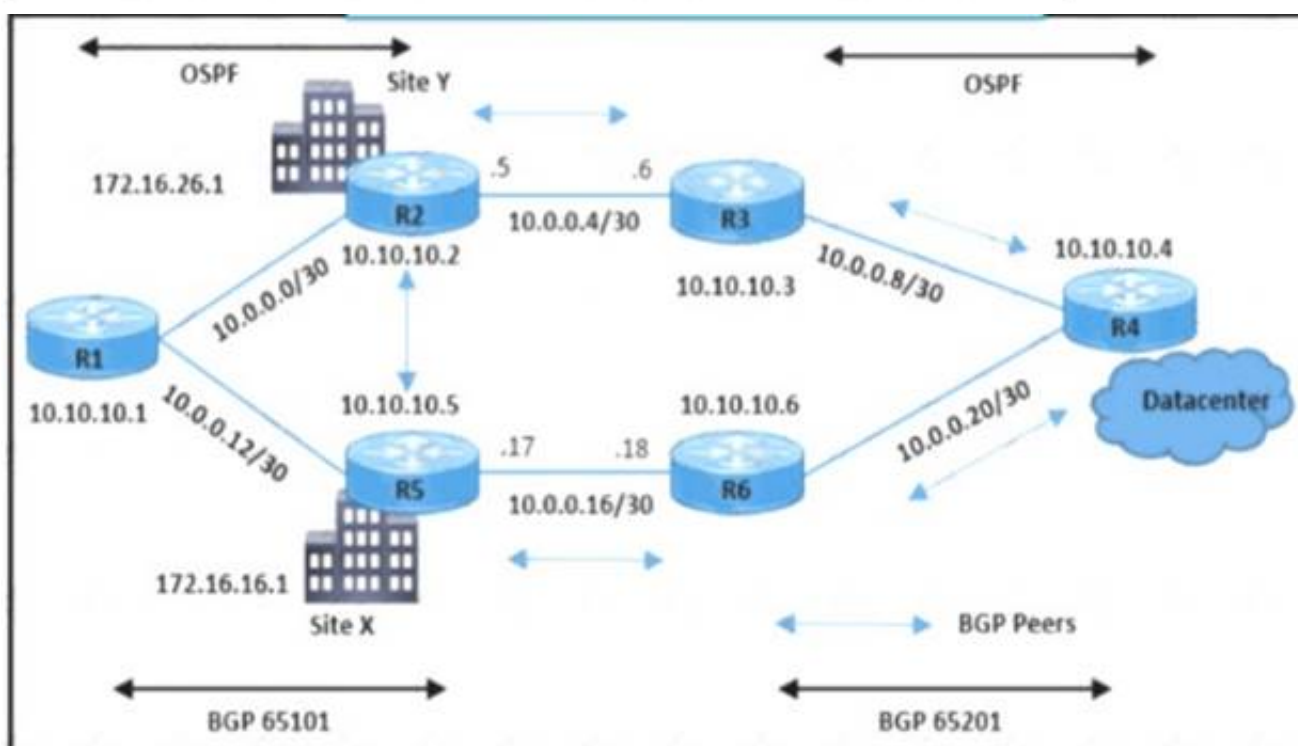
Reference: <https://blog.ipspace.net/2013/07/first-hop-ipv6-security-features-in.html>

### NEW QUESTION 93

- (Exam Topic 3)

```
R5#
*Sep 19 08:29:51.088: BGP: 10.10.10.2 open active, local address 10.0.0.14
*Sep 19 08:29:51.120: BGP: 10.10.10.2 read request no-op
*Sep 19 08:29:51.124: BGP: 10.10.10.2 open failed: Connection refused by
remote host, open active delayed 12988ms (20000ms max, 60% jitter)

R2#show ip bgp neighbors 10.10.10.5
BGP neighbor is 10.10.10.5, remote AS 65101, internal link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:01:18, last write 00:01:18, hold time is 15, keepalive
interval is 3 seconds
  Configured hold time is 15, keepalive interval is 3 seconds
  Minimum holdtime from neighbor is 0 seconds
  Address tracking is enabled, the RIB does have a route to 10.10.10.5
  Connections established 13; dropped 13
  Last reset 00:01:18, due to User reset
  Transport(tcp) path-mtu-discovery is enabled
  No active TCP connection
```



Refer to the exhibit A customer reported a failure and intermittent disconnection between two office buildings site X and site Y The network team finds that site X and site Y are exchanging email application traffic with the data center network Which configuration resolves the issue between site X and site Y?

A)

RC(config)# ip prefix-list Customer seq 5 permit 192.168.30.1/32

B)

```
RC(config)#router bgp 65101
RC(config-router)# neighbor 10.0.0.18 prefix-list Customer in
```

C)

```
RF(config)#no ip prefix-list Customer seq 5 deny 192.168.1.1/32
```

D)

```
RF(config)#router bgp 65201
RF(config-router)# neighbor 10.0.0.17 prefix-list Customer out
```

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

**Answer: C**

#### NEW QUESTION 94

- (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 99

- (Exam Topic 3)

Which router takes an active role between two LDP neighbors when initiating LDP session negotiation and LDP TCP connection establishment?

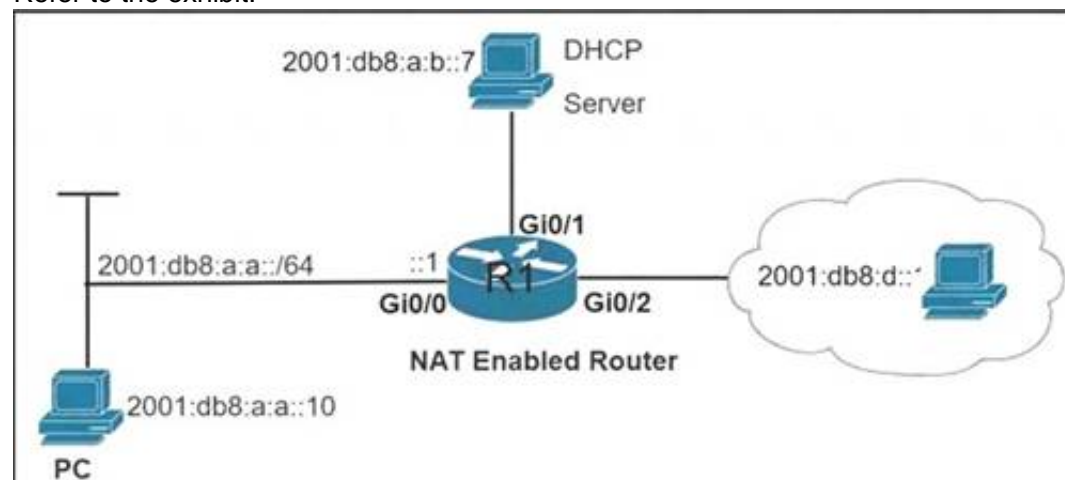
- A. with the higher IP address
- B. with the larger number of LDP TCP neighbors
- C. with the lowest IP address
- D. with one interface in the MPLS backbone

**Answer: A**

#### NEW QUESTION 100

- (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 103

- (Exam Topic 3)

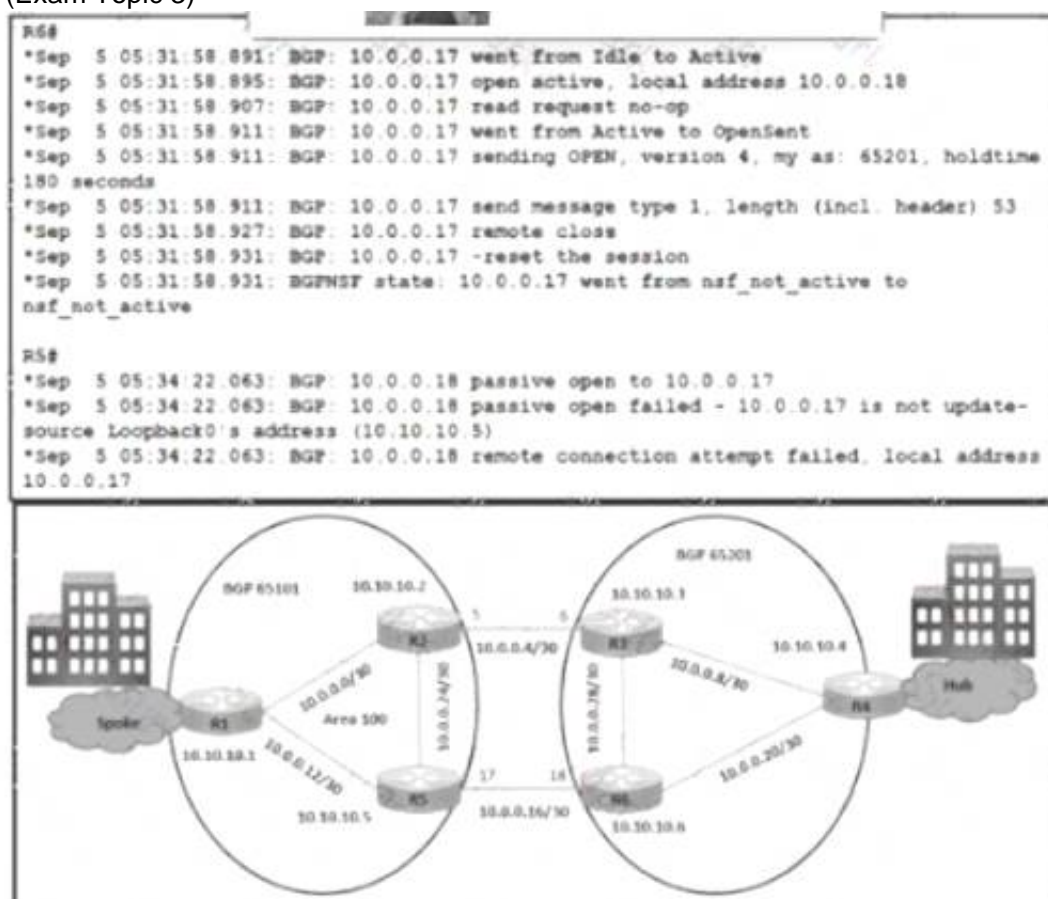
How does an MPLS Layer 3 VPN differentiate the IP address space used between each VPN?

- A. by RD
- B. by address family
- C. by MP-BGP
- D. by RT

Answer: A

#### NEW QUESTION 106

- (Exam Topic 3)



Refer to the exhibit. The traffic from spoke to hub is dropping. The operations team observes:

- R2-R3 link is down due to the fiber cut.
- R2 and R5 receive traffic from R1 in AS 65101.
- R3 and R5 receive traffic from R4 in AS 65201.

Which configuration resolves the issue?



- A)  
R6(config)#router bgp 65101  
R6(config-router)#no neighbor 10.0.0.17 update-source Loopback0
- B)  
R5(config)#router bgp 65101  
R5(config-router)#no neighbor 10.0.0.18 update-source Loopback0
- C)  
R6(config)#router bgp 65201  
R6(config-router)#neighbor 10.10.10.5 remote-as 65101  
R6(config-router)#neighbor 10.10.10.5 update-source Loopback0  
R6(config-router)#neighbor 10.10.10.5 ebgp-multihop 3
- D)  
R5(config)#router bgp 65101  
R5(config-router)#neighbor 10.10.10.6 remote-as 65201  
R5(config-router)#neighbor 10.10.10.6 update-source Loopback0  
R5(config-router)#neighbor 10.10.10.6 ebgp-multihop 3

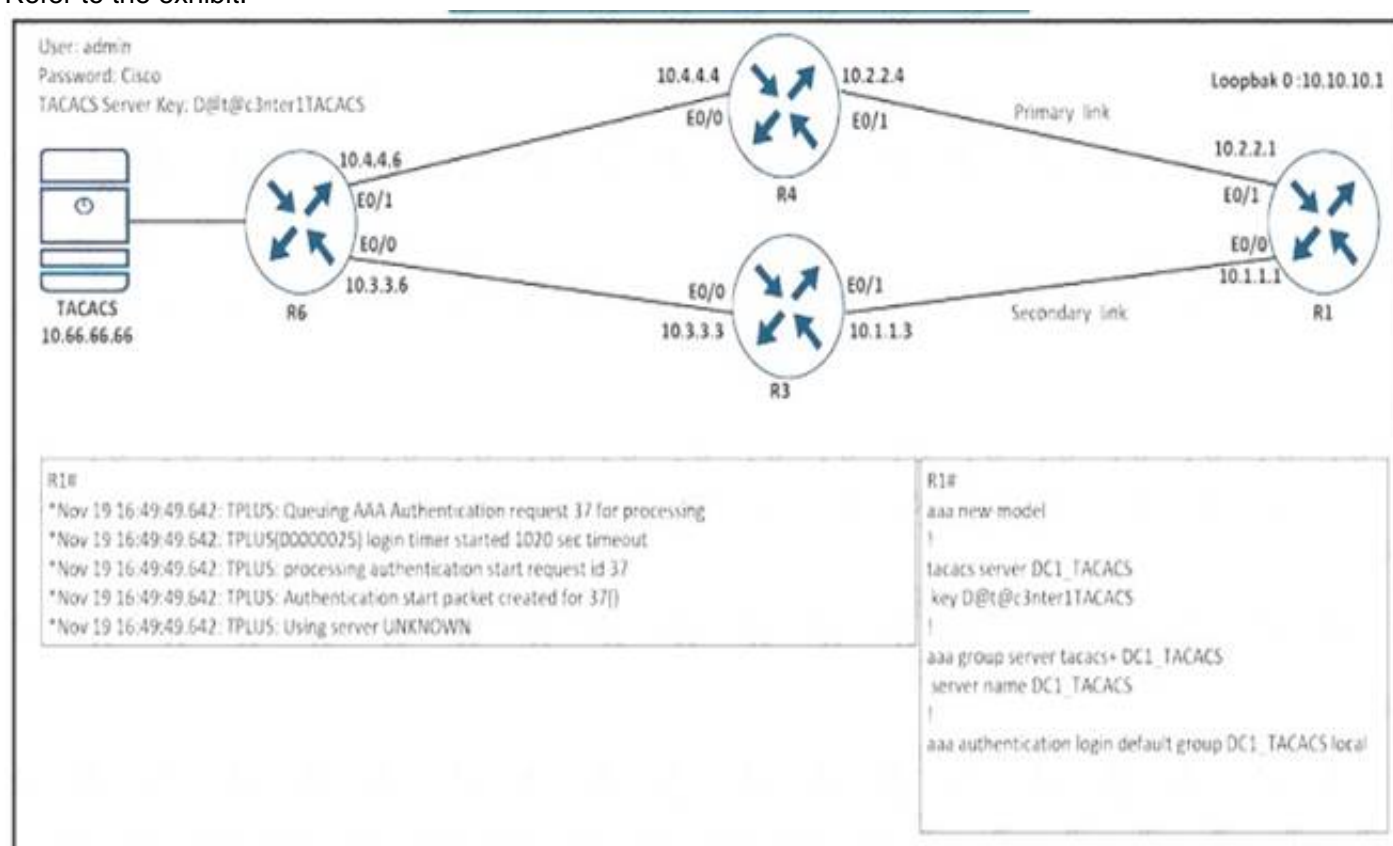
- A. Option A  
B. Option B  
C. Option C  
D. Option D

Answer: C

#### NEW QUESTION 107

- (Exam Topic 3)

Refer to the exhibit.



Refer to the exhibit R1 cannot authenticate via TACACS Which configuration resolves the issue?

- ☒ aaa group server tacacs+ DC\_TACACS  
server name DC\_TACACS
- ☐ tacacs server DC1\_TACACS  
address ipv4 10.66.66.66  
key D@t@c3nter1TACACS
- ☐ aaa group server tacacs+ DC1\_TACACS  
server name DC\_TACACS
- ☐ tacacs server DC1\_TACACS  
address ipv4 10.60.66.66  
key D@t@c3nter1TACACS

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

Answer: B

#### NEW QUESTION 110

- (Exam Topic 3)

What must be configured by the network engineer to circumvent AS\_PATH prevention mechanism in IP/VPN Hub and Spoke deployment scenarios?

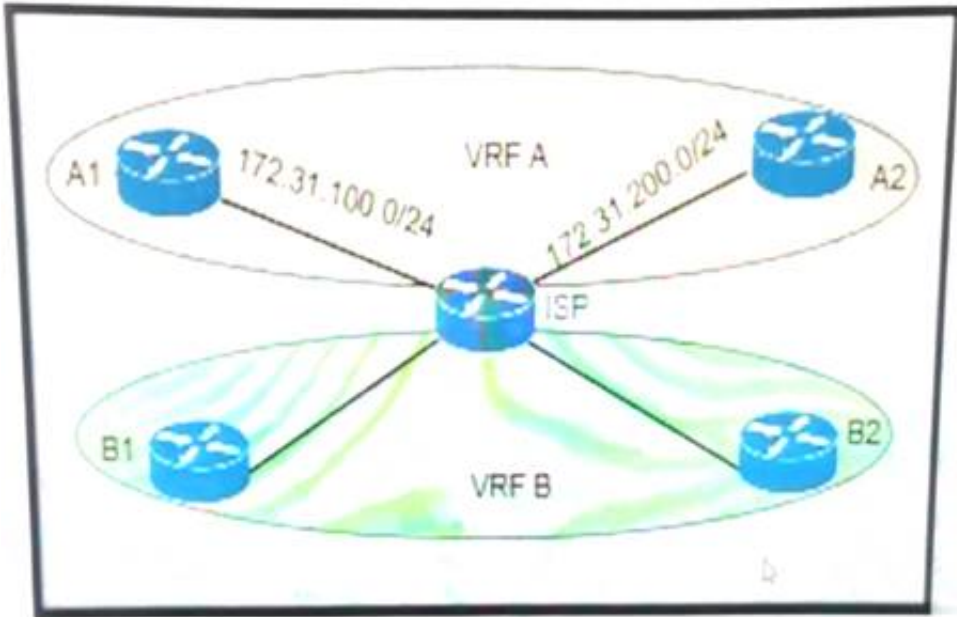
- A. Use allows in and as-override at all Pes.
- B. Use allows in and as-override at the PE-Hub.
- C. Use Allowas-in the PE\_Hub
- D. Use as-override at the PE\_Hub

Answer: D

#### NEW QUESTION 111

- (Exam Topic 3)

Refer to the exhibit. The ISP router is fully configured for customer A and customer B using the VRF-Lite feature. What is the minimum configuration required for customer A to communicate between routers A1 and A2?



- A. A1interface fa0/0 description To->ISPIp add 172.31.100.1 255.255.255.0no shut!router ospf 100net 172.31.100.1 0.0.0.255 area 0 A2interface fa0/0 description To->ISPIp add 172.31.200.1 255.255.255.0no shut!router ospf 100net 172.31.200.1 0.0.0.255 area 0
- B. A1interface fa0/0 description To->ISP ip vrf forwarding Aip add 172.31.100.1 255.255.255.0no shut!router ospf 100net 172.31.100.1 0.0.0.255 area 0 A2interface fa0/0 description To->ISP ip vrf forwarding Aip add 172.31.200.1 255.255.255.0no shut!router ospf 100net 172.31.200.1 0.0.0.255 area 0
- C. A1interface fa0/0 description To->ISPIp add 172.31.200.1 255.255.255.0no shut!router ospf 100net 172.31.200.1 0.0.0.255 area 0 A2interface fa0/0 description To->ISPIp add 172.31.100.1 255.255.255.0no shut!router ospf 100net 172.31.100.1 0.0.0.255 area 0
- D. A1interface fa0/0 description To->ISP ip vrf forwarding Aip add 172.31.100.1 255.255.255.0no shut!router ospf 100 vrf A net 172.31.200.1 0.0.0.255 area 0 A2interface fa0/0 description To->ISP ip vrf forwarding Aip add 172.31.100.1 255.255.255.0no shut!router ospf 100 vrf A net 172.31.200.1 0.0.0.255 area 0

Answer: C

#### Explanation:

A1 and A2 routers do not know they belong to VRF A. The two interfaces of ISP (which are connected to A1 & A2) should be configured like this (we only show the configure of one interface):

ISP router:

```
interface g0/0
description ISP->To_CustomerA ip vrf forwarding A
ip address 172.31.100.2 255.255.255.0
router ospf 100 vrf A
network 172.31.200.2 0.0.0.255 area 0
```

#### NEW QUESTION 113

- (Exam Topic 3)

Users report issues with reachability between areas as soon as an engineer configured summary routes between areas in a multiple area OSPF autonomous system. Which action resolves the issue?

- A. Configure the summary-address command on the ASBR.
- B. Configure the summary-address command on the ABR.
- C. Configure the area range command on the ABR.
- D. Configure the area range command on the ASBR.

Answer: C

#### Explanation:

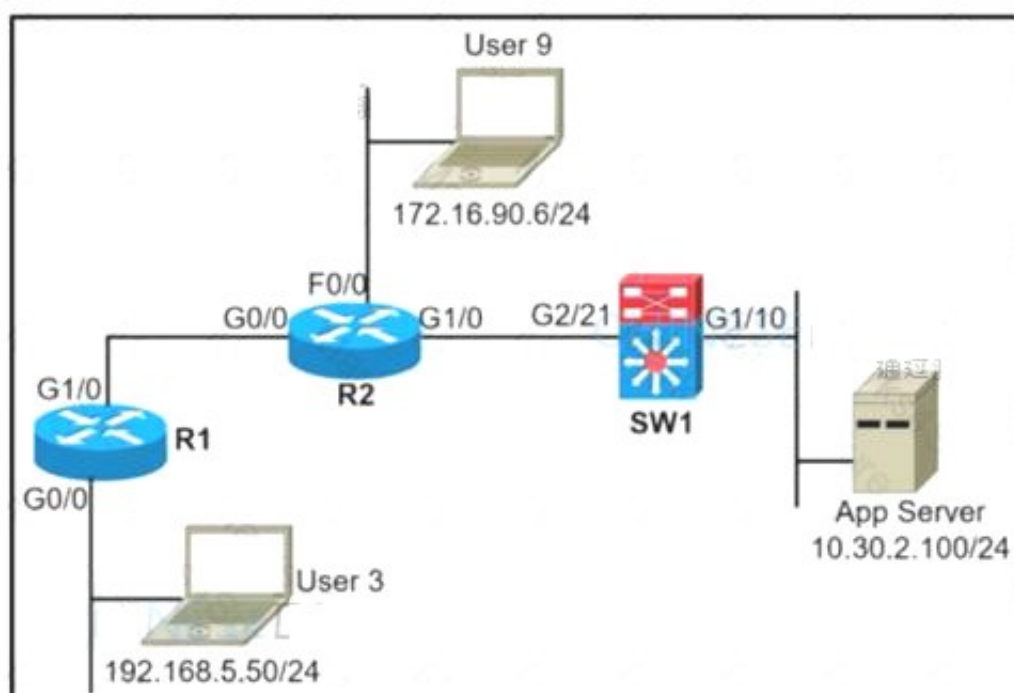
For OSPF, we can only summary at the ABR with the command “area range” or at the ASBR with the command “summary-address” -> Therefore answer A and answer B are not correct.

In this question, the most likely problem is that when doing summarization, the network mask is configured wrong and summarization doesn’t work because of the misconfiguration. When configuring the area range command, make sure that the summarization mask is in the form of a prefix mask rather than a wildcard mask (that is, 255.255.255.0 instead of 0.0.0.255).

Good reference: <https://www.confirouter.com/troubleshooting-route-summarization-ospf-14082/>

#### NEW QUESTION 114

- (Exam Topic 3)  
Refer to the exhibit.



A network administrator must block ping from user 3 to the App Server only. An inbound standard access list is applied to R1 interface G0/0 to block ping. The network administrator was notified that user 3 cannot even ping user 9 anymore. Where must the access list be applied in the outgoing direction to resolve the issue?

- A. R2 interface G1/0
- B. R2 interface G0/0
- C. SW1 interface G1/10
- D. SW1 interface G2/21

**Answer:** D

#### NEW QUESTION 117

- (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/xr-3s/ipv6-xr-3s-book/ipv6-src-guar](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xr-3s/ipv6-xr-3s-book/ipv6-src-guar)

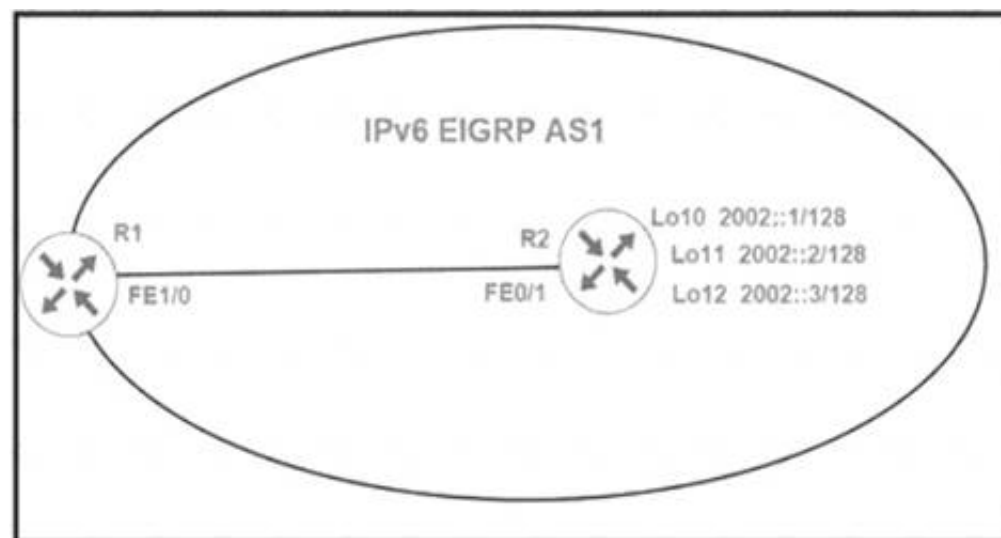
#### NEW QUESTION 119

- (Exam Topic 3)

```

R1#sh ipv6 route eigrp
IPv6 Routing Table - default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery, I - LISP
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R1#
R1#show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(1)
H Address          Interface      Hold Uptime  SRTT  RTO  Q Seq
  (sec)              (ms)          Cnt Num
0 Link-local address: Fa1/0          11 00:04:22 1593 5000 0 15
  FE80::C004:22FF:FE78:1
R1#
  
```





```
R2#show run
interface Loopback10
no ip address
ipv6 address 2002::1/128
ipv6 eigrp 1
|
interface Loopback11
no ip address
ipv6 address 2002::2/128
ipv6 eigrp 1
|
interface Loopback12
no ip address
ipv6 address 2002::3/128
ipv6 eigrp 1
|
interface FastEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address autoconfig
ipv6 eigrp 1
|
ipv6 router eigrp 1
stub summary
no shutdown
```

R1 cannot receive the R2 Interfaces with individual prefixes. What must be reconfigured to advertise R2 Interfaces to R1?

- A. EIGRP process on R2 by removing the stub command Keyword summary
- B. interface FastEthernet0/1 on R2 with an EIGRP summary for all three loopback prefixes
- C. EIGRP process on R2 with the command stub summary receive-only
- D. EIGRP process on R2 with the command stub summary connected

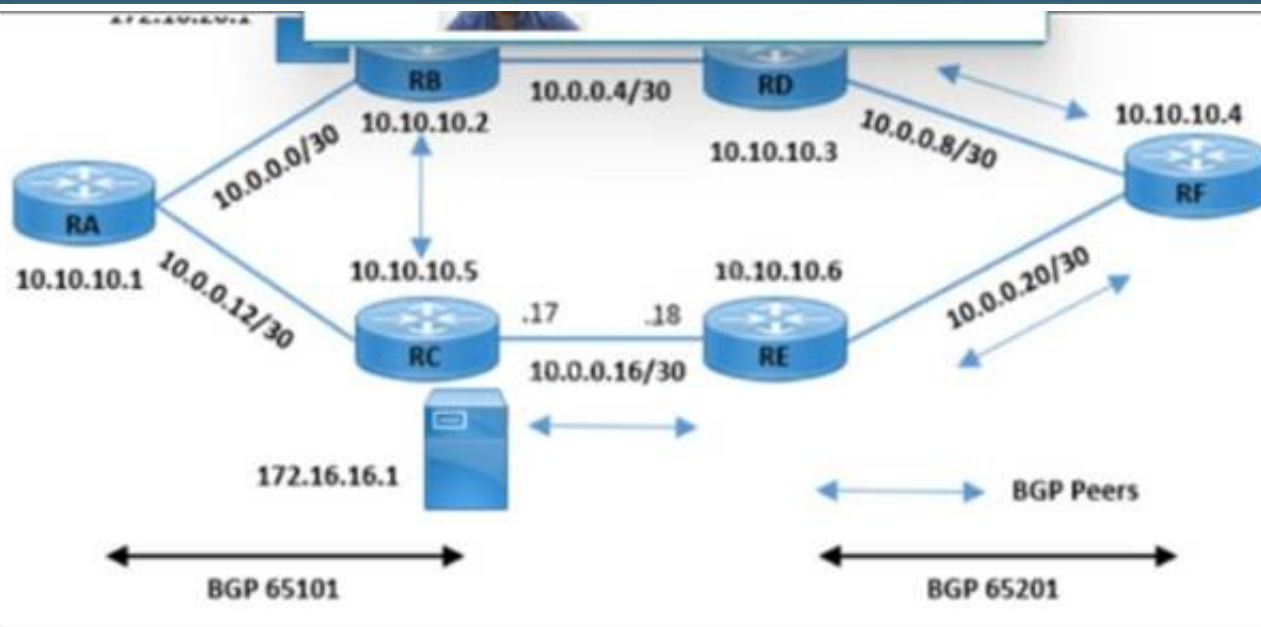
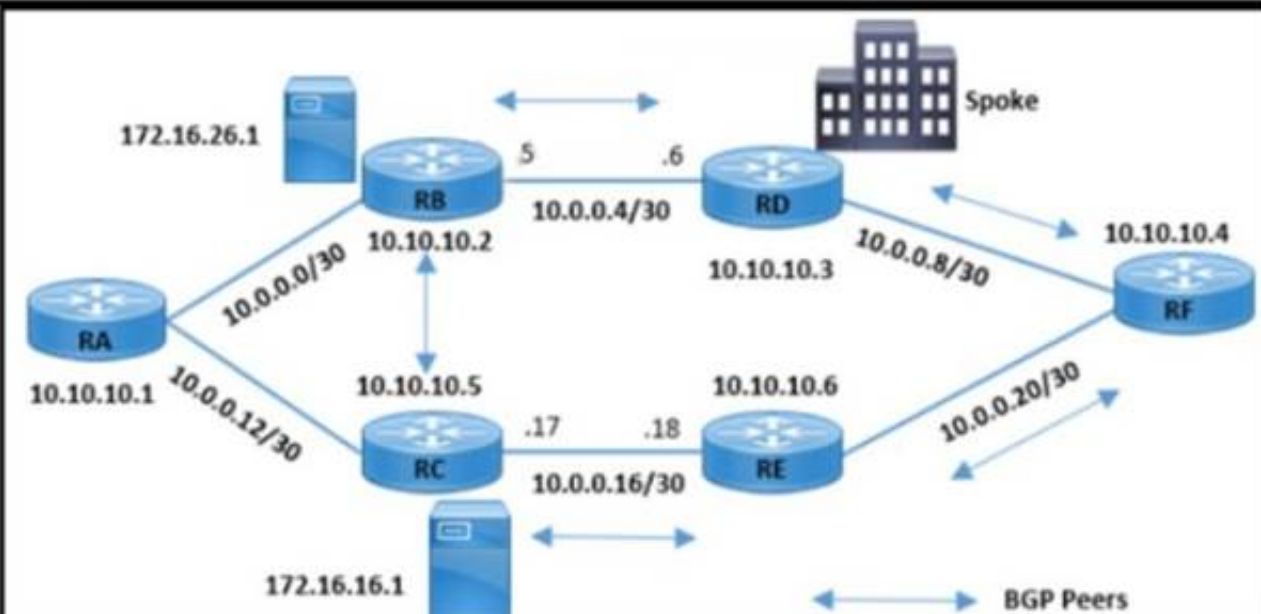
**Answer:** D

#### NEW QUESTION 120

- (Exam Topic 3)

```
RB#show ip bgp 172.16.16.1
BGP routing table entry for 172.16.16.1/32, version 11
Paths: (1 available, no best path)
Not advertised to any peer
Local
 10.10.10.5 (metric 3) from 10.10.10.5 (172.16.16.1)
  Origin IGP, metric 0, localpref 100, valid, internal, not synchronized
```

```
RD#traceroute 172.16.16.1
Tracing the route to 172.16.16.1
 1 10.0.0.10 [MPLS: Label 29 Exp 0] 64 msec 56 msec 60 msec
 2 10.0.0.21 60 msec 56 msec 72 msec
 3 * * *
```



Refer to the exhibit A customer reported an issue with a fiber link failure between RC and RE Users connected through the spoke location face disconnection and packet drops with the primary email server (172.16.16.1) but have no issues with the backup email server (172.16.26.1). All the router loopback IPs are advertised through the OSPF protocol. Which configuration resolves the issue?

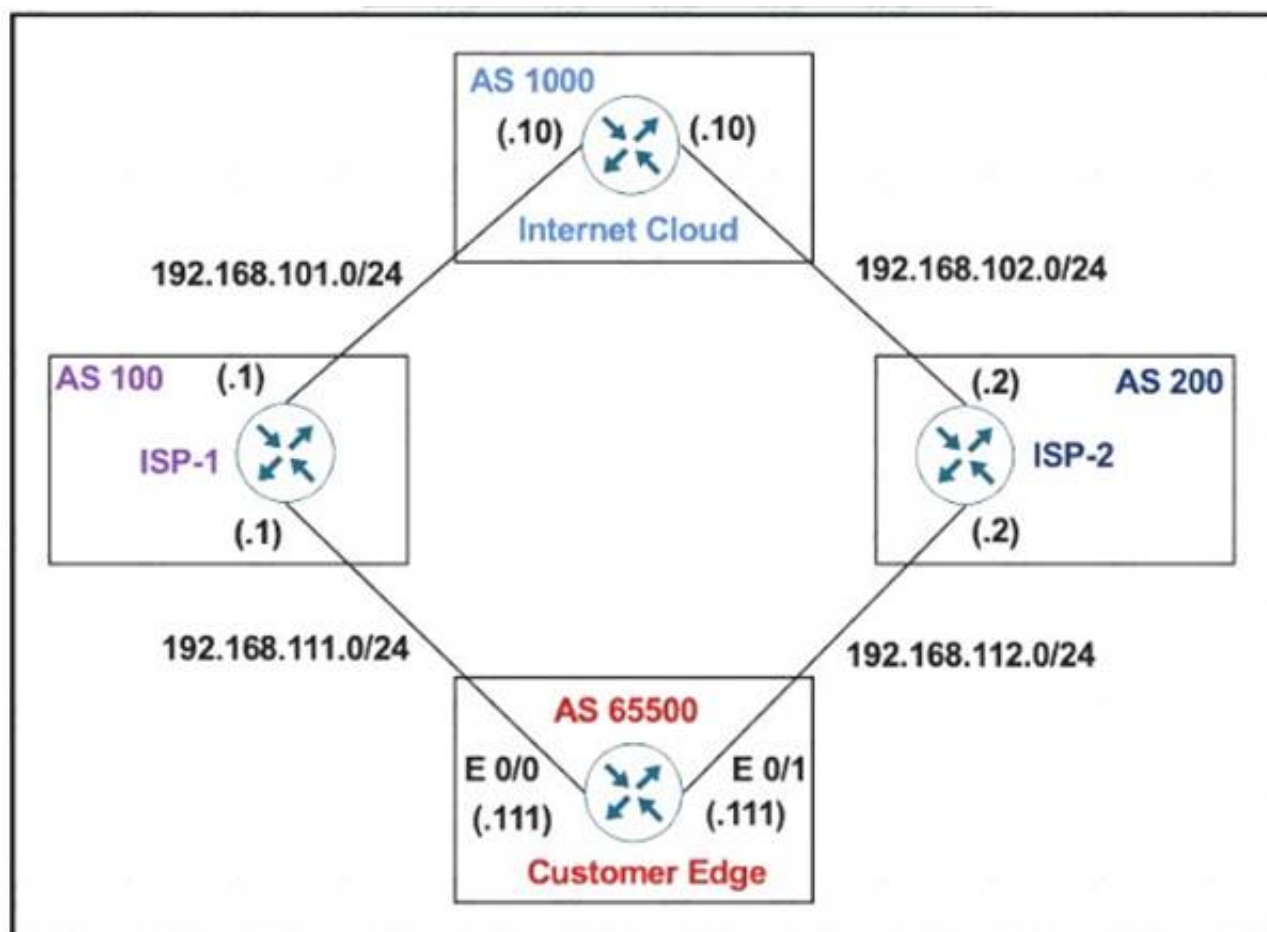
- ☐ RB(config)#router bgp 65101  
RB(config-router)#no synchronization
- ☐ RC(config)#router bgp 65101  
RC(config-router)#neighbor 10.10.10.2 next-hop-self
- ☐ RB(config)#router bgp 65101  
RB(config-router)#neighbor 10.10.10.5 next-hop-self
- ☐ RC(config)#router bgp 65101  
RC(config-router)#no synchronization

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

Answer: B

#### NEW QUESTION 121

- (Exam Topic 3)  
Refer to the exhibit.



The Customer Edge router (AS 65500) wants to use AS 100 as the preferred ISP for all external routes.

```

Customer Edge
route-map SETLP
set local-preference 111
!
router bgp 65500
neighbor 192.168.111.1 remote-as 100
neighbor 192.168.111.1 route-map SETLP out
neighbor 192.168.112.2 remote-as 200
  
```

This configuration failed to send routes to AS 100 as the preferred path. Which set of configuration resolves the issue?

- ☐ route-map SETLP  
set local-preference 111  
!  
router bgp 65500  
neighbor 192.168.111.1 remote-as 100  
neighbor 192.168.111.1 route-map SETLP out  
neighbor 192.168.112.2 remote-as 200
- ☐ route-map SETLP  
set local-preference 111  
!  
router bgp 65500  
neighbor 192.168.111.1 remote-as 100  
neighbor 192.168.111.1 route-map SETLP in
- ☐ route-map SETPP  
set as-path prepend 111 111  
!  
router bgp 65500  
neighbor 192.168.111.1 remote-as 100  
neighbor 192.168.111.1 route-map SETPP out
- ☒ route-map SETPP  
set as-path prepend 100 100  
!  
router bgp 65500  
neighbor 192.168.111.1 remote-as 100  
neighbor 192.168.111.1 route-map SETPP in

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

Answer: B

#### NEW QUESTION 126

- (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 of 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 131

- (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

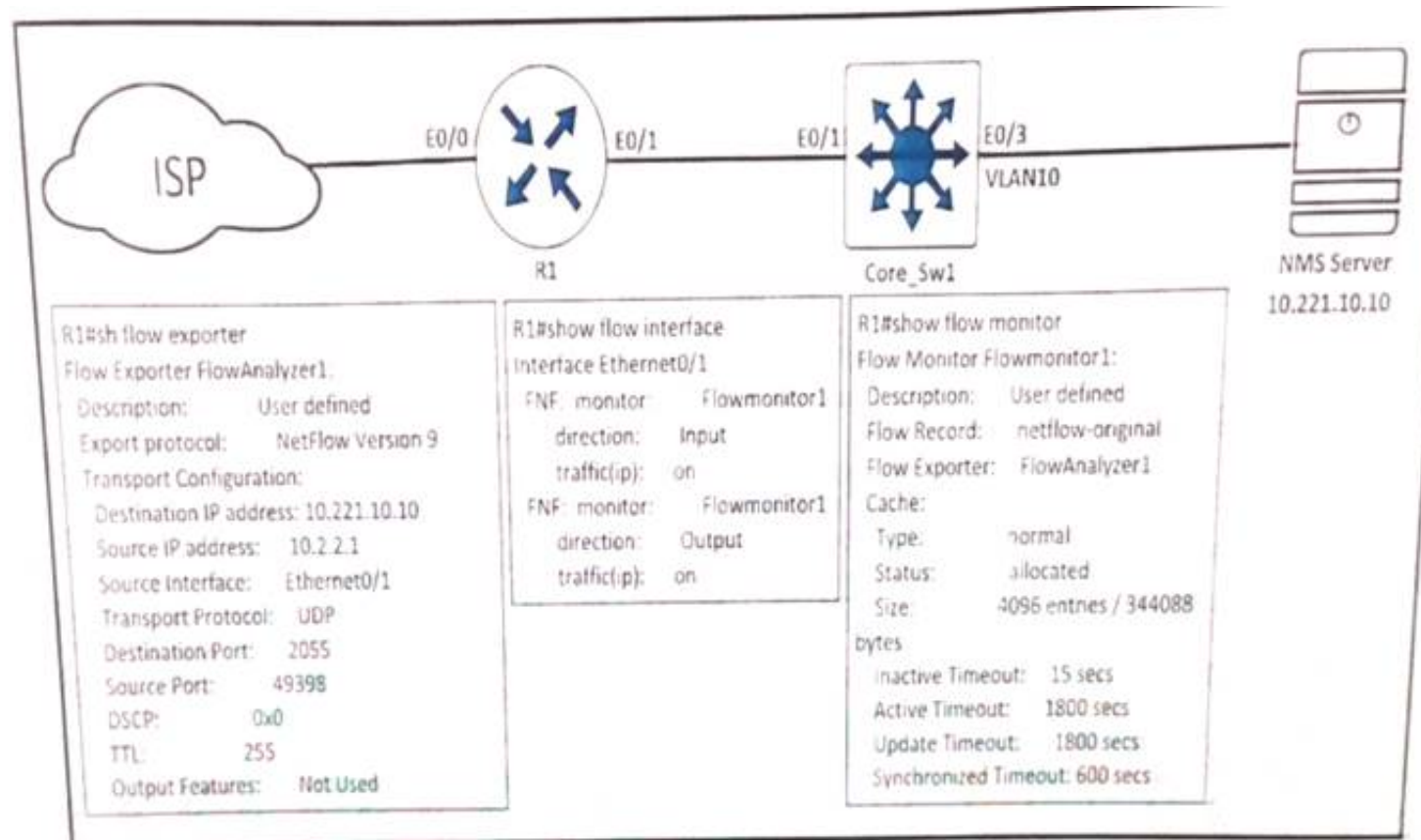
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

#### NEW QUESTION 134

- (Exam Topic 3)

Refer to the exhibit.



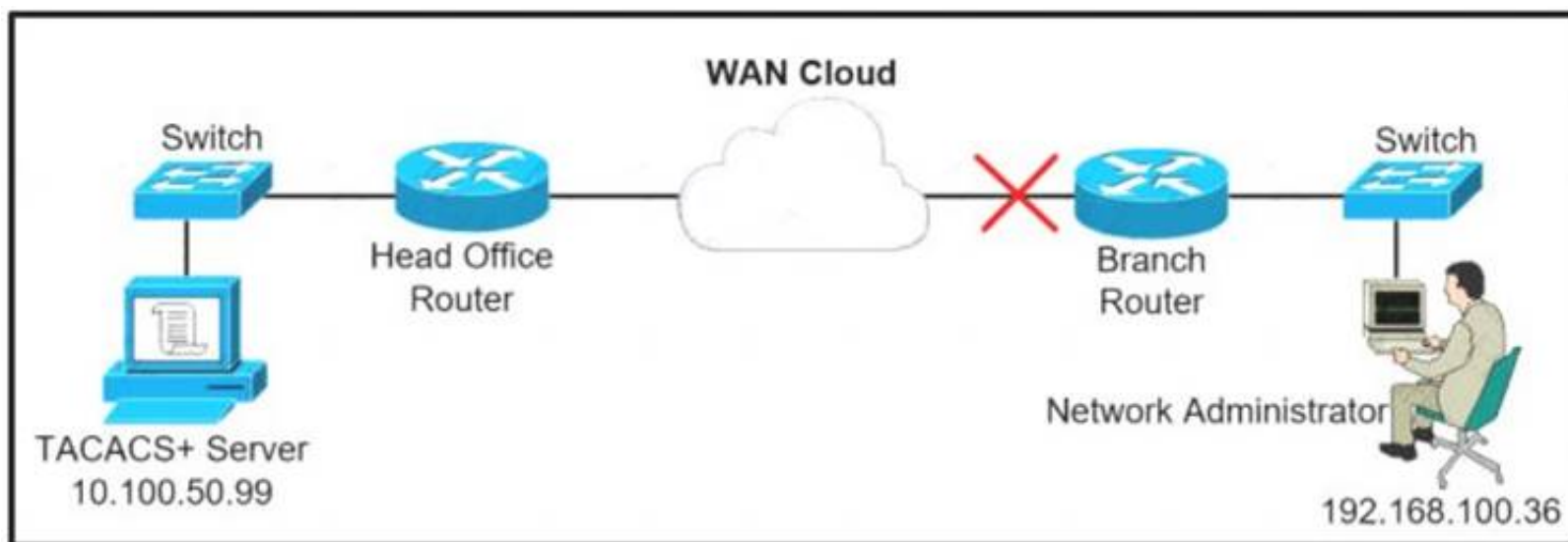
An engineer configured NetFlow on R1, but the NMS server cannot see the flow from ethernet 0/0 of R1. Which configuration resolves the issue?

- A. flow monitor Flowmonitor1 source Ethernet0/0
- B. interface Ethernet0/1ip flow monitor Flowmonitor1 input ip flow monitor Flowmonitor1 output
- C. interface Ethernet0/0ip flow monitor Flowmonitor1 input ip flow monitor Flowmonitor1 output
- D. flow exporter FlowAnalyzer1 source Ethernet0/0

Answer: C

#### NEW QUESTION 138

- (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 Cisco123
```

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**

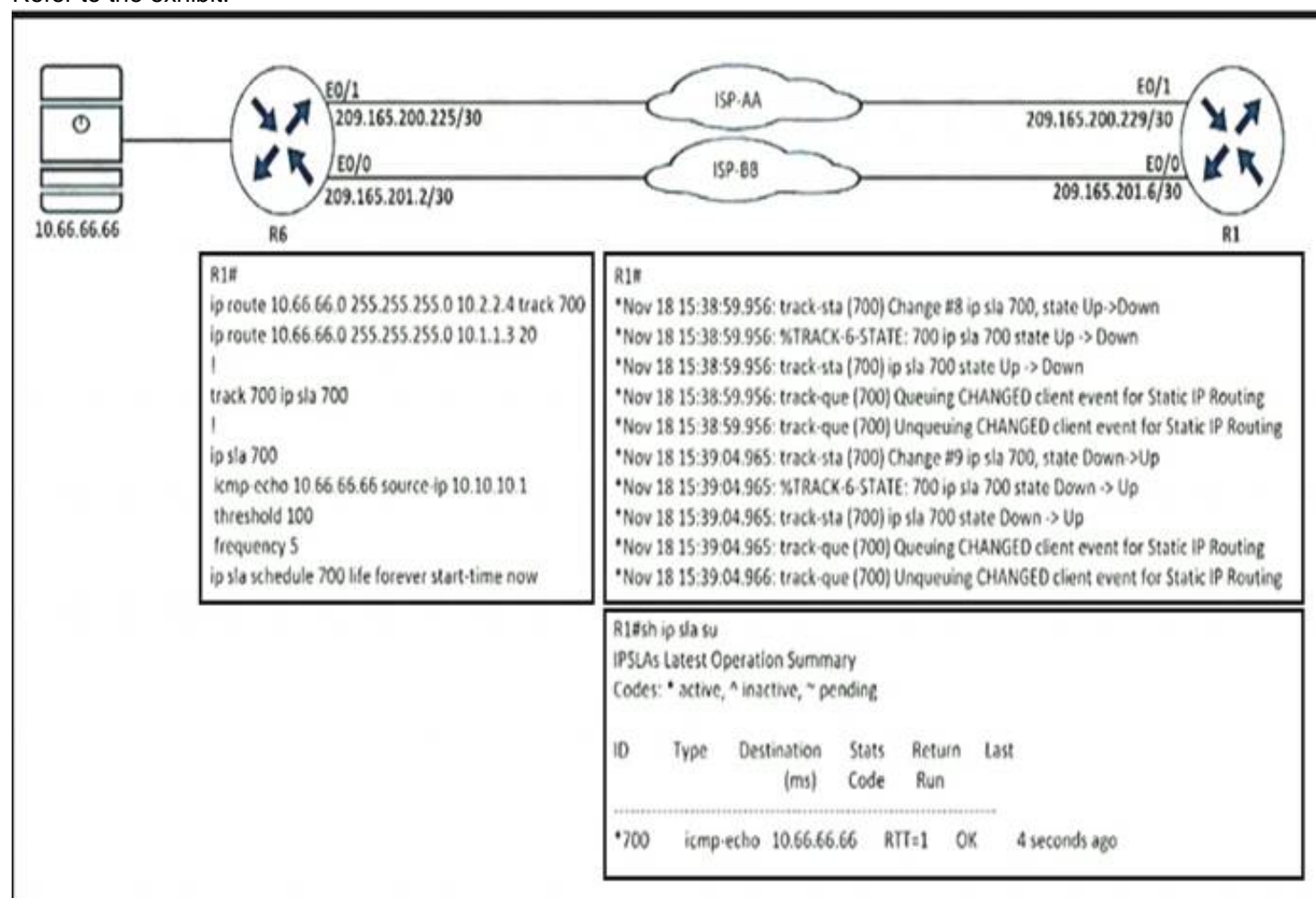
#### Explanation:

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 139

- (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 141

- (Exam Topic 3)



The network administrator configured R1 for Control Plane Policing so that the inbound Telnet traffic is policed to 100 kbps. This policy must not apply to traffic coming in from 10.1.1.1/32 and 172.16.1.1/32. The administrator has configured this:

```
access-list 101 permit tcp host 10.1.1.1 any eq 23
access-list 101 permit tcp host 172.16.1.1 any eq 23
!
class-map CoPP-TELNET
match access-group 101
!
policy-map PM-CoPP
class CoPP-TELNET
police 100000 conform transmit exceed drop
!
control-plane
service-policy input PM-CoPP
```

The network administrator is not getting the desired results. Which set of configurations resolves this issue?

- A. control-planeno service-policy input PM-CoPP!interface Ethernet 0/0service-policy input PM-CoPP
- B. control-planeno service-policy input PM-CoPPservice-policy input PM-CoPP
- C. no access-list 101access-list 101 deny tcp host 10,1,1.1 any eq 23access-list 101 deny tcp host 172,16.1.1 any eq 23 access-list 101 permit ip any any
- D. no access-list 101access-list 101 deny tcp host 10,1.1.1 any eq 23access-list 101 deny tcp host 172.16.1.1 any eq 23 access-list 101 permit ip any any!interface E0/0service-policy input PM-CoPP

**Answer: C**

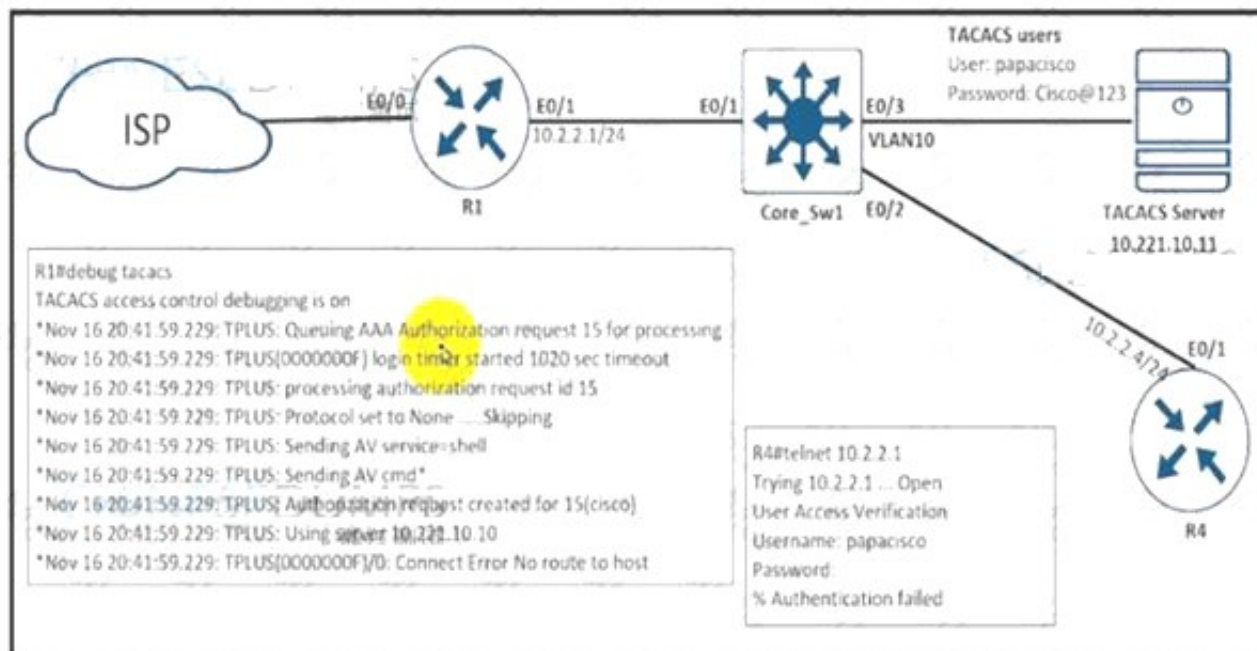
**Explanation:**

Packets that match a deny rule are excluded from that class and cascade to the next class (if one exists) for classification. Therefore if we don't want to CoPP traffic from 10.1.1.1/32 and 172.16.1.1/32, we must "deny" them in the ACL.

**NEW QUESTION 142**

- (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 144**



- (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 145

- (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

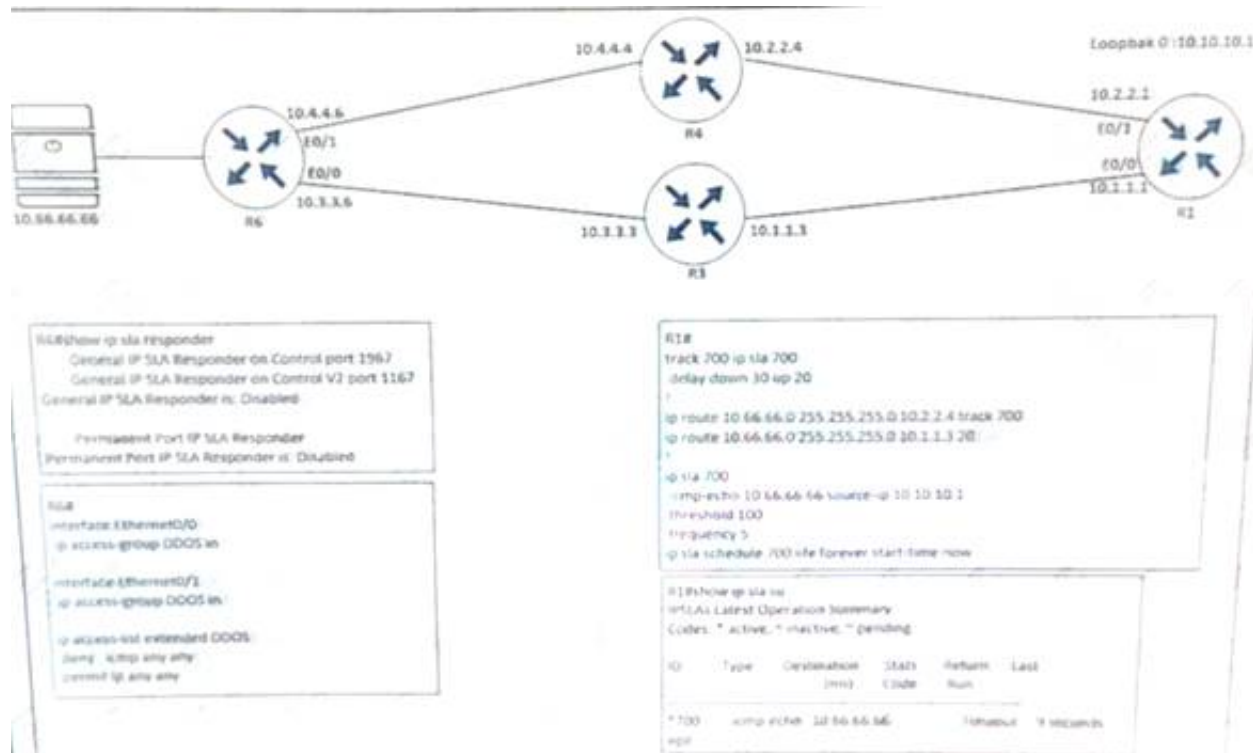
- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

**Answer:** CE

#### NEW QUESTION 146

- (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. R6(config)# ip sla responder
- B. R6(config)# ip sla responder udp-echo ip address 10.10.10.1 port 5000
- C. R6(config)# ip access-list extended DDOSR6(config ext-nac)# 5 permit icmp host 10.66.66.66 host 10.10.10.1
- D. R6(config)# ip access-list extended DDOSR6(config ext-nac)# 5 permit icmp host 10.10.10.1 host 10.66.66.66

**Answer: D**

#### Explanation:

In this IP SLA tracking, we don't need a IP SLA Responder so the command "ip sla responder" on R6 is not necessary. We also notice that the ACL is blocking ICMP packets on both interfaces E0/0 & E0/1 of R6 so we need to allow ICMP from source 10.10.10.1 to destination 10.66.66.66.

#### NEW QUESTION 148

- (Exam Topic 3)

What is a function of an end device configured with DHCPv6 guard?

- A. If it is configured as a server, only prefix assignments are permitted.
- B. If it is configured as a relay agent, only prefix assignments are permitted.
- C. If it is configured as a client, messages are switched regardless of the assigned role.
- D. If it is configured as a client, only DHCP requests are permitted.

**Answer: C**

#### Explanation:

The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized DHCP servers and relay agents. Packets are classified into one of the three DHCP type messages. All client messages are always switched regardless of device role. DHCP server messages are only processed further if the device role is set to server. Further processing of server messages includes DHCP server advertisements (for source validation and server preference) and DHCP server replies (for permitted prefixes). If the device is configured as a DHCP server, all the messages need to be switched, regardless of the device role configuration.

#### NEW QUESTION 149

- (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 150

- (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?

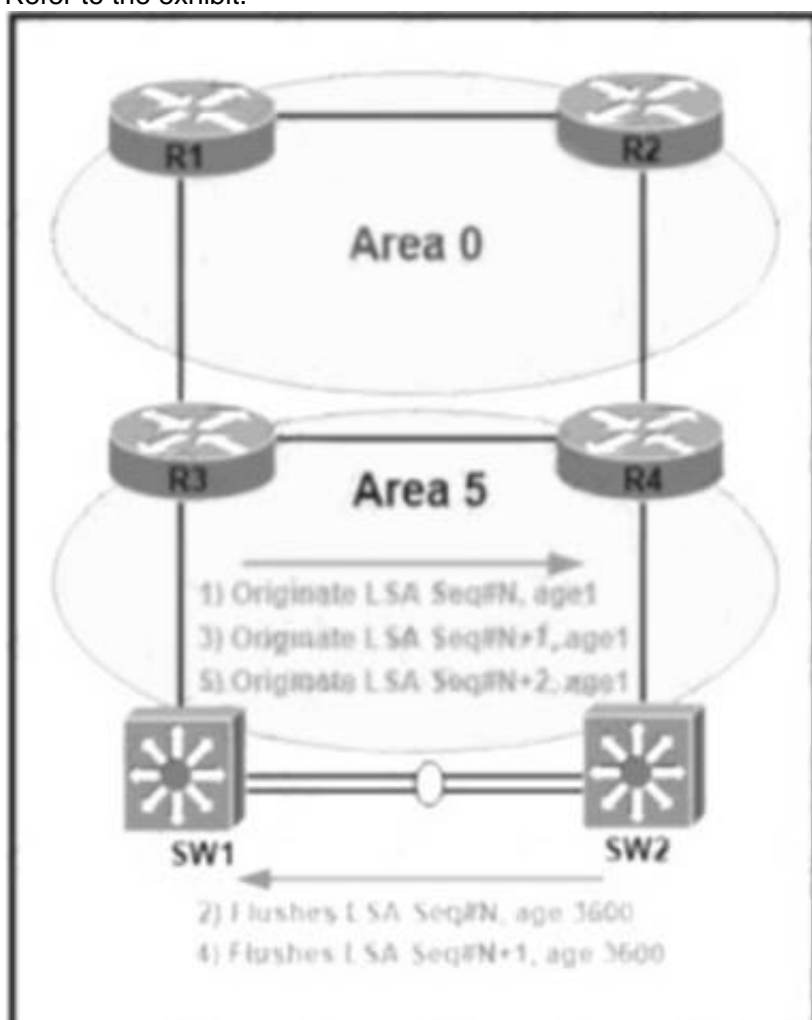
- A. Change the R1 dead timer to 20.
- B. Change the R2 dead timer to 20.
- C. Change the R2 hello timer to 20.
- D. Change the R1 hello timer to 20.

Answer: A

#### NEW QUESTION 152

- (Exam Topic 3)

Refer to the exhibit.



An error message "an OSPF-4-FLOOD\_WAR" is received on SW2 from SW1. SW2 is repeatedly receiving its own link-state advertisement and flushes it from the network. Which action resolves the issue?

- A. Change area 5 to a normal area from a nonstub area
- B. Resolve different subnet mask issue on the link
- C. Configure Layer 3 port channel on interfaces between switches
- D. Resolve duplicate IP address issue in the network

Answer: D

#### NEW QUESTION 157

- (Exam Topic 3)

Refer to the exhibit.



```
R1#sh run | s bgp
router bgp 65001
no synchronization
bgp router-id 10.100.1.50
bgp log-neighbor-changes
network 10.1.1.0 mask 255.255.255.252
network 10.1.1.12 mask 255.255.255.252
network 10.100.1.50 mask 255.255.255.255
timers bgp 20 60
neighbor R2 peer-group
neighbor R4 peer-group
neighbor 10.1.1.2 remote-as 65001
neighbor 10.1.1.2 peer-group R2
neighbor 10.1.1.14 remote-as 65001
neighbor 10.1.1.14 peer-group R4
no auto-summary
```

While troubleshooting a BGP route reflector configuration, an engineer notices that reflected routes are missing from neighboring routers. Which two BGP configurations are needed to resolve the issue? (Choose two)

- A. neighbor 10.1.1.14 route-reflector-client
- B. neighbor R2 route-reflector-client
- C. neighbor 10.1.1.2 allowas-in
- D. neighbor R4 route-reflector-client
- E. neighbor 10.1.1.2 route-reflector-client

**Answer:** AE

#### NEW QUESTION 160

- (Exam Topic 3)

Refer to the exhibit.

```
CPE# show ntp associations

address      ref clock    st  when  poll reach  delay
offset disp
-10.1.255.40 .INIT.      16   64    0  0.000
0.000 15937.
* syn-peer, + selected, + candidate, - outlier, x false-ticker,
- configured

CPE# debug ip icmp
*Feb 20 22:49:32.913: ICMP: dst (10.0.12.1) port unreachable rcv
from 10.1.255.40
*Feb 20 22:50:37.918: ICMP: dst (10.0.12.1) port unreachable rcv
from 10.1.255.40
*Feb 20 22:51:44.951: ICMP: dst (10.0.12.1) port unreachable rcv
from 10.1.255.40
```

An administrator is troubleshooting a time synchronization problem for the router time to another Cisco IOS XE-based device that has recently undergone hardening. Which action resolves the issue?

- A. Allow NTP in the ingress ACL on 10.1.225.40 by permitting UDP destined to port 123.
- B. Ensure that the CPE router has a valid route to 10.1.255.40 for NTP and rectify if not reachable.
- C. NTP service is disabled and must be enabled on 10.1.225.40.
- D. Allow NTP in the ingress ACL on 10.1.255.40 by permitting TCP destined to port 123.

**Answer:** C

#### NEW QUESTION 165

- (Exam Topic 3)

What is the function of BFD?

- A. It provides uniform failure detection regardless of media type.
- B. It creates high CPU utilization on hardware deployments.
- C. It negotiates to the highest version if the neighbor version differs.
- D. It provides uniform failure detection on the same media type.

**Answer:** A

#### NEW QUESTION 167

- (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 171**

- (Exam Topic 3)

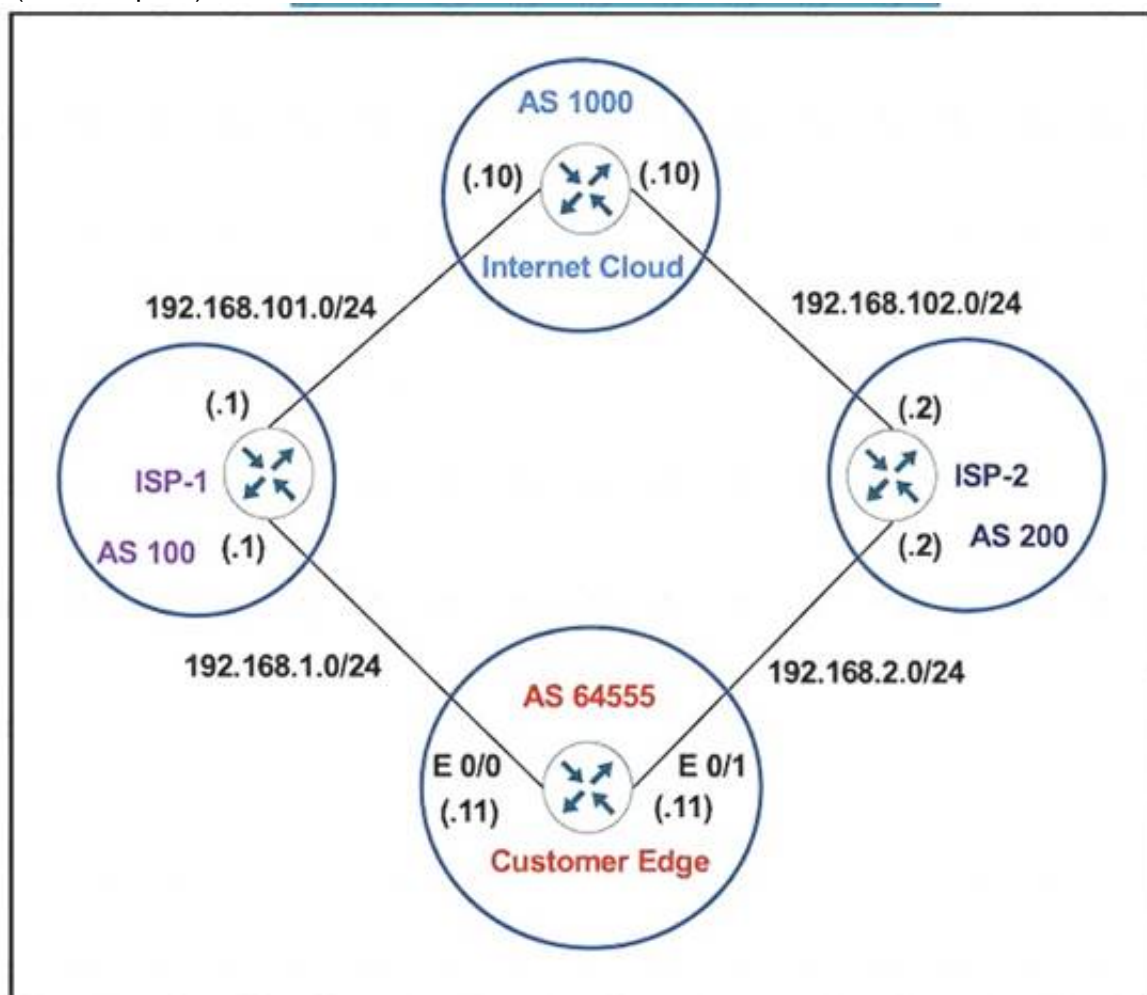
What action is performed for untagged outgoing labels in an MPLS router?

- 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 174**

- (Exam Topic 3)



Refer to the exhibit. The Customer Edge router wants to use AS 100 as the preferred ISP for all external routes and ISP-2 as a backup.

**Customer-Edge**

```
route-map SETAS
set as-path prepend 111
!
router bgp 64555
neighbor 192.168.1.1 remote-as 100
neighbor 192.168.2.2 remote-as 200
neighbor 192.168.2.2 route-map SETAS in
```

After this configuration, all the backup routes have disappeared from the BGP table on the Customer Edge router. Which set of configurations resolves the issue on the Customer Edge router?

A)

```
route-map SETAS
set as-path prepend 111
!
router bgp 64555
neighbor 192.168.2.2 remote-as 100
neighbor 192.168.1.1 remote-as 200
neighbor 192.168.1.1 route-map SETAS in
```

B)

```
route-map SETAS
set as-path prepend 200
!
router bgp 64555
neighbor 192.168.1.1 remote-as 100
neighbor 192.168.2.2 remote-as 200
neighbor 192.168.2.2 route-map SETAS in
```

C)

```
route-map SETAS
set as-path prepend 200
!
router bgp 64555
neighbor 192.168.1.1 remote-as 100
neighbor 192.168.2.2 remote-as 200
neighbor 192.168.2.2 route-map SETAS out
```

D)

```
route-map SETAS
set as-path prepend 111
!
router bgp 64555
neighbor 192.168.1.1 remote-as 100
neighbor 192.168.2.2 remote-as 200
neighbor 192.168.2.2 route-map SETAS out
```

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

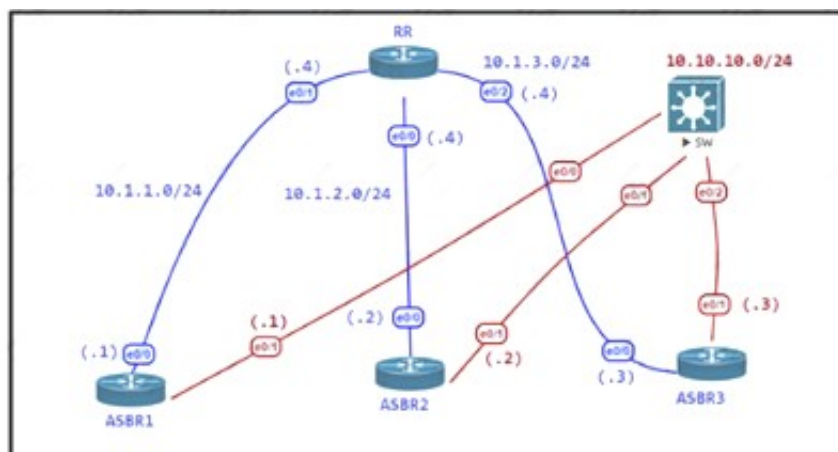
**Answer:** C

#### NEW QUESTION 179

- (Exam Topic 3)

Exhibits:





#### RR

```
router bgp 100
  neighbor 10.1.1.1 remote-as 100
  neighbor 10.1.2.2 remote-as 100
  neighbor 10.1.3.3 remote-as 100
```

#### ASBR2

```
router bgp 100
  neighbor 10.1.1.4 remote-as 100
```

#### ASBR2

```
router bgp 100
  neighbor 10.1.1.4 remote-as 100
```

#### ASBR3

```
router bgp 100
  neighbor 10.1.2.4 remote-as 100
```

#### ASBR4

```
router bgp 100
  neighbor 10.1.3.4 remote-as 100
```

Refer to the exhibit The administrator configured the network devices for end-to-end reachability, but the ASBRs are not propagating routes to each other Which set of configurations resolves this issue?

- ☐ router bgp 100  
neighbor 10.1.1.1 route-reflector-client  
neighbor 10.1.2.2 route-reflector-client  
neighbor 10.1.3.3 route-reflector-client
- ☐ router bgp 100  
neighbor 10.1.1.1 update-source Loopback0  
neighbor 10.1.2.2 update-source Loopback0  
neighbor 10.1.3.3 update-source Loopback0
- ☐ 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 10.1.1.1 ebgp-multihop  
neighbor 10.1.2.2 ebgp-multihop  
neighbor 10.1.3.3 ebgp-multihop

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

Answer: A

#### NEW QUESTION 181

- (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
```

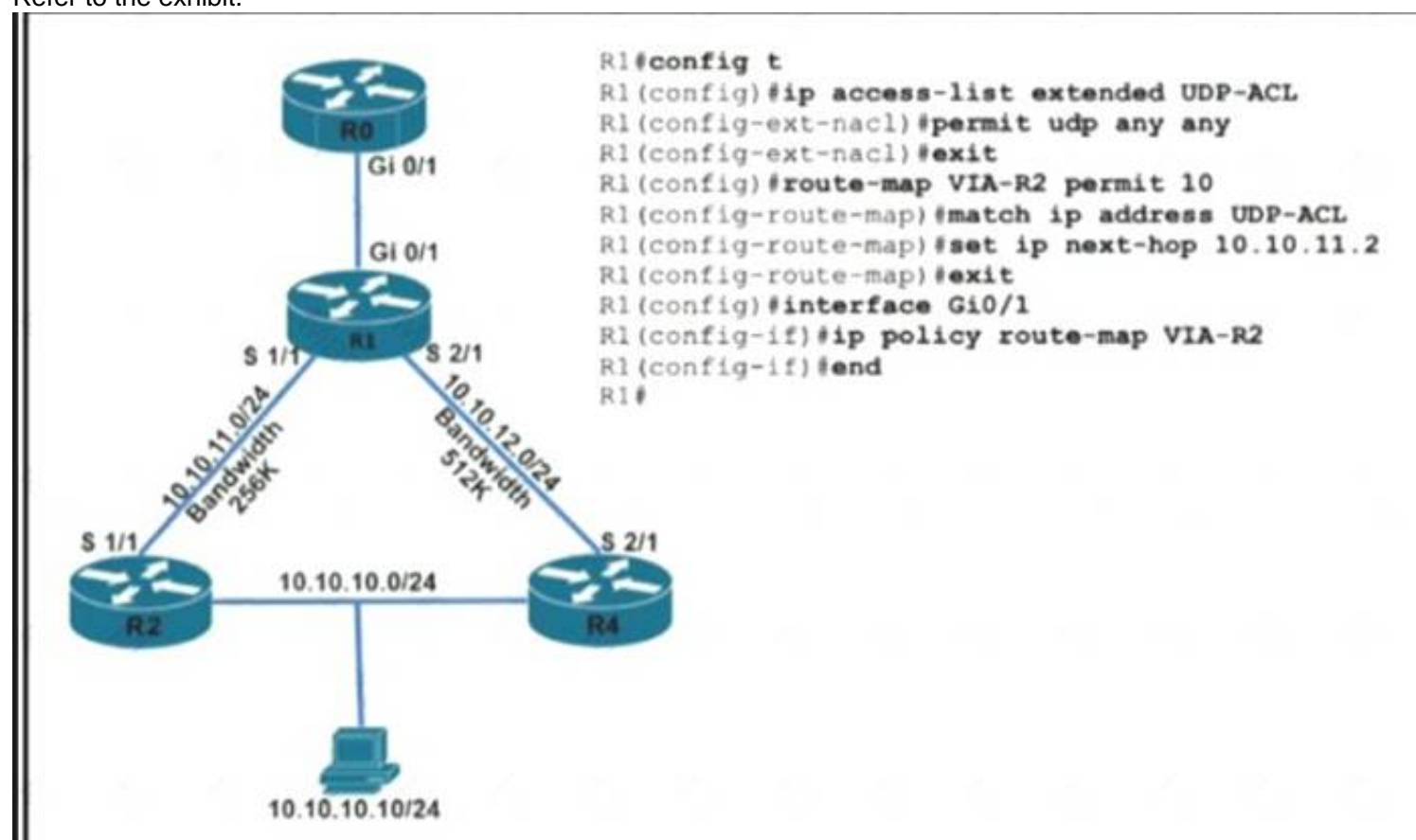
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

#### NEW QUESTION 182

- (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 187

- (Exam Topic 3)

Refer to the exhibit.

```
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.
```

Which command must be configured to make VRF CCNP work?

- A. interface Loopback0 vrf forwarding CCNP
- B. interface Loopback0 ip address 10.1.1.1 255.255.255.0
- C. interface Loopback0 ip address 10.1.1.1 255.255.255.0 vrf forwarding CCNP
- D. interface Loopback0 ip address 10.1.1.1 255.255.255.0 ip vrf forwarding CCNP

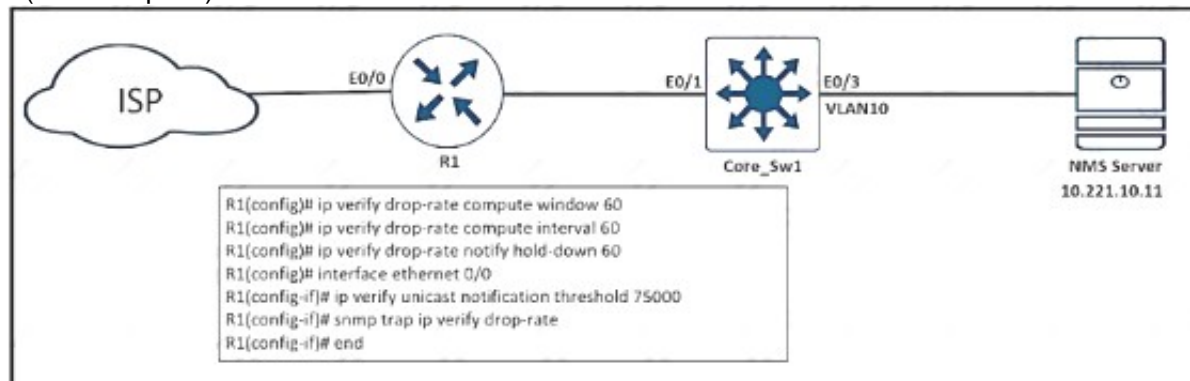
**Answer: B**

**Explanation:**

From the exhibit, we learn that the command “ip address 10.1.1.1 255.255.255.0” has been issued before the command “ip vrf forwarding CCNP”. But the second command removed the IP address configured in the first command so we have to retype the IP address command.

**NEW QUESTION 191**

- (Exam Topic 3)



Refer to the exhibit. An engineer configured SNMP traps to record spoofed packets drop of more than 48000 a minute on the ethernet0/0 interlace. During an IP spoofing attack, the engineer noticed that no notifications have been received by the SNMP server. Which configuration resolves the issue on R1?

- A. ip verify unicast notification threshold 48000
- B. ip verify unicast notification threshold 8000
- C. ip verify unicast notification threshold 800
- D. ip verify unicast notification threshold 80

**Answer: C**

**NEW QUESTION 193**

- (Exam Topic 3)

A customer reports that traffic is not passing on an EIGRP enabled multipoint interface on a router configured as below:

```
interface Serial0/0 no ip address
interface Server0/0/0.9 multipoint ip address 10.1.1.1 255.255.255.248
ip split-horizon eigrp 1
```

Which action resolves the issue?

- A. Enable poison reverse
- B. Enable split horizon
- C. Disable poison reverse
- D. Disable split horizon

**Answer: D**

**NEW QUESTION 194**

- (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 195**



- (Exam Topic 3)

```

100.0.0.0/32 is subnetted, 3 subnets
C 100.1.1.1 is directly connected, Loopback0
D 100.2.2.2 [90/156160] via 10.1.1.2, 00:00:46, FastEthernet0/0
D 100.3.3.3 [90/158720] via 10.1.1.14, 00:00:44, FastEthernet1/0
  [90/158720] via 10.1.1.2, 00:00:44, FastEthernet0/0
10.0.0.0/8 is variably subnetted, 13 subnets, 4 masks
D 10.1.1.8/30 [90/30720] via 10.1.1.14, 00:00:44, FastEthernet1/0
C 10.1.1.12/30 is directly connected, FastEthernet1/0
C 10.1.1.0/30 is directly connected, FastEthernet0/0
D 10.1.1.4/30 [90/30720] via 10.1.1.2, 00:00:45, FastEthernet0/0
C 10.100.1.40/32 is directly connected, Loopback40
D EX 10.1.1.80/29 [170/33280] via 10.1.1.14, 00:00:45, FastEthernet1/0
  [170/33280] via 10.1.1.2, 00:00:45, FastEthernet0/0
C 10.100.1.50/32 is directly connected, Loopback50
C 10.100.1.10/32 is directly connected, Loopback10
S 10.100.1.0/24 is a summary, 00:00:48, Null0
C 10.100.1.30/32 is directly connected, Loopback30
C 10.100.1.20/32 is directly connected, Loopback20
C 10.200.1.0/24 is directly connected, FastEthernet0/1
D EX 10.247.10.0/30 [170/2174976] via 10.1.1.14, 00:00:46, FastEthernet1/0
  [170/2174976] via 10.1.1.2, 00:00:46, FastEthernet0/0

```

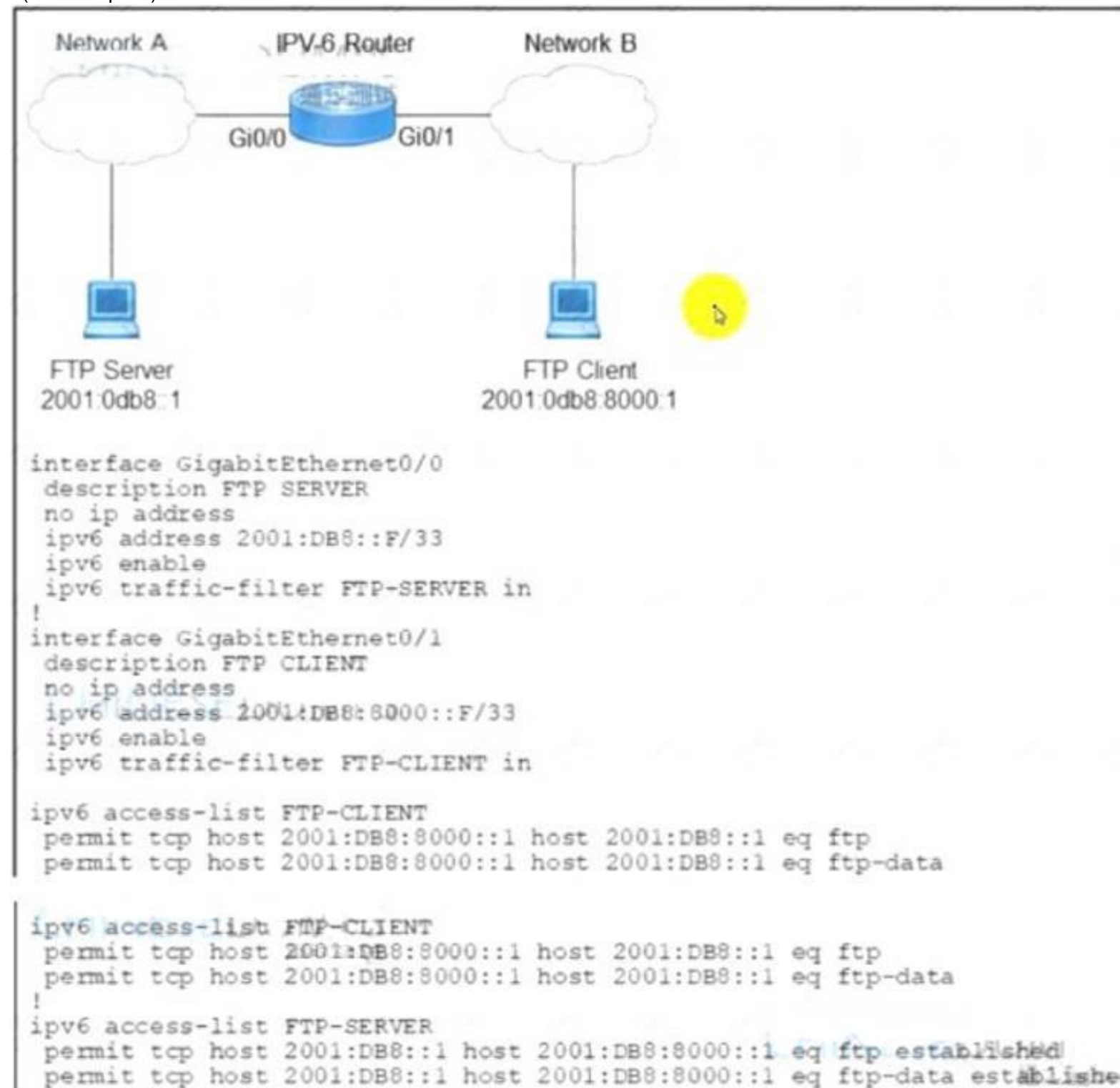
Refer to the exhibit. R1 must advertise all loopback interfaces IP addresses to neighbors, but EIGRP neighbors receive a summary route. Which action resolves the issue?

- A. Redistribute connected routes into EIGRP Enable
- B. EIGRP on loopback Interfaces.
- C. Disable auto summarization on R1.
- D. Remove the 10.100.1.0/24 static route.

Answer: D

#### NEW QUESTION 199

- (Exam Topic 3)



Refer to the exhibit. When an FTP client attempts to use passive FTP to connect to the FTP server, the file transfers fail Which action resolves the issue?

- A. Configure active FTP traffic.
- B. Modify FTP-SERVER access list to remove established at the end.
- C. Modify traffic filter FTP-SERVER in to the outbound direction.
- D. Configure to permit TCP ports higher than 1023.

Answer: D

#### NEW QUESTION 200

- (Exam Topic 3)

Refer to the exhibit.

```
Configuration Output:
aaa new-model
aaa group server tacacs+ admin
server name admin
!
ip tacacs source-interface GigabitEthernet1
aaa authentication login admin group tacacs+ local enable
aaa session-id common
!
tacacs server admin
address ip 10.11.15.6
key 7 01150F165E1C07032D
!
line vty 0 4
login authentication admin

Debug Output:
Oct 22 12:38:57.587: AAA/BIND(0000001A): Bind if
Oct 22 12:38:57.587: AAA/AUTHEN/LOGIN (0000001A): Pick method list 'admin'
Oct 22 12:38:57.587: AAA/AUTHEN/ENABLE(0000001A): Processing request action LOGIN
Oct 22 12:38:57.587: AAA/AUTHEN/ENABLE(0000001A): Done status GET_PASSWORD
Oct 22 12:39:02.327: AAA/AUTHEN/ENABLE(0000001A): Processing request action LOGIN
Oct 22 12:39:02.327: AAA/AUTHEN/ENABLE(0000001A): Done status FAIL - bad password
```

An administrator configured a Cisco router for TACACS authentication, but the router is using the local enable password instead. Which action resolves the issue?

- A. Configure the aaa authentication login admin group admin local enable command instead.
- B. Configure the aaa authentication login admin group tacacs+ local enable none command instead.
- C. Configure the aaa authentication login admin group tacacs+ local if-authenticated command instead.
- D. Configure the aaa authentication login default group admin local if-authenticated command instead.

**Answer: C**

#### NEW QUESTION 204

- (Exam Topic 3)

Which table is used to map the packets in an MPLS LSP that exit from the same interface, via the same next hop, and have the same queuing policies?

- A. RIB
- B. FEC
- C. LDP
- D. CEF

**Answer: B**

#### NEW QUESTION 206

- (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 209

- (Exam Topic 3)

Refer to the exhibits.

# London – "show ip route" output

Gateway of last resort is not set

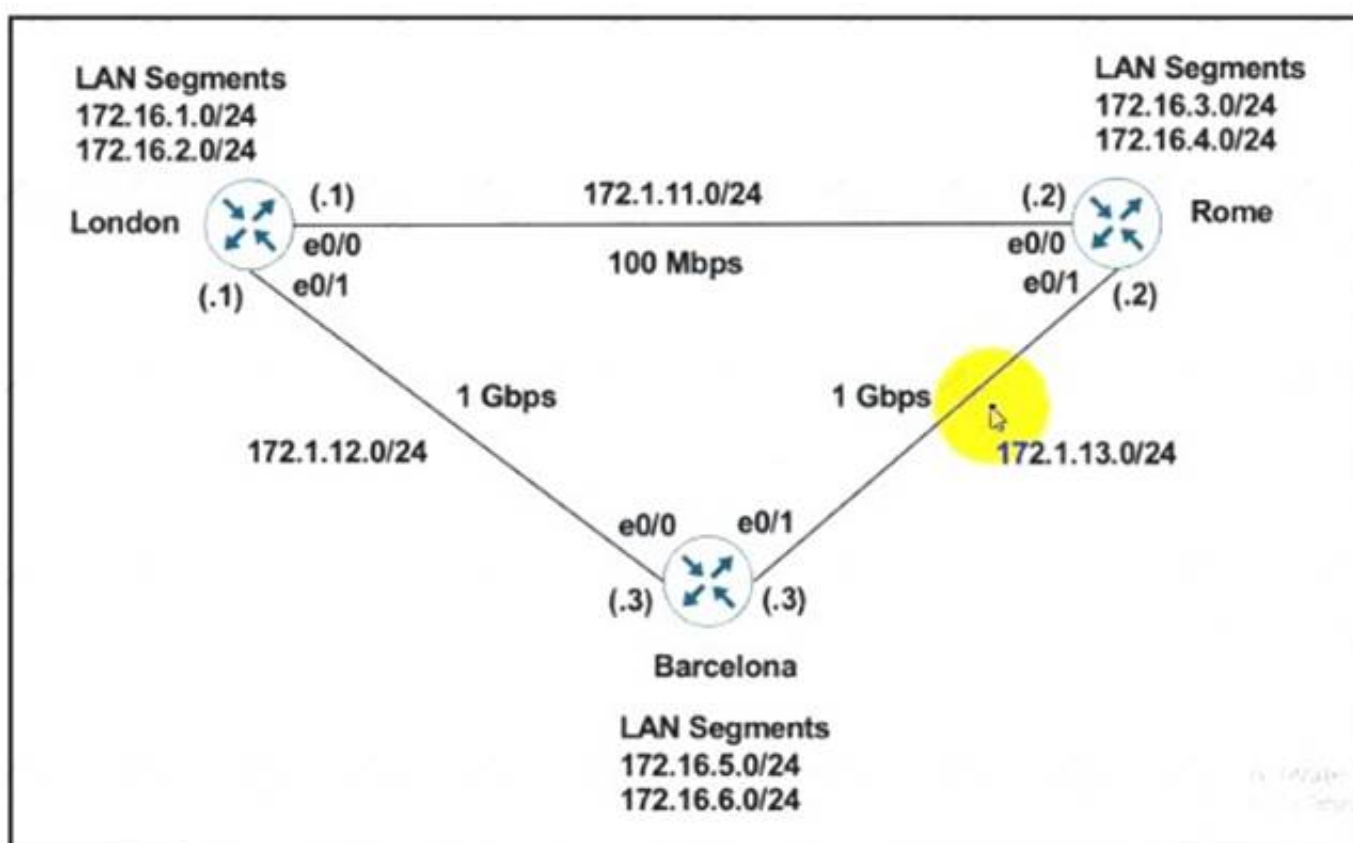
```

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?

- Increase the bandwidth of the link between London and Barcelona
- Use the network statement on London to inject the 172.16.0.0/24 networks into EIGRP.
- Change the administrative distance of RIP to 150
- Use the network statement on Rome to inject the 172.16.0.0/24 networks into EIGRP

Answer: D

## NEW QUESTION 210

- (Exam Topic 3)

Refer to the exhibit.

```

ip vrf CCNP
 rd 1:1
 interface Ethernet1
 ip vrf forwarding CCNP
 ip address 10.1.1.1 255.255.255.252
 !
 interface Ethernet2
 ip vrf forwarding CCNP
 ip address 10.2.2.2 255.255.255.252
    
```

Which configuration enables OSPF for area 0 interfaces to adjacency with a neighboring router with the same VRF?



- A. router ospf 1 vrf CCNP interface Ethernet1 ip ospf 1 area 0.0.0.0 interface Ethernet2 ip ospf 1 area 0.0.0.0
- B. router ospf 1 interface Ethernet1 ip ospf 1 area 0.0.0.0 interface Ethernet2 ip ospf 1 area 0.0.0.0
- C. router ospf 1 vrf CCNP network 10.1.1.1 0.0.0.0 area 0 network 10.2.2.2 0.0.0.0 area 0
- D. router ospf 1 vrf CCNP network 10.0.0.0 0.0.255.255 area 0

**Answer:** C

#### NEW QUESTION 213

- (Exam Topic 3)

Refer to the exhibit.

```
Route-map PBR, permit, sequence 10
Match clauses:
  ip address (access-lists): FILTER_ACL
Set clauses:
  ip next-hop verify-availability 209.165.202.129 1 track 100 [down]
  ip next-hop verify-availability 209.165.202.131 2 track 200 [up]
Policy routing matches: 0 packets, 0 bytes
route-map PBR, deny, sequence 20
Match clauses:
Set clauses:
  ip next-hop 209.165.201.30
Policy routing matches: 275364861 packets, 12200235037 bytes
```

An engineer has configured policy-based routing and applied the configured to the correct interface. How is the configuration applied to the traffic that matches the access list?

- A. It is sent to 209.165.202.131.
- B. It is sent to 209.165.202.129.
- C. It is dropped.
- D. It is forwarded using the routing table lookup.

**Answer:** A

#### Explanation:

The set ip next-hop verify-availability command in route-map configuration mode to configure policy routing to verify the reachability of the next hop of a route map before the router performs policy routing to that next hop. In this question we see track 100 is down so the PBR will not use this next-hop, it will use the second next-hop with track 200 (up).

#### NEW QUESTION 214

- (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-NUL for traffic congestion from source to destination forwarding
- D. PE removes the outer label before sending to the P router.

**Answer:** A

#### NEW QUESTION 216

- (Exam Topic 3)

What are the two prerequisites to enable BFD on Cisco routers? (Choose two)

- A. A supported IP routing protocol must be configured on the participating routers.
- B. OSPF Demand Circuit must run BFD on all participating routers.
- C. ICMP must be allowed on all participating routers.
- D. UDP port 1985 must be allowed on all participating routers.
- E. Cisco Express Forwarding and IP Routing must be enabled on all participating routers.

**Answer:** CE

#### NEW QUESTION 221

- (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/xen-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/xen-3s/mp-te-path-setup-xe-3s-book/mp-te-enhance-xe.html)

#### NEW QUESTION 223

- (Exam Topic 3)

Which feature is used by LDP in the forwarding path within the MPLS cloud?

- A. IP forwarding
- B. TTL
- C. TDP
- D. LSP

**Answer: D**

#### NEW QUESTION 226

- (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 231

- (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 dvmp  
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 232

- (Exam Topic 3)

R1 and R2 are configured as eBGP neighbor, R1 is in AS100 and R2 is in AS200. R2 is advertising these networks to R1:

```
172.16.16.0/20
172.16.3.0/24
172.16.4.0/24
192.168.1.0/24
192.168.2.0/24
172.16.0.0/16
```

The network administrator on R1 must improve convergence by blocking all subnets of 172.16.0.0/16 major network with a mask lower than 23 from coming in, Which set of configurations accomplishes the task on R1?

- A. ip prefix-list PL-1 deny 172.16.0.0/16 le 23 ip prefix-list PL-1 permit 0.0.0.0/0 le 32!router bgp 100neighbor 192.168.100.2 remote-as 200 neighbor 192.168.100.2 prefix-list PL-1 in
- B. ip prefix-list PL-1 deny 172.16.0.0/16 ge 23 ip prefix-list PL-1 permit 0.0.0.0/0 le 32!router bgp 100neighbor 192.168.100.2 remote-as 200 neighbor 192.168.100.2 prefix-list PL-1 in
- C. access-list 1 deny 172.16.0.0 0.0.254.255 access-list 1 permit any!router bgp 100neighbor 192.168.100.2 remote-as 200neighbor 192.168.100.2 distribute-list 1 in
- D. ip prefix-list PL-1 deny 172.16.0.0/16 ip prefix-list PL-1 permit 0.0.0.0/0!router bgp 100neighbor 192.168.100.2 remote-as 200 neighbor 192.168.100.2 prefix-list PL-1 in

**Answer: A**

#### Explanation:

"Blocking all subnets of 172.16.0.0/16 major network with a mask lower than 23 from coming in" would block 172.16.16.0/20.

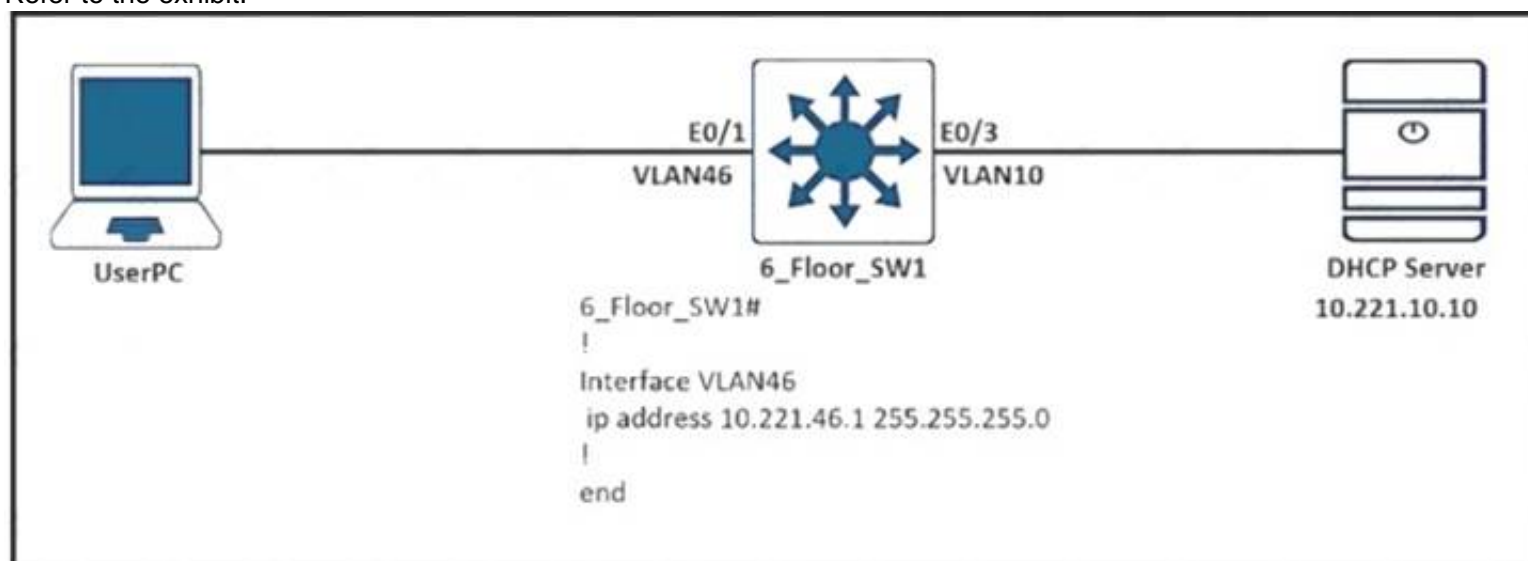
The first prefix-list "ip prefix-list PL-1 deny 172.16.0.0/16 le 23" means "all networks that fall within the 172.16.0.0/16 range AND that have a subnet mask of /23 or less" are denied.

The second prefix-list "ip prefix-list PL-1 permit 0.0.0.0/0 le 32" means allows all other prefixes.

### NEW QUESTION 234

- (Exam Topic 3)

Refer to the exhibit.



Users in VLAN46 cannot get the IP from the DHCP server. Assume that all the parameters are configured properly in VLAN 10 and on the DHCP server Which command on interlace VLAN46 allows users to receive IP from the DHCP server?

- A. ip dhcp-address 10.221.10.10
- B. ip dhcp server 10.221.10.10
- C. ip helper-address 10.221.10.10
- D. ip dhcp relay information trust-all

**Answer: C**

### NEW QUESTION 238

- (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 243

- (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 247

- (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 administrator must configure the router with OSPF for IPv4 and IPv6 networks under a single process. The OSPF adjacencies are not established and did not meet the requirement. Which action resolves the issue?

- A. Replace OSPF process 10 on the interface with OSPF process 1, and configure an additional router ID with IPv6 address.

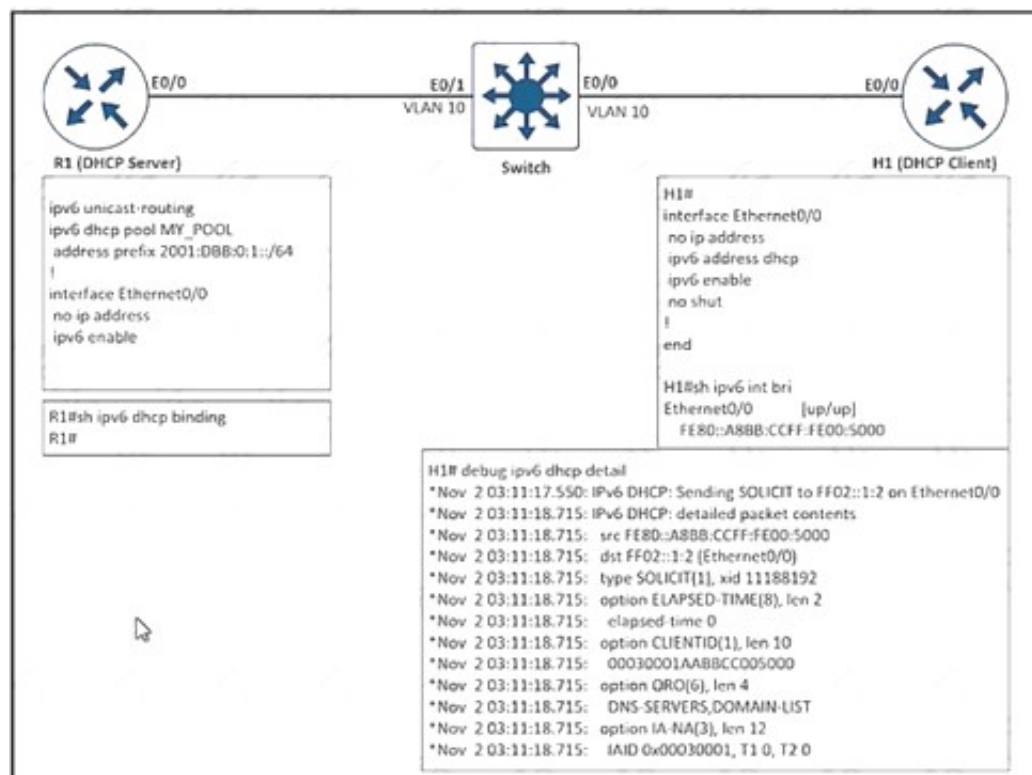
- B. Replace OSPF process 10 on the interface with OSPF process 1, for the VPv6 addressma nd remove process route ID with IPv6 address.
- C. Replace OSPF process 10 on the interface with OSPF process 1, and remove process 10 from the global configuration.
- D. Replace OSPF process 10 on the interface with OSPF process 1 for the IPv4 address, and remove process 10 from the global configuration.

Answer: C

#### NEW QUESTION 249

- (Exam Topic 3)

Refer to the exhibit.



After the network administrator rebuilds the IPv6 DHCP server, clients are not getting the IPv6 address lease. Which action resolves the issue?

- A. Remove FE80 A8BB CCFF FE00 5000 assigned by the IPV6 DHCP server.
- B. Add Ipv6 dhcp sarver MY\_POOL under the interface ethernet 0/0 on H1.
- C. Add Ipv6 dhcp server MY\_POOL under the interface ethernet 0/0 on R1.
- D. Configure FF02::1:2 to discover al IPv6 OHCP cfcents

Answer: C

#### NEW QUESTION 253

- (Exam Topic 3)

Refer to the exhibit.

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

R1#show ip route eigrp | include 10.
D EX 10.0.0.0/8 [170/2665332] via 192.168.10.1, 00:00:10,
Ethernet0/0
```

An engineer applies a prefix-list filter that filters most of the network 10 prefixes instead of allowing them. Which action resolves the issue?

- A. Modify the ip prefix-list EIGRP seq 10 permit 10.0.0.0/8 le 9 command.
- B. Modify the command Modify the Ip prefix-list EIGRP seq 10 permit 10.0.0.0/8 le 32 command.
- C. Modify the Ip prefix-list EIGRP seq 20 permit 0.0.0.0/0 le 32 command.
- D. Modify the ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9 command

Answer: C

#### NEW QUESTION 257

- (Exam Topic 3)

```
Router#show ip bgp vpnv4 rd 1100:1001 10.30.116.0/23
BGP routing table entry for 1100:1001:10.30.116.0/23, version 26765275
Paths: (9 available, best #6, no table)
Advertised to update-groups:
  1      2      3
(65001 64955 65003) 65089, (Received from a RR-client)
 172.16.254.226 (metric 20645) from 172.16.224.236 (172.16.224.236)
  Origin IGP, metric 0, localpref 100, valid, confed-internal
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/362
(65008 64955 65003) 65089
 172.16.254.226 (metric 20645) from 10.131.123.71 (10.131.123.71)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/362
(65001 64955 65003) 65089
 172.16.254.226 (metric 20645) from 172.16.216.253 (172.16.216.253)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/362
(65001 64955 65003) 65089
 172.16.254.226 (metric 20645) from 172.16.216.252 (172.16.216.252)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/362
(64955 65003) 65089
 172.16.254.226 (metric 20645) from 10.77.255.57 (10.77.255.57)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/362
(64955 65003) 65089
 172.16.254.226 (metric 20645) from 10.57.255.11 (10.57.255.11)
  Origin IGP, metric 0, localpref 100, valid, confed-external, best
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/362
```

```
(64955 65003) 65089
 172.16.254.226 (metric 20645) from 172.16.224.253 (172.16.224.253)
  Origin IGP, metric 0, localpref 100, valid, confed-internal
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/362
(65003) 65089
 172.16.254.226 (metric 20645) from 172.16.254.234 (172.16.254.234)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/362
65089, (Received from a RR-client)
 172.16.228.226 (metric 20645) from 172.16.228.226 (172.16.228.226)
  Origin IGP, metric 0, localpref 100, valid, confed-internal
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/278
```

Refer to the exhibit. An engineer configured BGP and wants to select the path from 10.77.255.57 as the best path instead of current best path. Which action resolves the issue?

- A. Configure AS\_PATH prepend for the desired best path
- B. Configure higher MED to select as the best path.
- C. Configure lower LOCAL\_PREF to select as the best path.
- D. Configure AS\_PATH prepend for the current best path

**Answer: D**

#### NEW QUESTION 260

- (Exam Topic 3)

A network administrator successfully established a DMVPN tunnel with one hub and two spokes using EIGRP. One of the requirements was to enable spoke-to-spoke tunnels through the hub router using EIGRP. Which configuration command must the engineer configure to meet the requirement?

- A. no ip eigrp 1 mode multipoint
- B. no ip eigrp 1 split-horizon
- C. no ip eigrp 1 tunnel-redirect
- D. no ip eigrp 1 mode mgre

**Answer: B**

#### NEW QUESTION 261

- (Exam Topic 3)

Which routing protocol is used by the PE router to advertise routes to a CE router without redistribution or static after removing the RD tag from the P router?

- A. IS-IS
- B. OSPF
- C. BGP
- D. MP-BGP

**Answer: C**

#### NEW QUESTION 264



- (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 265

- (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**

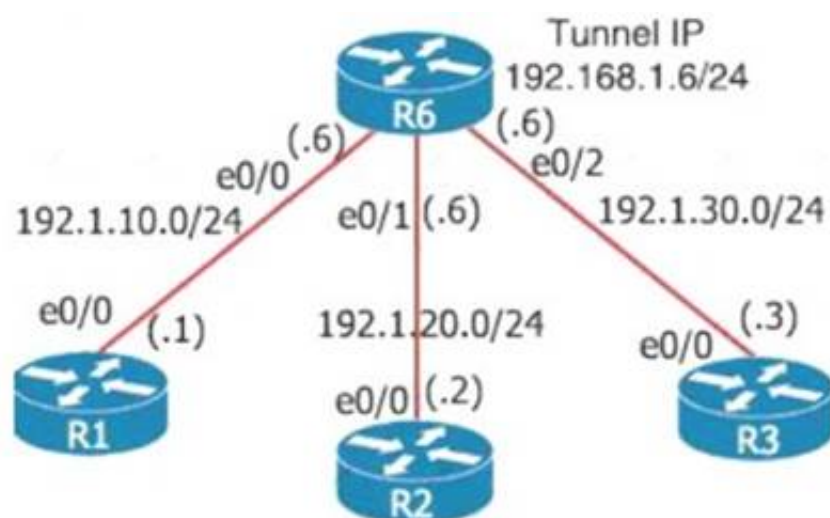
#### Explanation:

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

#### NEW QUESTION 266

- (Exam Topic 3)

Refer to the exhibit.



An engineer must establish multipoint GRE tunnels between hub router R6 and branch routers R1, R2, and R3. Which configuration accomplishes this task on R1?

A)

```
interface Tunnel 1
ip address 192.168.1.1 255.255.255.0
tunnel source e0/1
tunnel mode gre multipoint
ip nhrp nhs 192.168.1.6
ip nhrp map 192.168.1.6 192.1.10.6
```

B)

```
interface Tunnel 1
ip address 192.168.1.1 255.255.255.0
tunnel source e0/1
tunnel mode gre multipoint
ip nhrp network-id 1
ip nhrp nhs 192.168.1.6
ip nhrp map 192.168.1.6 192.1.10.1
ip nhrp map 192.168.1.2 192.1.20.2
ip nhrp map 192.168.1.3 192.1.30.3
```

C)

```
interface Tunnel 1
ip address 192.168.1.1 255.255.255.0
tunnel source e0/0
tunnel mode gre multipoint
ip nhrp nhs 192.168.1.6
ip nhrp map 192.168.1.6 192.1.10.1
ip nhrp map 192.168.1.2 192.1.20.2
ip nhrp map 192.168.1.3 192.1.30.3
```

D)

```
interface Tunnel 1
ip address 192.168.1.1 255.255.255.0
tunnel source e0/0
tunnel mode gre multipoint
ip nhrp network-id 1
ip nhrp nhs 192.168.1.6
ip nhrp map 192.168.1.6 192.1.10.6
```

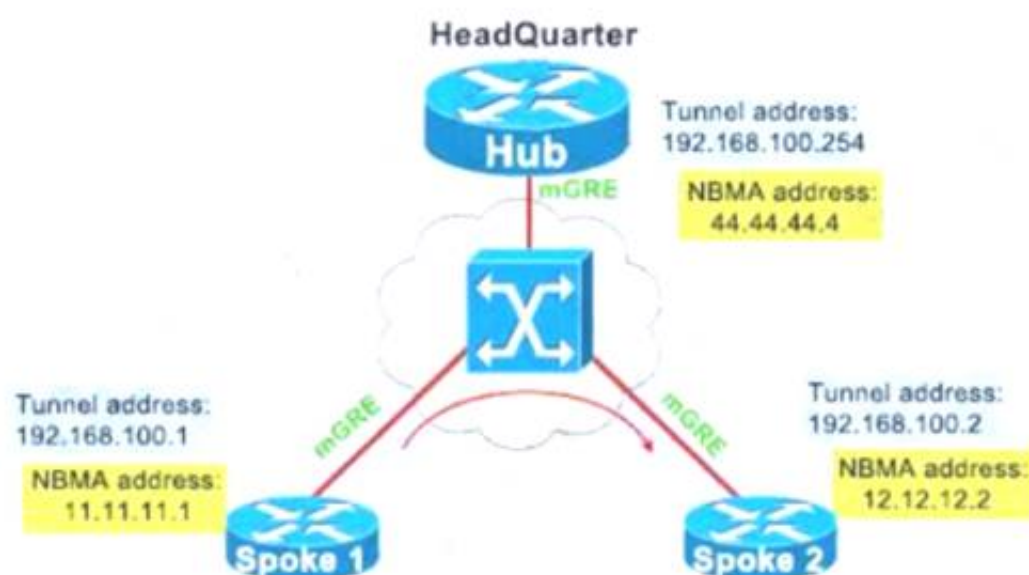
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

#### Explanation:

We have an example of how to configure DMVPN Phase II and we show the configuration here for your reference:

Diagram Description automatically generated



DMVPN Phase II – Dynamic Mapping  
Text Description automatically generated



Hub	Spoke 1	Spoke 2
interface tunnel 1 ip address 192.168.100.254 255.255.255.0 tunnel source 44.44.44.4 tunnel mode gre multipoint ip nhrp network 10	interface tunnel 1 ip address 192.168.100.1 255.255.255.0 tunnel source 11.11.11.1 tunnel mode gre multipoint ip nhrp network 10 ip nhrp map 192.168.100.254 44.44.44.4 ip nhrp nhs 192.168.100.254	interface tunnel 1 ip address 192.168.100.2 255.255.255.0 tunnel source 12.12.12.2 tunnel mode gre multipoint ip nhrp network 10 ip nhrp map 192.168.100.254 44.44.44.4 ip nhrp nhs 192.168.100.254

Note: Although Phase II – Dynamic Mapping is “dynamic” but we still need to add a static entry for the hub because without that entry, the NHRP registration cannot be sent.

#### NEW QUESTION 268

- (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?

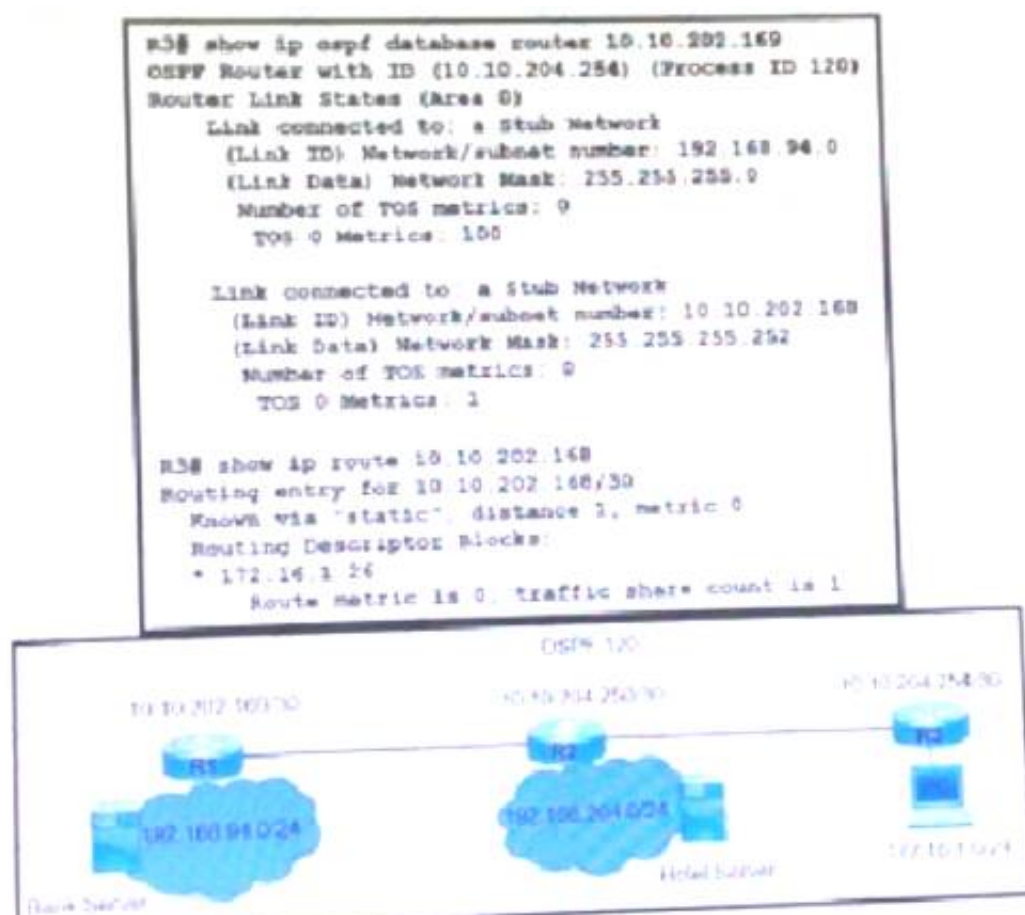
- A. Configure the next hop of 10.20.20.1 in the prefix list DMZ-STATIC
- B. Configure the next-hop interface at the end of the static router for it to get redistributed
- C. Configure a permit 20 statement to the route map to redistribute the static route
- D. Configure the subnets keyword in the redistribution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

Answer: D

#### NEW QUESTION 273

- (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?

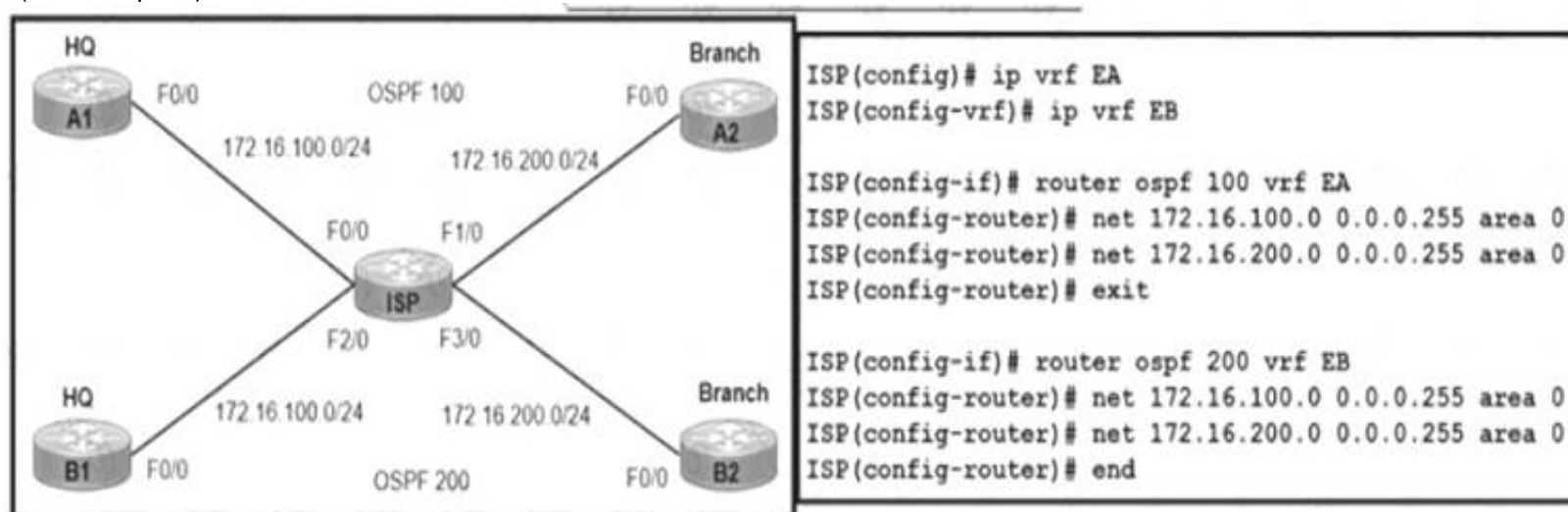
- A. Allow stub network 10.10.202.168/30 on router R3 OSPF.
- B. Decrease the AD to 5 OSPF route 192.168.94.0 on R1.
- C. Increase the AD to 200 of static route 192.168.94.0 on R3.
- D. Configure a reverse route on R1 for PC1 172.16.1.0/24.



Answer: A

### NEW QUESTION 277

- (Exam Topic 3)



Refer to the exhibit. A network engineer is provisioning end-to-end traffic service for two different enterprise networks with these requirements

- > The OSPF process must differ between customers on HQ and Branch office routers, and adjacencies should come up instantly.
- > The enterprise networks are connected with overlapping networks between HQ and a branch office Which configuration meets the requirements for a customer site?

A)

```

ISP(config)#int f3/0
ISP(config-if)#ip vrf forwarding EA
ISP(config-if)#description TO->EA2_Branch
ISP(config-if)#ip address 172.16.200.2 255.255.255.0
ISP(config-if)#no shut
  
```

B)

```

ISP(config)#int f2/0
ISP(config-if)#ip vrf forwarding EA
ISP(config-if)#description TO->EA1_HQ
ISP(config-if)#ip address 172.16.100.2 255.255.255.0
ISP(config-if)#no shut
  
```

C)

```

ISP(config-vrf)#int f0/0
ISP(config-if)#ip vrf forwarding EB
ISP(config-if)#description TO->EB1_HQ
ISP(config-if)#ip add 172.16.100.2 255.255.255.0
ISP(config-if)#no shut
  
```

D)

```

ISP(config-if)#int f1/0
ISP(config-if)#ip vrf forwarding EA
ISP(config-if)#description TO->EA2_Branch
ISP(config-if)#ip add 172.16.200.2 255.255.255.0
ISP(config-if)#no shut
  
```

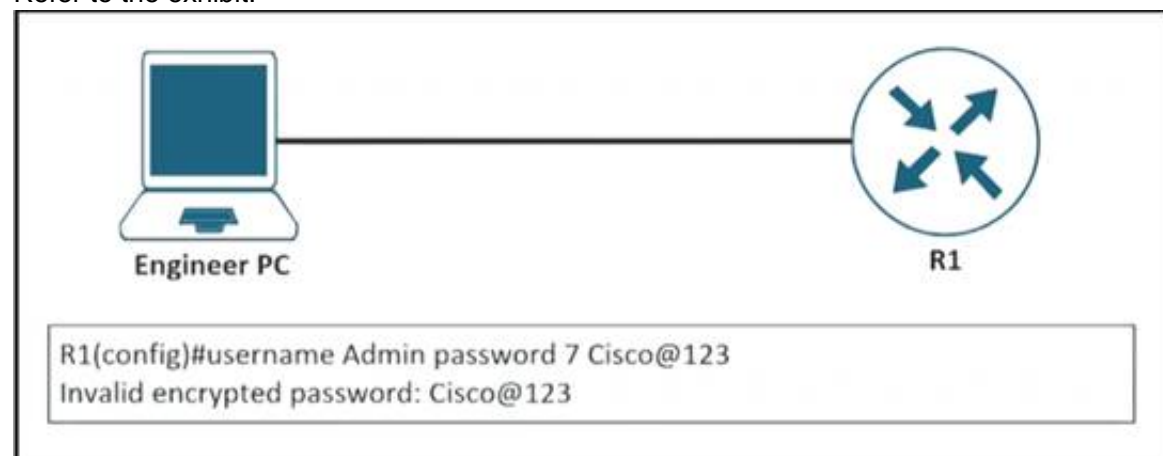
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

### NEW QUESTION 281

- (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 283

- (Exam Topic 3)

Refer to the exhibit.

```
R2(config)# int tun0
*Jun 23 00:42:06.179: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down

R2(config-if)# ip address 192.168.12.2 255.255.255.0
R2(config-if)# tunnel source lo0
R2(config-if)# tunnel destination 10.255.255.1

*Jun 23 00:42:15.845: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to up

R2(config-if)# router eigrp E
R2(config-router)# address-family ipv4 autonomous-system 1
R2(config-router-af)# net 192.168.12.2 0.0.0.0

*Jun 23 00:43:05.730: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.12.1 (Tunnel0) is up: new adjacency
* Jun 23 00:43:05.993: %ADJ-5-PARENT: Midchain parent maintenance
for IP midchain out of Tunnel0 - looped chain attempting to stack
*Jun 23 00:43:15.193: %TUN-5-RECURDOWN: Tunnel0 temporarily
disabled due to recursive routing

*Jun 23 00:43:15.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down
```

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

**Answer:** C

#### Explanation:

In this question we are advertising the tunnel IP address 192.168.12.2 to the other side. When other end receives the EIGRP advertisement, it realizes it can reach the other side of the tunnel via EIGRP. In other words, it reaches the tunnel destination through the tunnel itself -> This causes "recursive routing" error.

Note: In order to avoid this error, do not advertise the tunnel destination IP address on the tunnel interface to other side.

Good recursive routing reference: <https://networklessons.com/cisco/ccie-routing-switching/gretunnel-recursive-routing-error>

#### NEW QUESTION 286

- (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 289

- (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 291**

- (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 292**

- (Exam Topic 3)

```
R2#show policy-map control-plane
Control Plane
Service-policy input: CoPP
Class-map: SSH (match-all)
  29 packets, 2215 bytes
  5 minute offered rate 0000 bps
  Match: access-group 100

Class-map: ANY (match-all)
  46 packets, 3878 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: access-group 199
  drop

Class-map: class-default (match-any)
  41 packets, 5687 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any

R2#show access-list 100
Extended IP access list 100
  10 deny tcp any any eq 22 (14 matches)
  20 permit tcp host 192.168.12.1 any eq 22 (29 matches)
R2#show access-list 199
Extended IP access list 199
  10 permit ip any any (51 matches)
```

Refer to the exhibit. Which action limits the access to R2 from 192.168.12.1?

- A. Swap sequence 10 with sequence 20 in access-list 100.
- B. Modify sequence 20 to permit tcp host 192.168.12.1 eq 22 any to access-list 100
- C. Swap sequence 20 with sequence 10 in access-list 100
- D. Modify sequence 10 to deny tcp any eq 22 any to access-list 100.

**Answer: C**

#### NEW QUESTION 294

- (Exam Topic 3)

```
March 10 19:28:53.254 GMT: %SNMP-3-AUTHFAIL: Authentication
failure for SNMP request from host 10.1.1.1

snmp-server community public RO 15
snmp-server community private RW 16
!
logging snmp-authfail
!
access-list 15 permit 10.1.1.1

access-list 16 permit 10.1.1.2
```

Refer to the exhibit Which action resolves the issue?

- A. Configure host IP address in access-list 16
- B. Configure SNMPv3 on the router
- C. Configure SNMP authentication on the router
- D. Configure a valid SNMP community string

**Answer: D**

#### NEW QUESTION 296

- (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/xr-16/ip6fxe-16-book/ip6-dhcpv6-guard.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xr-16/ip6fxe-16-book/ip6-dhcpv6-guard.html)

#### NEW QUESTION 300

- (Exam Topic 3)

IPv6 is enabled in the infrastructure to support customers with an IPv6 network over WAN and to connect the head office to branch offices in the local network. One of the customers is already running IPv6 and wants to enable IPv6 over the DMVPN network infrastructure between the headend and branch sites. Which configuration command must be applied to establish an mGRE IPv6 tunnel neighborship?

- A. tunnel protection mode ipv6

- B. ipv6 unicast-routing
- C. ipv6 nhrp holdtime 30
- D. tunnel mode gre multipoint ipv6

**Answer:** D

**Explanation:**

The command "tunnel mode gre multipoint ipv" sets the encapsulation mode of the tunnel to mGRE IPv6.

**NEW QUESTION 301**

- (Exam Topic 3)

```
R1#show bgp ipv6 unicast 2001:db8::1/128
BGP routing table entry for 2001:db8::1/128, version 3
Paths: (1 available, best #1, table Global-IPv6-Table)
Not advertised to any peer
Local
2001:db8:33:33::33 (metric 128) from 2001:db8:11:11::11 (1.1.1.1)
Origin IGP, metric 0, localpref 100, valid, internal, best
Originator: 3.3.3.3, Cluster list: 1.1.1.1
```

Refer to the exhibit. An engineer examines the BGP update for the IPv6 prefix 2001:db8::1/128, which should have been summarized into a /64 prefix. Which sequence of actions achieves the summarization?

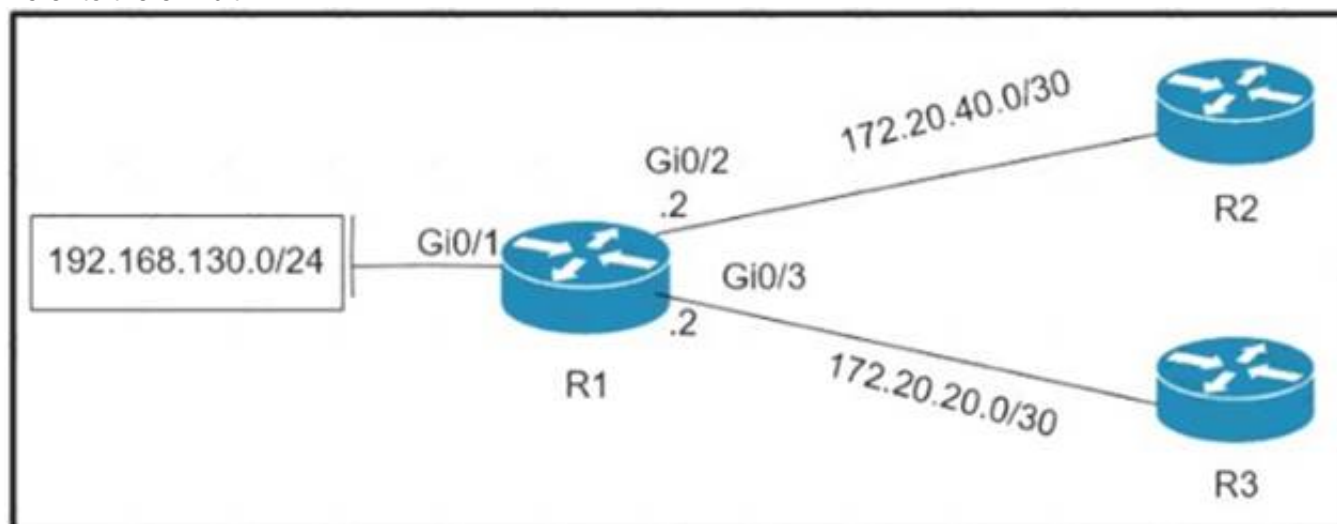
- A. R1 is a route reflector client of a RR with a router ID of 1.1.1.1. and the originator of the prefix has a router ID of 3.3.3.3. Both routers belong to different AS
- B. The prefix is not advertised to any peer and must be advertised using the network statement on R3.
- C. R1 is a route reflector with a router ID of 3.3.3.3. and the originator of the prefix is a route reflector client, which has a router ID of 3.3.3.3. Both routers belong to the same AS Configure an aggregate address on the router with ID 1.1.1.1 for the prefix
- D. R1 is a route reflector with a router ID of 1.1.1.1. and the originator of the prefix is a route reflector client, which has a router ID of 3.3.3.3. Both routers belong to the same AS Configure an aggregate address on the router with ID 1.1.1.1 for the prefix
- E. R1 is a route reflector client of a RR with a router ID of 1.1.1.1. and the originator of the prefix has a router ID of 3.3.3.3. Both routers belong to the same AS
- F. Configure an aggregate address on the router with ID 3.3.3.3 for the prefix.

**Answer:** D

**NEW QUESTION 306**

- (Exam Topic 3)

Refer to the exhibit.



Which policy configuration on R1 forwards any traffic that is sourced from the 192 168 130 0/24 network to R2?

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
```

B)



```
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
```

C)

```
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 307

- (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?

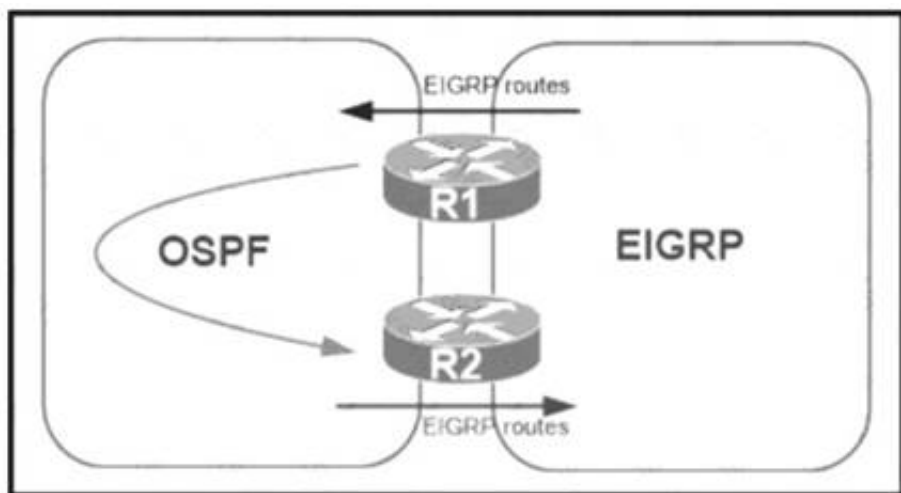
- A. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9.
- B. ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
- C. ip prefix-list EIGRP seq 5 permit 10.0.0.0/8 ge 9 no ip prefix-list EIGRP seq 20 permit 10.0.0.0/8
- D. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9 ip prefix-list EIGRP seq 10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

**Answer:** C

#### NEW QUESTION 310

- (Exam Topic 2)

Refer to the exhibit.



A network administrator configured mutual redistribution on R1 and R2 routers, which caused instability in the network. Which action resolves the issue?

- A. Set a tag in the route map when redistributing EIGRP into OSPF on R1, and match the same tag on R2 to allow when redistributing OSPF into EIGRP.
- B. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the EIGRP routing domain.
- C. Set a tag in the route map when redistributing EIGRP into OSPF on R1, and match the same tag on R2 to deny when redistributing OSPF into EIGRP.
- D. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing into OSPF.

**Answer: C**

**Explanation:**

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

#### NEW QUESTION 315

- (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 317

- (Exam Topic 2)

Refer to the exhibit.

```
router# show running-config
Building configuration
|
<output omitted ---->
|
hostname R1
|
ip domain-name cisco.com
|
crypto key generate rsa modulus 2048
|
username admin privilege 15 secret cisco123
|
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 1 deny any log
|
line vty 0 15
access-class 1 in
login local
|
<output omitted ---->
|
end
```

A user cannot SSH to the router. What action must be taken to resolve this issue?

- A. Configure transport input ssh
- B. Configure transport output ssh
- C. Configure ip ssh version 2
- D. Configure ip ssh source-interface loopback0

**Answer:** A

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0\\_2\\_EX/security/configuration\\_](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_)

#### NEW QUESTION 319

- (Exam Topic 2)

An engineer configured a DHCP server for Cisco IP phones to download its configuration from a TFTP server, but the IP phones failed to load the configuration. What must be configured to resolve the issue?

- A. BOOTP port 67
- B. DHCP option 66
- C. BOOTP port 68
- D. DHCP option 69

**Answer:** B

**Explanation:**

Command	Purpose
<code>dhcpd option 66 ascii server_name</code>	Provides the IP address or name of a TFTP server for option 66.
<b>Example:</b> <pre>hostname(config)# dhcpd option 66 ascii exampleserver</pre>	

DHCP options 3, 66, and 150 are used to configure Cisco IP Phones. Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information. + DHCP option 150 provides the IP addresses of a list of TFTP servers. + DHCP option 66 gives the IP address or the hostname of a single TFTP server.

Reference:

[http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa\\_84\\_cli\\_config/basic\\_dhcp.pdf](http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/basic_dhcp.pdf)

#### NEW QUESTION 321

- (Exam Topic 2)

Refer to the exhibit.

<b>Router# show ip route</b>					
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
<b>Router# show ip bgp</b>					
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 323

- (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 324

- (Exam Topic 2)

Refer to Exhibit.

```
HQ_R2 9100
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.2 track 1
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.6 5
!
BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.6
BRANCH(config-ip-sla)# timeout 200
BRANCH(config-ip-sla)# frequency 5
!
BRANCH(config)# ip sla schedule 1 life forever start-time now
!
BRANCH(config)# track 1 ip sla 1 reachability
```

Traffic from the branch network should route through HQ R1 unless the path is unavailable. An engineer tests this functionality by shutting down interface on the BRANCH router toward HQ\_R1 router but 192.168.20.0/24 is no longer reachable from the branch router. Which set of configurations resolves the issue?

- A. HQ\_R1(config)# ip sla responderHQ\_R1(config)# ip sla responder icmp-echo 172.16.35.2
- B. BRANCH(config)# ip sla 1BRANCH(config-ip-sla)# icmp-echo 172.16.35.1
- C. HQ\_R2(config)# ip sla responderHQ\_R2(config)# ip sla responder icmp-echo 172.16.35.5
- D. BRANCH(config)# ip sla 1BRANCH(config-ip-sla)# icmp-echo 172.16.35.2

**Answer:** D

**Explanation:**

In the configuration above, the engineer has made a mistake as he was tracking 172.16.35.6 (the backup path) instead of tracking the main path (172.16.35.2). Therefore, when he shut down the main path, the track 1 was still up so traffic still went through the main path -> it failed. To fix this issue, we just need to correct the tracking interface of the main path.

**NEW QUESTION 327**

- (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 in 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 in the output direction

**Answer:** B

**NEW QUESTION 329**

- (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 330**

- (Exam Topic 2)

Refer to the exhibit.

```

R1
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
router eigrp 100
 no auto-summary
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.2 FastEthernet0/0

R2
interface Loopback0
 ip address 172.16.2.2 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0
router eigrp 100
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.1 FastEthernet0/0
 passive-interface FastEthernet0/0

```

R1 and R2 cannot establish an EIGRP adjacency. Which action establishes EIGRP adjacency?

- A. Remove the current autonomous system number on one of the routers and change to a different value.
- B. Remove the passive-interface command from the R2 configuration so that it matches the R1 configuration.
- C. Add the no auto-summary command to the R2 configuration so that it matches the R1 configuration.
- D. Add the passive-interface command to the R1 configuration so that it matches the R2 configuration.

**Answer: B**

### NEW QUESTION 333

- (Exam Topic 2)

Refer to the exhibit.

```

*Jun 24 08:54:51.530: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:52.525: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*Jun 24 08:54:52.528: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:53.215: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:54.998: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 24 08:54:55.006: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to UP
*Jun 24 08:54:55.998: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

```

R1 is connected with R2 via GigabitEthernet0/0, and R2 cannot ping R1. What action will fix the issue?

- A. Fix route dampening configured on the router.
- B. Replace the SFP module because it is not supported.
- C. Fix IP Event Dampening configured on the interface.
- D. Correct the IP SLA probe that failed.

**Answer: C**

### Explanation:

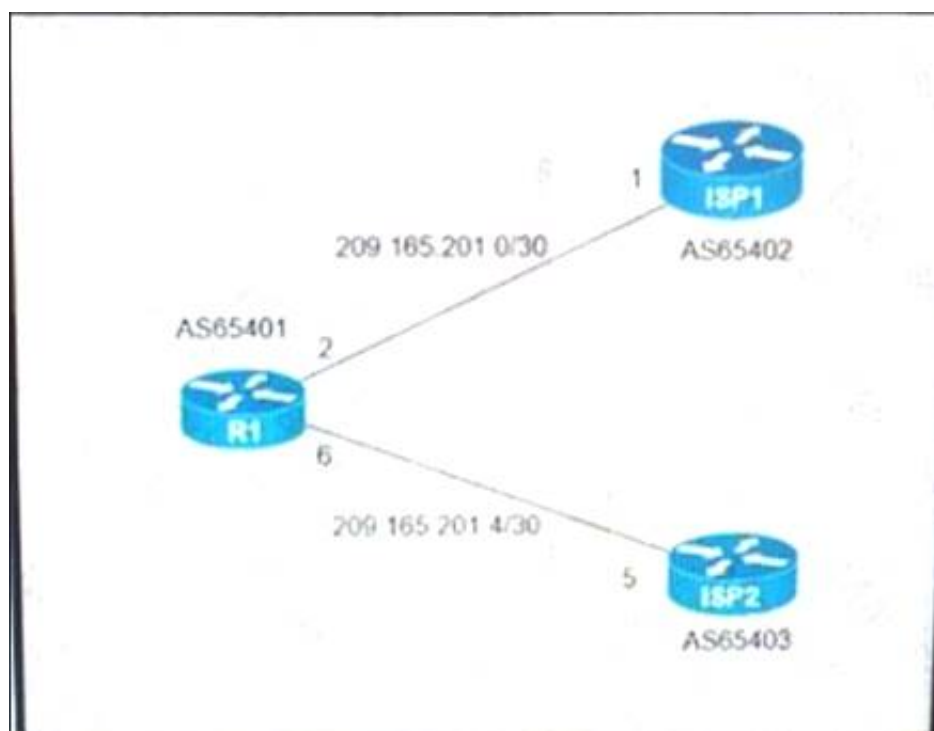
The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping.

### NEW QUESTION 335

- (Exam Topic 2)

Refer to the exhibit.





```

R1#
interface GigabitEthernet0/0
 ip address 209.165.201.2 255.255.255.252
!
interface GigabitEthernet0/1
 ip address 209.165.201.6 255.255.255.252
!
router bgp 65401
  bgp log-neighbor-changes
  redistribute static
  neighbor 209.165.201.1 remote-as 65402
  neighbor 209.165.201.5 remote-as 65403
!
ip route 209.165.200.224 255.255.255.224 Null0
ip route 209.165.202.128 255.255.255.224 Null0
!
  
```

A company with autonomous system number AS65401 has obtained IP address block 209.165.200.224/27 from ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer at ISP1 reports they are receiving ISP2 routes from AS65401. Which configuration on R1 resolves the issue?

A)

```

access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
  neighbor 209.165.201.1 distribute-list 10 out
  
```

B)

```

access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
  neighbor 209.165.201.1 distribute-list 10 in
  
```

C)

```

ip route 209.165.200.224 255.255.255.224 209.165.201.1
ip route 209.165.202.128 255.255.255.224 209.165.201.5
  
```

D)

```

ip route 0.0.0.0 0.0.0.0 209.165.201.1
ip route 0.0.0.0 0.0.0.0 100 209.165.201.5
  
```

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

**Answer:** A

**Explanation:**

<https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/23675-27.html>

**NEW QUESTION 337**

- (Exam Topic 2)

```

Ipv6 unicast-routing
!
Router ospfv3 4
  Router-id 192.168.1.1
!
Interface E 0/0
  Ipv6 enable
  Ip address 10.1.1.1 255.255.255.0
  Ospfv3 4 area 0 ipv4
  No shut
!
Interface Loopback0
  Ipv6 enable
  Ipv4 172.16.1.1 255.255.255.0
  Ospfv3 4 area 0 ipv4

```

Refer to the exhibit. The network administrator configured the branch router for IPv6 on the E 0/0 interface. The neighboring router is fully configured to meet requirements, but the neighbor relationship is not coming up. Which action fixes the problem on the branch router to bring the IPv6 neighbors up?

- A. Enable the IPv4 address family under the E 0/0 interface by using the address-family ipv4 unicast command
- B. Disable IPv6 on the E 0/0 interface using the no ipv6 enable command
- C. Enable the IPv4 address family under the router ospfv3 4 process by using the address-family ipv4 unicast command
- D. Disable OSPF for IPv4 using the no ospfv3 4 area 0 ipv4 command under the E 0/0 interface.

**Answer:** C

**Explanation:**

Once again, Cisco changed the IOS configuration commands required for OSPFv3 configuration. The new OSPFv3 configuration uses the “ospfv3” keyword instead of the earlier “ipv6 router ospf” routing process command and “ipv6 ospf” interface commands.

The Open Shortest Path First version 3 (OSPFv3) address families feature enables both IPv4 and IPv6 unicast traffic to be supported. With this feature, users may have two processes per interface, but only one process per address family (AF).

**NEW QUESTION 338**

- (Exam Topic 2)

How does an MPLS Layer 3 VPN function?

- A. set of sites use multiprotocol BGP at the customer site for aggregation
- B. multiple customer sites interconnect through service provider network to create secure tunnels between customer edge devices
- C. set of sites interconnect privately over the Internet for security
- D. multiple customer sites interconnect through a service provider network using customer edge to provider edge connectivity

**Answer:** D

**Explanation:**

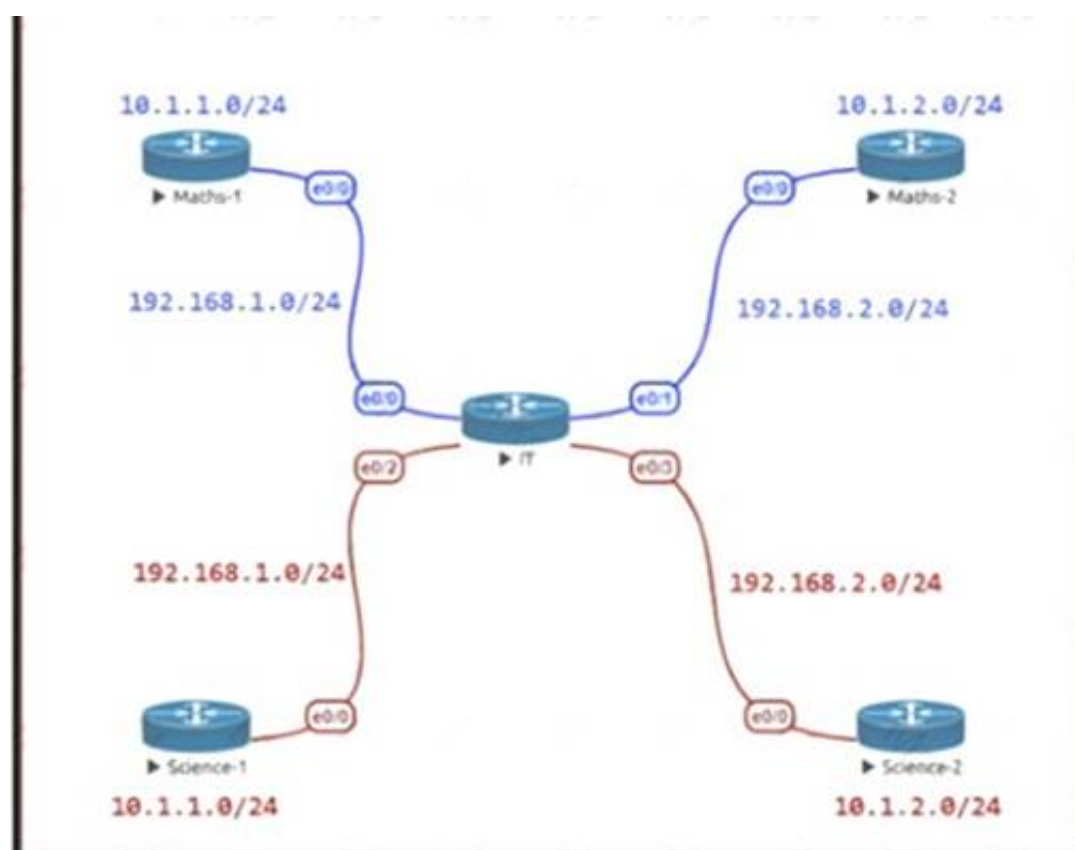
A Multiprotocol Label Switching (MPLS) Layer 3 Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers. Reference:

[https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-5/lxvpn/configuration/guide/b-l3vpn-cg-asr9000-65x/b-l3vpn-cg-asr9000-65x\\_chapter\\_010.pdf](https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-5/lxvpn/configuration/guide/b-l3vpn-cg-asr9000-65x/b-l3vpn-cg-asr9000-65x_chapter_010.pdf)

**NEW QUESTION 343**

- (Exam Topic 2)

Refer to the exhibit.



The Math and Science departments connect through the corporate. IT router but users in the Math department must not be able to reach the Science department and vice versa Which configuration accomplishes this task?

- A. vrf definition Science interface E 0/2 ip address 192.168.1.1 255.255.255.0 no shut interface E 0/3 ip address 192.168.2.1 255.255.255.0 no shut
- B. vrf definition Science address-family ipv4 ! interface E 0/2 ip address 192.168.1.1 255.255.255.0 vrf forwarding Science no shut ! interface E 0/3 ip address 192.168.2.1 255.255.255.0 vrf forwarding Science no shut
- C. vrf definition Science address-family ipv4 ! interface E 0/2 ip address 192.168.1.1 255.255.255.0 no shut ! interface E 0/3 ip address 192.168.2.1 255.255.255.0 no shut
- D. vrf definition Science address-family ipv4 ! interface E 0/2 vrf forwarding Science ip address 192.168.1.1 255.255.255.0 no shut ! interface E 0/3 vrf forwarding Science ip address 192.168.2.1

Answer: D

#### NEW QUESTION 344

- (Exam Topic 2)

What does the PE router convert the Ipv4 prefix to within an MPLS VPN?

- A. VPN-IPv4 prefix combined with the 64-bit route distinguisher
- B. 48-bit route combining the IP and PE router-id
- C. prefix that combines the ASN, PE router-id, and IP prefix
- D. eBGP path association between the PE and CE sessions

Answer: A

#### Explanation:

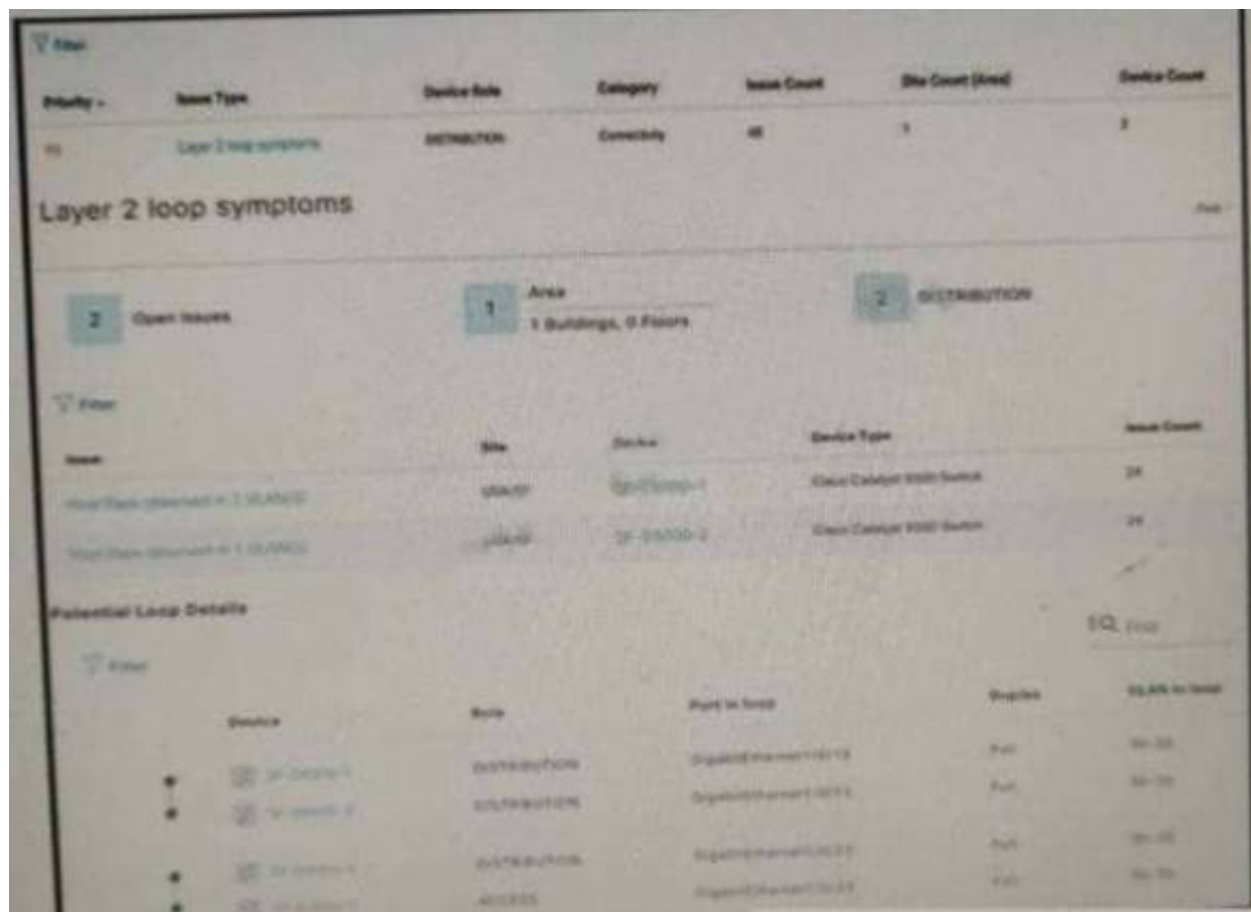
The IP prefix is a member of the IPv4 address family. After the PE device learns the IP prefix, the PE converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher (RD). The generated prefix is a member of the VPN-IPv4 address family. It uniquely identifies the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses. The route distinguisher used to generate the VPN-IPv4 prefix is specified by a configuration command associated with the virtual routing and forwarding (VRF) instance on the PE device.

#### NEW QUESTION 345

- (Exam Topic 2)

Refer to the exhibit.





```
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 30-33
 switchport mode trunk
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 30-33
 switchport mode trunk
```

An engineer identifier a Layer 2 loop using DNAC. Which command fixes the problem in the SF-D9300-1 switch?

- A. no spanning-tree uplinkfast
- B. spanning-tree loopguard default
- C. spanning-tree backbonesfast
- D. spanning-tree portfast bpduguard

**Answer:** D

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dnacenter/tech\\_notes/b\\_dnac\\_sda\\_lan\\_automation\\_deployment.html](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dnacenter/tech_notes/b_dnac_sda_lan_automation_deployment.html)

#### NEW QUESTION 347

- (Exam Topic 2)

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

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

**Answer:** BC

**Explanation:**

Reference:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch\\_cef/configuration/xs-3s/isw-cef-xe-3s-book/isw-cef](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/xs-3s/isw-cef-xe-3s-book/isw-cef)

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

#### NEW QUESTION 351

- (Exam Topic 2)

Refer to the exhibit.

Loopback1: 100A:0:100C::1/64  
Loopback2: 200A:0:200C::1/64  
Loopback3: 300A:0:300C::1/64  
Loopback4: 400A:0:400C::1/64

**B2B Network**

R1 E0/0  
AB01:2011:7:100::1/64

**BGP AS 6501**

**Partner**

Loopback1: 1001:ABC:2011:7::1/64  
Loopback2: 2001:ABC:2011:7::1/64

R3 E0/1  
AB01:2011:7:100::3/64

```

R1#sh bgp ipv6 sum
BGP router identifier 1.1.1.1, local AS number 6501
BGP table version is 1, main routing table version 1

Neighbor          V    AS  MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
AB01:2011:7:100::3 4   6502    0      0       1    0  0   never      Idle

R1#debug ip bgp all
* Nov 8 17:22:11.223: BGP: AB01:2011:7:100::3 active went from Idle to Active
* Nov 8 17:22:11.223: BGP: AB01:2011:7:100::3 open active, local address AB01:2011:7:100::1
* Nov 8 17:22:11.224: BGP: AB01:2011:7:100::3 open failed: Connection refused by remote host
* Nov 8 17:22:11.224: BGP: AB01:2011:7:100::3 Active open failed - tcb is not available, open
active delayed 11264 ms (35000ms max, 60% jitter)
* Nov 8 17:22:11.224: BGP: ses global AB01:2011:7:100::3 (0xC3F49FF0:0) act Reset (Active open failed)
* Nov 8 17:22:11.232: BGP: AB01:2011:7:100::3 active went from Active to Idle
* Nov 8 17:22:11.232: BGP: nrb global AB01:2011:7:100::3 Active open failed - open timer running

R1#ping ipv6 AB01:2011:7:100::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to AB01:2011:7:100::3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
    
```

Sending 5, 100-byte ICMP Echos to AB01:2011:7:100::3, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

An engineer configured BGP between routers R1 and R3. The BGP peers cannot establish neighbor adjacency to be able to exchange routes. Which configuration resolves this issue?

- A. R3router bgp 6502 address-family ipv6neighbor AB01:2011:7:100::1 activate
- B. R1router bgp 6501 address-family ipv6neighbor AB01:2011:7:100::3 activate
- C. R3router bgp 6502neighbor AB01:2011:7:100::1 ebgp-multihop 255
- D. R1router bgp 6501 neighborAB01:2011:7:100::3ebgp-multihop255

**Answer: A**

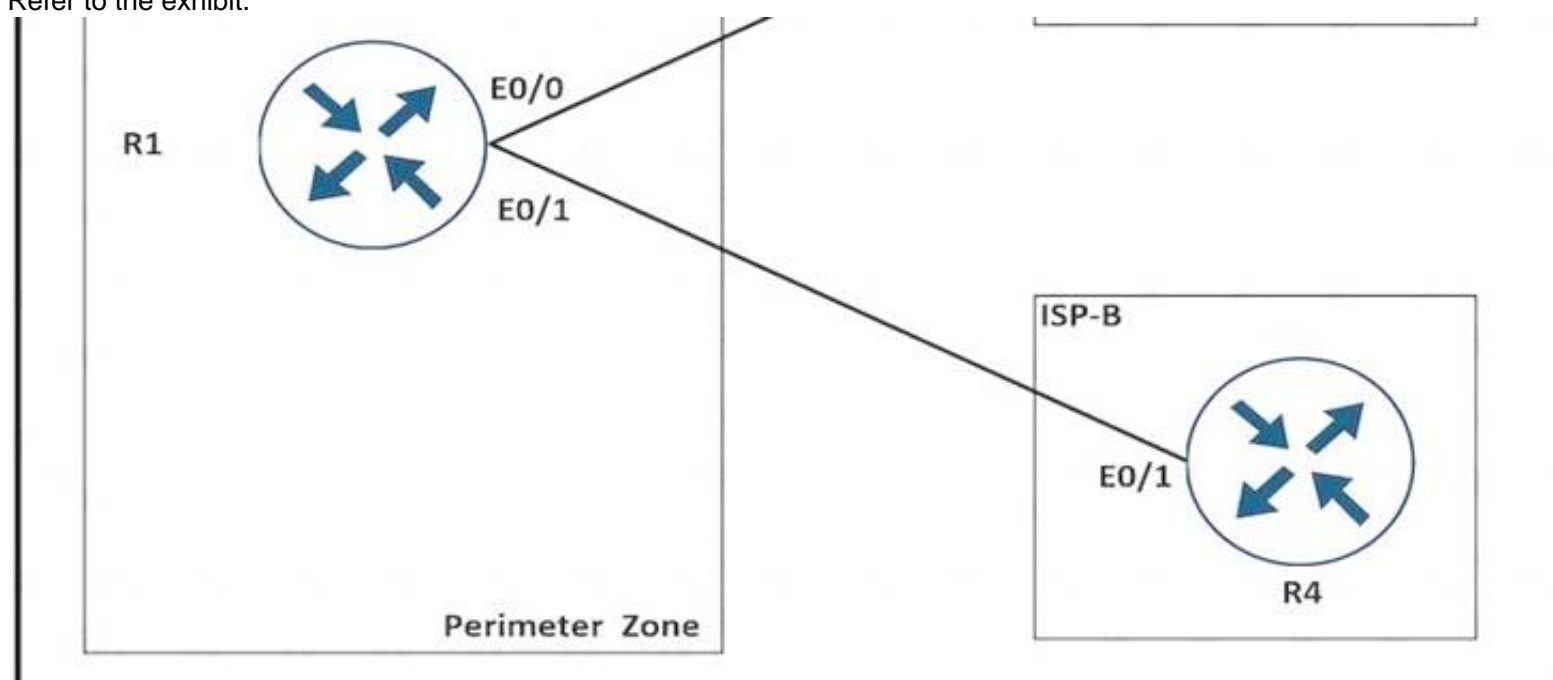
**Explanation:**

From the output, we learned that R1 was trying to establish BGP neighbor relationship with R3 but failed. Both of them were using physical interface to establish neighbor relationship so we don't need the "... ebgp-multihop" command here. The only reasonable answer is R3 has not been configured to activate BGP neighbor relationship with R1.

**NEW QUESTION 353**

- (Exam Topic 2)

Refer to the exhibit.



A network is under a cyberattack. A network engineer connected to R1 by SSH and enabled the terminal monitor via SSH session to find the source and destination of the attack. The session was flooded with messages, which made it impossible for the engineer to troubleshoot the issue. Which command resolves this issue on R1?

- A. no terminal monitor
- B. (config)#terminal no monitor
- C. #terminal no monitor
- D. (config)#no terminal monitor

**Answer: C**

**Explanation:**

To turn off terminal monitor, use "terminal no monitor" in the enable mode

**NEW QUESTION 355**

- (Exam Topic 2)

Which configuration feature should be used to block rogue router advertisements instead of using the IPv6 Router Advertisement Guard feature?

- A. VACL blocking broadcast frames from nonauthorized hosts
- B. PVLANS with promiscuous ports associated to route advertisements and isolated ports for nodes
- C. PVLANS with community ports associated to route advertisements and isolated ports for nodes
- D. IPv4 ACL blocking route advertisements from nonauthorized hosts

**Answer: B**

**Explanation:**

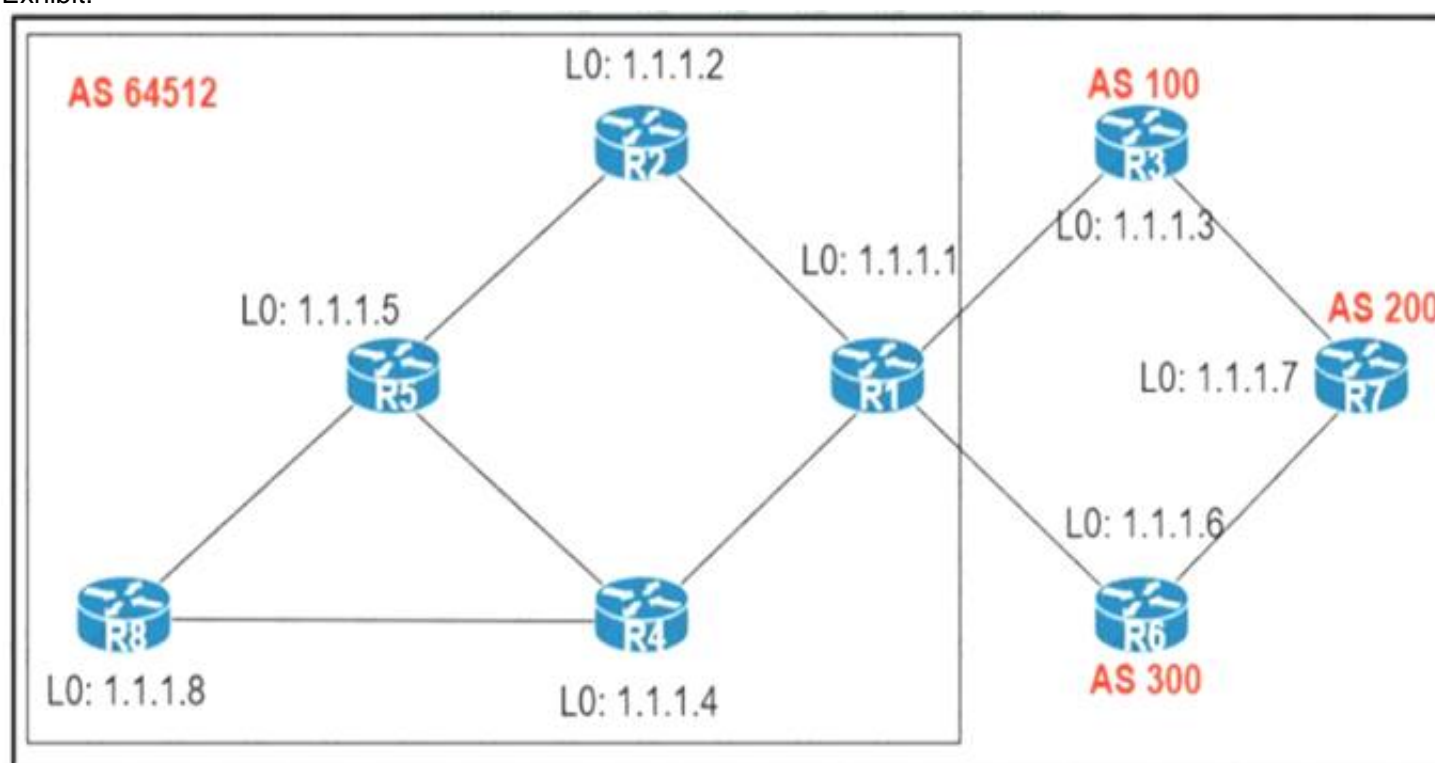
The IPv6 Router Advertisement Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement guard messages that arrive at the network device platform. Router Advertisements are used by devices to announce themselves on the link. The IPv6 Router Advertisement Guard feature analyzes these router advertisements and filters out router advertisements that are sent by unauthorized devices. Certain switch platforms can already implement some level of rogue RA filtering by the administrator configuring Access Control Lists (ACLs) that block RA ICMP messages that might be inbound on "user" ports.

Reference: <https://datatracker.ietf.org/doc/html/rfc6104>

**NEW QUESTION 359**

- (Exam Topic 2)

Exhibit:



An engineer configured R2 and R5 as route reflectors and noticed that not all routes are sent to R1 to advertise to the eBGP peers. Which iBGP routers must be configured as route reflectors to advertise all routes to restore reachability across all networks?

- A. R1 and R4
- B. R1 and R5
- C. R4 and R5
- D. R2 and R5

**Answer: C**

**Explanation:**

When R2 & R5 are route reflectors (RRs), routes from R4 & R8 are advertised to R5 and R5 advertises to R2. But R2 would drop them as R2 is also a RR. Therefore some routes are missing on R1 to advertise to eBGP peers.

Good reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/TECRST-2310.pdf>

Route reflectors (RR) must be fully iBGP meshed so we cannot configure RR on both R1 and R5.

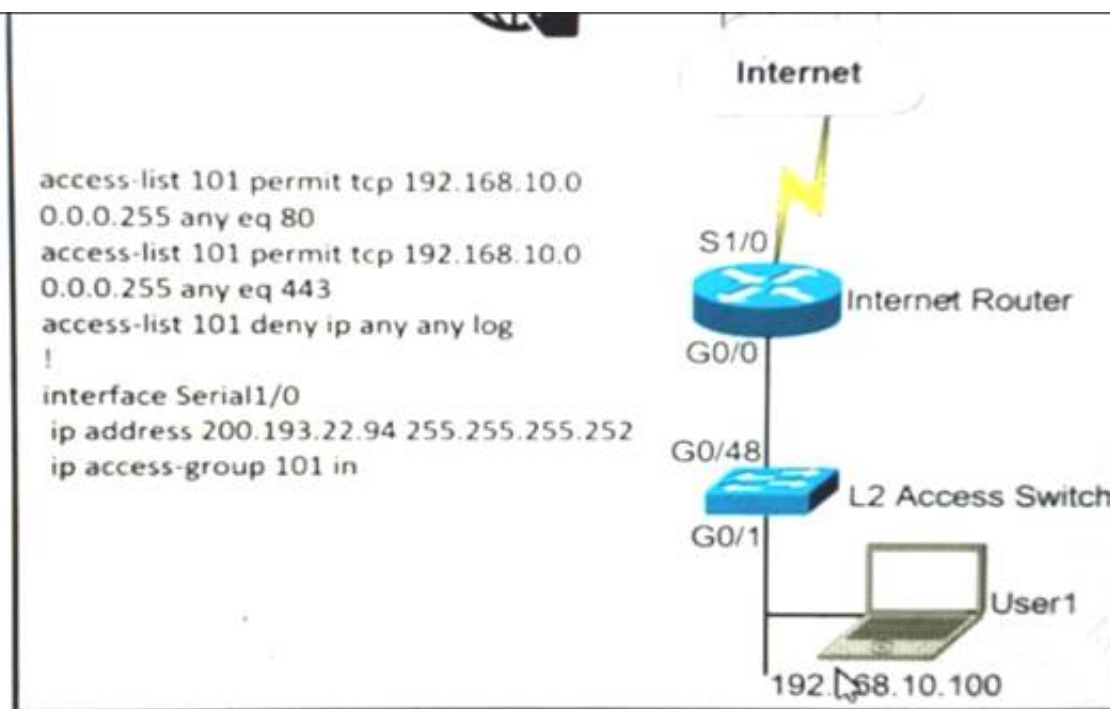
We should choose routers at the center of the topology RRs, in this case R4 & R5.

**NEW QUESTION 364**

- (Exam Topic 2)

A network administrator is tasked to permit http and https traffic only toward the internet from the User1 laptop to adhere to company's security policy. The administrator can still ping to www.cisco.com Which interface should the access list 101 be applied to resolve this issue?





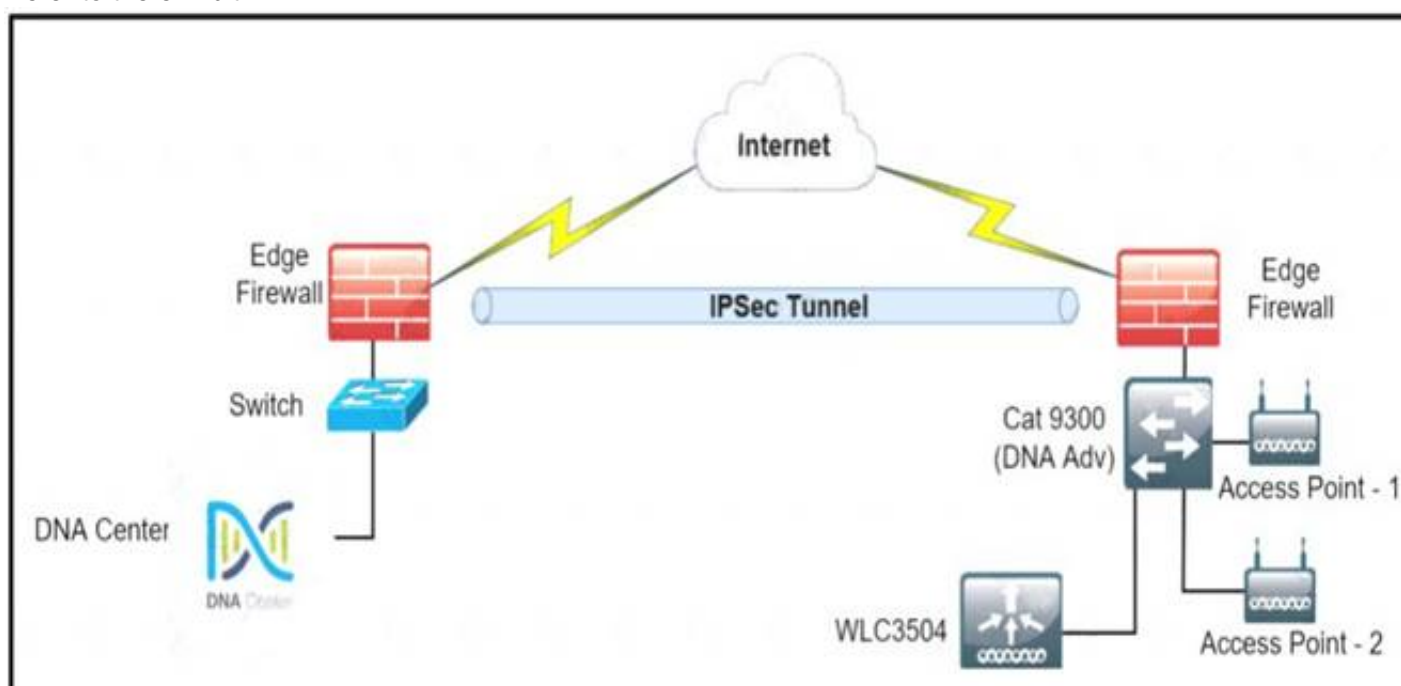
- A. Interface G0/48 in the incoming direction
- B. Interface G0/0 in the outgoing direction.
- C. Interface S1/0 in the outgoing direction.
- D. Interface G0/0 in the incoming direction.

Answer: D

#### NEW QUESTION 366

- (Exam Topic 2)

Refer to the exhibit.



A network administrator is discovering a Cisco Catalyst 9300 and a Cisco WLC 3504 in Cisco DNA Center. The Catalyst 9300 is added successfully However the WLC is showing [ error "uncontactable" when the administrator tries to add it in Cisco DNA Center. Which action discovers WLC in Cisco DNA Center successfully?

- A. Copy the .cert file from the Cisco DNA Center on the USB and upload it to the WLC 3504.
- B. Delete the WLC 3504 from Cisco DNA Center and add it to Cisco DNA Center again.
- C. Add the WLC 3504 under the hierarchy of the Catalyst 9300 connected devices.
- D. Copy the .pem file from the Cisco DNA Center on the USB and upload it to the WLC 3504.

Answer: D

#### Explanation:

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-c>

#### NEW QUESTION 367

- (Exam Topic 2)

Refer to the exhibit.

```
login block-for 15 attempts 10 within 120
login on-failure log
login on-success log
archive
log config
logging enable
logging size 300
notify syslog
```

```
snmp-server enable traps syslog
snmp-server host 172.16.17.1 public syslog
```

The administrator can see the traps for the failed login attempts, but cannot see the traps of successful login attempts. What command is needed to resolve the issue?

- A. Configure logging history 2
- B. Configure logging history 3
- C. Configure logging history 4
- D. Configure logging history 5

**Answer:** D

**Explanation:**

By default, the maximum severity sent as a syslog trap is warning. That is why you see syslog traps for login failures. Since a login success is severity 5 (notifications), those syslog messages will not be converted to traps. To fix this, configure:

**logging history 5**

Syslog levels are listed below

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

Note:

The syntax of login block is:

login block-for seconds attempts tries within seconds

**NEW QUESTION 371**

- (Exam Topic 2)

An engineer configured access list NON-CISCO in a policy to influence routes

**route-map PBR, deny, sequence 5**

**Match clauses:**

**ip address (access-list): NON-CISCO**

**Set clauses:**

**Policy routing matches: 0 packets, 0 bytes**

**route-map PBR, permit, sequence 10**

**Match clauses:**

**Set clauses:**

**ip next-hop 192.168.1.5**

**Policy routing matches: 388213827 packets, 222009685077 bytes**

What are the two effects of this route map configuration? (Choose two.)

- A. Packets are not evaluated by sequence 10.
- B. Packets are evaluated by sequence 10.

- C. Packets are forwarded to the default gateway.
- D. Packets are forwarded using normal route lookup.
- E. Packets are dropped by the access list.

**Answer:** BC

**Explanation:**

<https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds-ce.html>

**NEW QUESTION 376**

- (Exam Topic 2)

Which IGPs are supported by the MPLS LDP autoconfiguration feature?

- A. RIPv2 and OSPF
- B. OSPF and EIGRP
- C. OSPF and ISIS
- D. ISIS and RIPv2

**Answer:** C

**Explanation:**

The MPLS LDP Autoconfiguration feature enables you to globally enable Label Distribution Protocol (LDP) on every interface associated with an Interior Gateway Protocol (IGP) instance. This feature is supported on Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) IGPs. It provides

**NEW QUESTION 378**

- (Exam Topic 2)

An engineer configured a Cisco router to send reliable and encrypted notifications for any events to the management server. It was noticed that the notification messages are reliable but not encrypted. Which action resolves the issue?

- A. Configure all devices for SNMPv3 informs with priv.
- B. Configure all devices for SNMPv3 informs with auth.
- C. Configure all devices for SNMPv3 traps with auth.
- D. Configure all devices for SNMPv3 traps with priv.

**Answer:** A

**Explanation:**

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when this device receives traps."Send reliable and encrypted notifications for any events" so it is SNMP notifications. For encryption we need to configure "priv".

**NEW QUESTION 383**

- (Exam Topic 2)

Refer to the exhibit.

```

NY
router ospf 1
 network 192.168.12.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
!
interface E 0/0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 Cisco123

```

The neighbor relationship is not coming up Which two configurations bring the adjacency up? (Choose two)

- A. NYrouter ospf 1area 0 authentication message-digest
- B. LAinterface E 0/0ip ospf message-digest-key 1 md5 Cisco123
- C. NYinterface E 0/0no ip ospf message-digest-key 1 md5 Cisco123 ip ospf authentication-key Cisco123
- D. LAinterface E 0/0ip ospf authentication-key Cisco123
- E. LArouter ospf 1area 0 authentication message-digest

**Answer:** BE

**Explanation:**

The configuration on NY router is good for OSPF authentication. So we must enable OSPF authentication on LA router with the following commands:

```

router ospf 1
area 0 authentication message-digest interface E0/0
ip ospf message-digest-key 1 md5 Cisco123

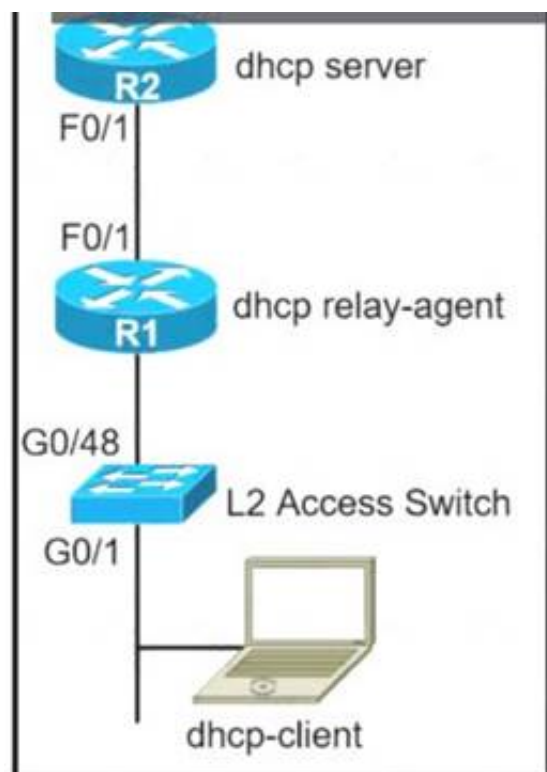
```

**NEW QUESTION 387**

- (Exam Topic 2)

Refer to the exhibit.





The network administrator can see the DHCP discovery packet in R1. but R2 is not replying to the DHCP request. The R1 related interface is configured with the DHCP helper address. If the PC is directly connected to the FaO/1 interface on R2, the DHCP server assigns as IP address from the DHCP pool to the PC. Which two commands resolve this issue? (Choose two.)

- A. service dhcp-relay command on R1
- B. ip dhcp option 82 command on R2
- C. service dhcp command on R1
- D. ip dhcp relay information enable command on R1
- E. ip dhcp relay information trust-all command on R2

**Answer:** CE

**Explanation:**

\* 1. R1 received DHCP packet and its interface was configured with the DHCP helper address. But we are not sure if R1 forward DHCP packet to R2 or not. 2. If we connect PC directly to R2 then this problem will not appear -> DHCP Server function was configured on R2.

From these facts, the most likely problem is related to Option 82. Maybe R2 ignored DHCP request packets because it was receiving these packets with the giant field set to 0.0.0.0.

By default Cisco IOS devices reject packets with zero "giaddr" and by default Cisco Catalyst switches use "giaddr" of zero when configured for DHCP snooping!

Reference: <https://blog.ine.com/2009/07/22/understanding-dhcp-option-82>

If we can run the "debug ip dhcp server packet" on R2, we may see these messages:

```
*Feb 22 23:54:57.759: IP: s=0.0.0.0 (FastEthernet0/1), d=255.255.255.255, len 34 4, input feature, MCI Check(64), rtype 0, forus FALSE, sendself FALSE, mtu 0, fw dchk FALSE
*Feb 22 23:54:57.759: IP: s=0.0.0.0 (FastEthernet0/1), d=255.255.255.255, len 34 4, rcvd 2
*Feb 22 23:54:57.759: IP: s=0.0.0.0 (FastEthernet0/1), d=255.255.255.255, len 34 4, stop process pak for forus packet
```

```
*Feb 22 23:54:57.759: DHCPDP: inconsistent relay information.
*Feb 22 23:54:57.759: DHCPDP: relay information option exists, but giaddr is zero
```

We are receiving the DHCP packet from R1, source 0.0.0.0, and destination 255.255.255.255 broadcast, but if you notice from the debug output, R2, our DHCP Server, is complaining that the relay information is inconsistent. Option 82, Information Option, is contained in the packet but the GIADDR is zero. The GIADDR stands for Gateway IP Address, which is the IP Address of the relaying agent. The Option 82, Information Option, would then contain the receiving port and hostname of the Relaying Agent by default.

R2 sees the Option 82 information, signalling that the DHCP packet might have been relayed, BUT there is no relaying IP Address. This is the behavior of DHCP Snooping when enabling it on a switch, and since the switchport does not contain an IP Address, since it's Layer 2, no GIADDR will be added.

Instead, just the Option 82 Information is added and this is the problem we have, but there are options:

- \* 1. You could trust all on R2 the DHCP Server, which will cause the server to not be so suspicious: – ip dhcp relay information trust-all – ip dhcp relay information trusted
- 2. Disable the addition of Option 82 information on SW: – no ip dhcp snooping information option
- 3. Trust the port that is receiving the DHCP Discover: – ip dhcp snooping trust

Any of these options will fix our predicament. Reference: <https://evilttl.com/wiki/DHCP-Snooping>

But in the answer choices, we only have 1 correct answer which is the command "ip dhcp relay information trust-all". We checked if we need any "service dhcp..." command on both IOS version 12.4 and 15.1:

Therefore we only have the "service dhcp" command, we don't have any "service dhcp-relay" command available. But the description of the "service dhcp" command says that it enables both DHCP server and relay agent so this is the best answer left.

**NEW QUESTION 390**

- (Exam Topic 2)

An engineer configured two routers connected to two different service providers using BGP with default attributes. One of the links is presenting high delay, which causes slowness in the network. Which BGP attribute must the engineer configure to avoid using the high-delay ISP link if the second ISP link is up?

- A. LOCAL\_PREF
- B. MED
- C. WEIGHT
- D. AS-PATH

**Answer:** A

**NEW QUESTION 392**

- (Exam Topic 2)

Refer to the exhibit.

```
admin@linux:~$ scp script.py admin@198.51.100.64:script.py
Password:
Administratively disabled.
admin@linux:~$ Connection to 198.51.100.64 closed by remote
host.
```

A network administrator has developed a Python script on the local Linux machine and is trying to transfer it to the router. However, the transfer fails. Which action resolves this issue?

- A. The SSH service must be enabled with the crypto key generate rsa command.
- B. The SCP service must be enabled with the ip scp server enable command.
- C. The Python interpreter must first be enabled with the guestshell enable command.
- D. The SSH access must be allowed on the VTY lines using the transport input ssh command.

**Answer:** B

**Explanation:**

The error “Administratively disabled” means we need to enable SCP on the router with the command: Router(config)#ip scp server enable

**NEW QUESTION 395**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-410 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-410 Product From:

<https://www.2passeasy.com/dumps/300-410/>

## Money Back Guarantee

### 300-410 Practice Exam Features:

- \* 300-410 Questions and Answers Updated Frequently
- \* 300-410 Practice Questions Verified by Expert Senior Certified Staff
- \* 300-410 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 300-410 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year